iab.

Privacy Laws & Digital Advertising:

Multi-jurisdictional Overview and Implications

July 2021

Cross-Jurisdiction Privacy Project (CJPP)

Table of Contents

Introduction 9
Acknowledgments 12
About Us 15
About Our Sponsors 16
CJPP Australia Data Guidance 17
1.The Law 18
2. Scope of Application 19
3. Definitions 26
4. Data Controller Rights and Responsibilities 37
5. Data Subject Rights/Exemptions 52
6. Data Controller and Processor Agreements 57
7. Data Transfer & Outsourcing 58
8. Audit/Accountability 59
9. Data Retention 60
10. Data Protection Authority | Regulatory Authority 60
11. Sanctions 61
12. Notification | Certification | Registration 64
13. Data Protection Officer 64
14. Self-Regulation 65
15. Pending Privacy Bills 67
CJPP Brazil Data Guidance 69
1.The Law 70
2. Scope of Application 71
3. Key Definitions | Basic Concepts 75
4. Data Controller Rights and Responsibilities 84
5. Data Subject Rights/Exemptions 101
6. Data Controller and Processor Agreements 105

7. Data Transfer & Outsourcing . . . 107
8. Audit/Accountability . . . 109
9. Data Retention . . . 109
10. Data Protection Authority | Regulatory Authority . . . 110
11. Sanctions . . . 113
12. Notification | Certification | Registration . . . 116
13. Data Protection Officer . . . 117
14. Self-Regulation . . . 118
15. Pending Privacy Bills . . . 119

CJPP Canada Data Guidance . . . 120
1.The Law . . . 121
2. Scope of Application . . . 122
3. Definitions . . . 130
4. Data Controller Rights and Responsibilities . . . 138
5. Data Subject Rights/Exemptions . . . 152
6. Data Controller and Processor Agreements . . . 155
7. Data Transfer & Outsourcing . . . 156
8. Audit/Accountability . . . 157
9. Data Retention . . . 158
10. Data Protection Authority | Regulatory Authority . . . 158
11. Sanctions . . . 159
12. Notification | Certification | Registration . . . 163
13. Data Protection Officer . . . 163
14. Self-Regulation . . . 164
15. Pending Privacy Bills . . . 164

CJPP China Data Guidance . . . 166
1.The Law . . . 167

2. Scope of Application . . . 172
3. Definitions . . . 180
4. Data Controller Rights and Responsibilities . . . 192
5. Data Subject Rights/Exemptions . . . 205
6. Data Controller and Processor Agreements . . . 209
7. Data Transfer & Outsourcing . . . 210
8. Audit/Accountability . . . 212
9. Data Retention . . . 213
10. Data Protection Authority | Regulatory Authority . . . 214
11. Sanctions . . . 215
12. Notification | Certification | Registration . . . 223
13. Data Protection Officer . . . 224
14. Self-Regulation . . . 225
15. Pending Privacy Bills . . . 227

CJPP India Data Guidance . . . 245

1.The Law . . . 246
2. Scope of Application . . . 249
3. Definitions . . . 253
4. Data Controller Rights and Responsibilities . . . 260
5. Data Subject Rights/Exemptions . . . 267
6. Data Controller and Processor Agreements . . . 268
7. Data Transfer & Outsourcing . . . 269
8. Audit/Accountability . . . 269
9. Data Retention . . . 270
10. Data Protection Authority | Regulatory Authority . . . 270
11. Sanctions . . . 271
12. Notification | Certification | Registration . . . 272
13. Data Protection Officer . . . 273

14. Self-Regulation 273
15. Pending Privacy Bills 274

CJPP Israel Data Guidance 280
1.The Law 281
2. Scope of Application 282
3. Definitions 284
4. Data Controller Rights And Responsibilities 292
5. Data Subject Rights/Exemptions 300
6. Data Controller and Processor Agreements 303
7. Data Transfer & Outsourcing 304
8. Audit/Accountability 306
9. Data Retention 307
10. Data Protection Authority | Regulatory Authority 307
11. Sanctions 308
12. Notification | Certification | Registration 313
13. Data Protection Officer 314
14. Self-Regulation 315
15. Pending Privacy Bills 315

CJPP Japan Data Guidance 318
1.The Law 319
2. Scope of Application 320
3. Definitions 322
4. Data Controller Rights and Responsibilities 330
5. Data Subject Rights/Exemptions 338
6. Data Controller and Processor Agreements 340
7. Data Transfer & Outsourcing 341
8. Audit/Accountability 342

9. Data Retention . . . 342
10. Data Protection Authority | Regulatory Authority . . . 343
11. Sanctions . . . 343
12. Notification | Certification | Registration . . . 347
13. Data Protection Officer . . . 347
14. Self-Regulation . . . 348
15. Pending Privacy Bills . . . 348

CJPP Mexico Data Guidance . . . 350
1.The Law . . . 351
2. Scope of Application . . . 352
3. Definitions . . . 356
4. Data Controller Rights and Responsibilities . . . 364
5. Data Subject Rights/Exemptions . . . 373
6. Data Controller and Processor Agreements . . . 375
7. Data Transfer & Outsourcing . . . 376
8. Audit/Accountability . . . 377
9. Data Retention . . . 378
10. Data Protection Authority | Regulatory Authority . . . 378
11. Sanctions . . . 379
12. Notification | Certification | Registration . . . 383
13. Data Protection Officer . . . 383
14. Self-Regulation . . . 384
15. Pending Privacy Bills . . . 384

CJPP Nigeria Data Guidance . . . 385
1.The Law . . . 386
2. Scope of Application . . . 389
3. Definitions . . . 393

4. Data Controller Rights and Responsibilities . . . 400
5. Data Subject Rights/Exemptions . . . 410
6. Data Controller and Processor Agreements . . . 413
7. Data Transfer & Outsourcing . . . 415
8. Audit/Accountability . . . 417
9. Data Retention . . . 419
10. Data Protection Authority | Regulatory Authority . . . 421
11. Sanctions . . . 423
12. Notification | Certification | Registration . . . 427
13. Data Protection Officer . . . 428
14. Self-Regulation . . . 429

CJPP Singapore Data Guidance . . . 430
1.The Law . . . 431
2. Scope of Application . . . 436
3. Definitions . . . 439
4. Data Controller Rights And Responsibilities . . . 452
5. Data Subject Rights/Exemptions . . . 468
6. Data Controller and Processor Agreements . . . 475
7. Data Transfer & Outsourcing . . . 479
8. Audit/Accountability . . . 482
9. Data Retention . . . 483
10. Data Protection Authority | Regulatory Authority . . . 485
11. Sanctions . . . 486
12. Notification | Certification | Registration . . . 494
13. Data Protection Officer . . . 495
14. Self-Regulation . . . 497
15. Pending Privacy Bills . . . 497

CJPP South Korea Data Guidance 501

1.The Law 502

2. Scope of Application 505

3. Definitions 507

4. Data Controller Rights and Responsibilities 516

5. Data Subject Rights/Exemptions 526

6. Data Controller and Processor Agreements 529

7. Data Transfer & Outsourcing 530

8. Audit/Accountability 531

9. Data Retention 532

10. Data Protection Authority | Regulatory Authority 533

11. Sanctions 534

12. Notification | Certification | Registration 537

13. Data Protection Officer 537

14. Self-Regulation 538

15. Pending Privacy Bills 539

Introduction

The IAB's Legal Affairs Council launched the Cross-Jurisdiction Privacy Project ("CJPP") in August of 2020 with the goal of exploring how the privacy laws of Australia, Brazil, Canada, China, India, Israel, Japan, Mexico, Nigeria, Singapore, and South Korea apply to the digital advertising industry. In addition to surfacing how these laws compare to each other, the CJPP provided an opportunity to examine how participants in digital ad transactions could more efficiently communicate their compliance with those laws through a global privacy string being developed by the IAB Tech Lab. The Cross-Jurisdiction Privacy Project consisted of two phases. The first phase encompassed the drafting of this **CJPP Compendium**. The second phase involved the compilation of a chart, the **CJPP Legal Specifications**, representing those elements of the applicable privacy laws that digital advertising counterparties need to communicate to one another to demonstrate their compliance with such laws through a global privacy string. That work product was prepared by us for the IAB Tech Lab and the industry.

The CJPP taught us much about each participating country's privacy laws. For example, we learned that each country's privacy regime has its own nuances and strikes its own balance between transparency into how information about consumers is processed for digital advertising and consumers' ability to understand and make choices about that processing. Indeed, at least half of the jurisdictions examined did not mandate affirmative consent to use personal information for digital advertising activities such as selecting which digital ads are shown to users or generating audience segments for advertising purposes. Moreover, nearly all of the jurisdictions examined (Brazil being the notable exception) did not require the kind of fine-grained purpose specification required under the European Union General Data Protection Regulation (GDPR). Further, with respect to the GDPR's requirements that necessitate a global vendor list for compliance, only two jurisdictions examined require a publisher to disclose a detailed list of the names of third parties who may participate in aforementioned digital advertising purposes. These findings disabused us of the popular misconception that emerging privacy regimes around the world are merely copies of the GDPR.

This CJPP Compendium sets forth not only an overview of the privacy laws of these countries, but also *how* they apply to digital advertising participants and the transactions they typically undertake. By way of example, many privacy laws across the globe define personal information, in some manner, as information about a natural person that is identifiable or reasonably identifiable to that person. However, that standard applies in different ways across different jurisdictions. Under some countries' privacy laws, for example, information about a person's internet-connected device (such as IP address or certain device IDs) taken alone is generally not deemed to be personal information. In contrast, under some countries' privacy laws, the mere possibility that the same information theoretically could, but never actually will, be paired with information that directly identifies an individual in the possession of another company can render it personal information. Other jurisdictions have further nuances in between those two positions. This CJPP Compendium sheds light on these and other very challenging scenarios that are common in the digital advertising industry.

Each chapter of this IAB CJPP Compendium covers how a particular jurisdiction's privacy regime applies to our industry, including:

- The statutes, guidelines, and case law relevant to digital advertising activities
- Whether and when publishers' and advertisers' data processing activities trigger the extraterritorial reach (if any) of the privacy law
- Key privacy law definitions, including what it means to "collect" personal information and who (the publisher or ad tech company) is deemed to collect personal information when a publisher allows an ad tech company to integrate with its digital properties
- Whether pseudonymous identifiers, such as mobile advertising IDs, IP addresses, hashed email address, or publisher IDs, constitute personal information, either alone or in combination with other information about a data subject
- Data controller obligations, including the notice requirements for sharing personal information with third parties for advertising purposes, and the specific digital advertising activities or purposes that must be disclosed to data subjects; whether and what type of consent must be obtained for different types or uses of data; and the available legal bases for specific digital advertising activities
- The rights available to data subjects and which entities in the advertising chain must provide those rights
- Contractual requirements for processors to provide digital advertising services on behalf of data controllers, and the cross-border transfer limitations and obligations when ad tech data recipients are in a different jurisdiction
- Audit, accountability, data retention, and data protection officer requirements for parties in the ad tech ecosystem
- The scope of liability for ad tech companies for the collection activities of publishers and advertisers, and vice versa
- Pending privacy bills and regulations that may change the digital advertising landscape if (or when) they go into effect

We are grateful to the more than 150 lawyers from across the globe who participated in this project. A list of our member companies who generously contributed the time of their legal teams to this endeavor is included in our Acknowledgements page. We are also indebted to the law firms in the 11 jurisdictions who provided their time, labor, expertise, and drafting skills in preparation of the CJPP Compendium, as well as their willingness to meet with working groups for nearly a year to refine the document to its present form. Those lawyers and their law firms are also included in the Acknowledgements page.

Finally, our work would not have been possible without the invaluable support of our strategic partners in this project, OneTrust LLC and BakerHostetler LLP. OneTrust generously provided the Cross-Jurisdiction Privacy Project with access to its OneTrust DataGuidance® tools, as well as to its research team. BakerHostetler generously provided support and legal acumen through an attorney assigned to each jurisdiction's working group, which helped immeasurably in coordinating such a complicated endeavor and refining this document into the most relevant work product possible.

The IAB Legal Affairs Council will continue to update this document and may cover other jurisdictions as legal changes warrant.

Note that this document includes information about the privacy requirements of participating jurisdictions, but it is not legal advice. Readers should consult with their own legal counsel regarding the privacy laws of jurisdictions where they do business.

Sincerely,

Michael Hahn
SVP & General Counsel
IAB & IAB Tech Lab

Acknowledgements

This report would not have been possible without the guidance and direction of the IAB Legal Affairs Committee and the time, dedication, and contributions of the Cross-Jurisdiction Privacy Project (CJPP) Working Group members and companies, and contributing law firms listed below. We extend our thanks and deepest appreciation.

Sponsors

BakerHostetler

OneTrust
PRIVACY, SECURITY & GOVERNANCE

Cross-Jurisdiction Privacy Project (CJPP) Working Group Member Participants

AccuWeather, Inc.
Adobe Systems Incorporated
Advance Publications Inc./Condé Nast
Akin Gump Strauss Hauer & Feld LLP
Alliant Cooperative Data Solutions, LLC
Amazon.com, Inc.
Amobee, Inc.
Ampersand/National Cable Communications LLC
BakerHostetler
Big Token Inc.
BuzzFeed Inc.
CDK Global LLC
Chipotle Mexican Grill Inc.
The Coca-Cola Company
Comcast Cable
Comscore Inc.
Criteo SA
Davis+Gilbert LLP
Dentons US LLP
Dentsu Aegis Network Ltd.
Dun & Bradstreet LLC
eBay Inc.
Epsilon Data Management, LLC
Extreme Reach, Inc.
Free Wheel, A Comcast Company
Google, Inc.
GroupM Worldwide Inc.
The Hershey Company
Index Exchange Inc.
Inmar Inc.
Integral Ad Science, Inc.
Kelley Drye & Warren LLP
LeDoux Consulting
Loeb & Loeb LLP
Lowenstein Sandler LLP
Maven Coalition Inc.
Norton Rose Fulbright LLP
OneTrust
OpenSlate
Paul Hastings LLP
Pubmatic Inc.
Samba TV
Samsung Electronics America, Inc.
Sizmek by Amazon.com Inc.
Sovrn Holdings Inc.
SRAX Inc./BIGtoken Inc.

Taboola Inc.
TripleLift Inc.
VEVO LLC
Vizio Inc.
Ziff Davis, LLC
ZipRecruiter Inc.
ZwillGen PLLC

Contributing Law Firms & Organizations

All Jurisdictions

BakerHostetler - Carolina Alonso, Stanton Burke, Gerald Ferguson, Nichole Sterling, Patrick Waldrop
OneTrust - Stephanie Hanson, Alexis Kateifides, Matteo Quartieri

Australia

Bird and Bird LLP - Sophie Dawson, James Hoy, Jeremy Tan
Clyde & Co LLP - Alec Christie
McCullough Robertson - Alex Hutchens
Thomson Geer - Peter LeGuay, Hannah Scrivener

Brazil

Kasznar Leonardos - Claudio Roberto Barbosa
Leonardi Advogados - Marcel Leonardi
Opice Blum, Bruno e Vainzof Advogados Associados - Renato Opice Blum, Henrique Fabretti Moraes, Caio César Carvalho Lima
Veirano Advogados - Cecilia Alberton Coutinho Silva, Fabio Pereira

Canada

Blake, Cassels & Graydon LLP - Wendy Mee
Dentons Canada LLP - Chantal Bernier
Fasken Martineau DuMoulin LLP - Alex Cameron, Daanish Samadmoten
Norton Rose Fulbright Canada LLP - Imran Ahmad
Osler, Hoskin & Harcourt LLP - John Salloum, Adam Kardash

China

Baker McKenzie LLP - Lex Kuo, Michael Wang, Anne Petterd, Daniel Pardede, Adhika Wiyoso
Baker Botts LLP - Manuel Maisog
Fieldfisher LLP - Dehao Zhang, Zhaofeng Zhou, Richard Lawne, Mark Webber
Hunton Andrews Kurth LLP - Dora Luo, Yanchen Wang

India

J. Sagar Associates (JSA) - Probir Roy Chowdhury, Kavya Thayil, Yajas Setlur
Spice Route Legal - Mathew Chacko, Aadya Misra, Purushotham Kittane

Israel

FISCHER (FBC & Co.) - Omri Rachum-Twaig, Amit Dat
Soroker Agmon Nordman - Eran Soroker, Jonathan Agmon, Ady Nordman, Robert Dorneanu, Devorah Spigelman
Sharir, Shiv & Co. Law Offices (now a part of FISHER (FBC & Co.)) - Yoram Shiv, Shira Nagar

Japan

Atsumi & Sakai - Chie Kasahara, Daniel Hounslow, Ryuichi Nozaki
Mori Hamada & Matsumoto - Atsushi Okada
Nishimura & Asahi - Yuki Kawai

Mexico

Basham, Ringe y Correa, S.C. - Adolfo Athié Cervantes, Renata Bueron Valenzuela,
Erika Rodgríguez Kushelevich
Davara Abogados S.C. - Isabel Davara, Alexis Cervantes
González Calvillo, S.C. - Lucia Fernandez Gonzalez, Maria de la Nieves Hernandez Solano,
Alberto Pliego Beguerisse

Nigeria

Lelaw Barristers & Solicitors - Chuks Okoriekwe, Gabriel Omoniyi, Samuel Ngwu
Olisa Agbakoba Legal (OAL) - Beverly Agbakoba, Dr. Olisa Agbakoba, Yvonne Ezekiel, Olayinka Suara,
Kaetochukwu M. Udeh, Ginika Ikechukwu
Paragon Advisors - Akinkunmi Akinwunmi
Templars - Khadija Osammor, Olumide Akpata, Tolulope Falokun, Ijeoma Uju, Dayo Okusami, Ifeoluwa Ibiyemi

Singapore

Drew & Napier LLC - Chong Kin Lim, David Alfred
Reed Smith LLP UK - Charmian Aw, Tania Teng

South Korea

Bae, Kim & Lee LLC - Tae Uk Kang, Susan Park, Do Yeup Kim
Lee & Ko - Kwang Bae Park, Minchae Kang

About Us

The Interactive Advertising Bureau empowers the media and marketing industries to thrive in the digital economy. Its membership comprises more than 650 leading media companies, brands, and the technology firms responsible for selling, delivering, and optimizing digital ad marketing campaigns. The trade group fields critical research on interactive advertising, while also educating brands, agencies, and the wider business community on the importance of digital marketing. In affiliation with the IAB Tech Lab, IAB develops technical standards and solutions. IAB is committed to professional development and elevating the knowledge, skills, expertise, and diversity of the workforce across the industry. Through the work of its public policy office in Washington, D.C., the trade association advocates for its members and promotes the value of the interactive advertising industry to legislators and policymakers. Founded in 1996, IAB is headquartered in New York City.

For more information, visit iab.com

About Our Sponsors

BakerHostetler

Recognized as one of the top firms for client service, BakerHostetler is a leading law firm that helps clients around the world address their most complex and critical business and regulatory issues. With six core practice groups – business, digital assets and data management, intellectual property, labor and employment, litigation and tax – the firm has nearly 1,000 lawyers located coast to coast.

For more information, visit bakerlaw.com

OneTrust
PRIVACY, SECURITY & GOVERNANCE

OneTrust is the #1 fastest-growing company on Inc. 500 and the category-defining enterprise platform to operationalize trust. More than 10,000 customers, including half of the Fortune Global 500, use OneTrust to make trust a competitive differentiator, implementing central agile workflows across privacy, security, data governance, GRC, third-party risk, ethics and compliance, and ESG programs.

To learn more: OneTrust.com and LinkedIn.

iab.

Australia

Cross-Jurisdiction Privacy Project

1. THE LAW

1.1 Overview

The key privacy laws in Australia which are applicable to the digital advertising ecosystem are contained in the Privacy Act 1988 (Cth) (**Privacy Act**), containing 13 Australian Privacy Principles (**APPs**), and the Spam Act 2003 (Cth) (**Spam Act**).

1.2 Key Acts, Regulations, and Directives

The Privacy Act generally regulates how Australian Government agencies and private sector organizations with an annual turnover of more than $3 million handle personal information (referred to, together with some other organizations, as **APP entities**). The Privacy Act includes 13 APPs which are the cornerstone of the privacy protection framework in the Privacy Act, and it establishes a set of standards, rights, and obligations that apply in relation to personal information.

The Spam Act regulates commercial email and other types of commercial electronic messages (such as instant messages, SMS, and MMS). It prohibits the sending of unsolicited commercial electronic messages and requires that commercial electronic messages identify the sender and contain a functional unsubscribe facility.

The following guidance is focused on the key privacy laws in Australia that are applicable to the digital advertising ecosystem. There are other laws that are applicable to digital advertising, including consumer and surveillance laws as well as copyright legislation, but these are not addressed here.

1.3 Guidelines

Relevant guidance published by the privacy regulator in Australia, the Office of the Australian Information Commissioner (**OAIC**), includes:

- What is personal information?
- Privacy Management Framework
- Guide to Undertaking Privacy Impact Assessments
- Guide to Securing Personal Information
- Data Breach Preparation and Response
- De-identification and the Privacy Act
- De-Identification Decision Making Framework
- Guide to Data Analytics and the Australian Privacy Principles
- Direct Marketing

- Targeted Advertising
- Spam and Telemarketing

Additionally, the APP Guidelines outline the mandatory requirements of the APPs, how the OAIC interprets them, and matters they take into account.

1.4 Caselaw

Recent case law in Australia regarding privacy that is relevant to the digital advertising ecosystem includes:

- Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4 (**Telstra**)
- Flight Centre Travel Group (Privacy) [2020] AICmr 57 (**Flight Centre**)
- Australian Information Commissioner v Facebook Inc (No 2) [2020] FCA 1307 (**Facebook No 2**).

The relevance of the cases mentioned above, and their application to the digital advertising ecosystem, will be explained in the sections they relate to.

1.5 Application to Digital Advertising

The Privacy Act and APPs apply to the handling of personal information by members of the digital advertising ecosystem, subject to issues of jurisdictional reach discussed below.

The Spam Act will also apply to members of the digital advertising ecosystem to the extent that they send commercial electronic messages with an "Australian link".

2. SCOPE OF APPLICATION

2.1 Who Do the Laws/Regulations Apply to and What Types of Processing Activities are Covered/Exempted?

As mentioned above, the Privacy Act and the APPs regulate "APP entities", comprising Australian Government agencies and certain private sector organisations, in relation to their handling of personal information.

The Privacy Act applies to acts done, or practices engaged in, in Australia. It also applies to acts done, or practices engaged in, outside Australia and the external territories by Australian Government agencies and by organizations or small business operators with an "Australian link," the meaning of which is explained below.

The Spam Act separately regulates the sending of commercial email and other types of commercial electronic messages (such as instant message, SMS, and MMS) with an "Australian link," the meaning of which is also explained below.

Overview

APP entities, to whom the Privacy Act and the APPs apply, include:

- Australian Government agencies.
- Private sector organizations with an annual turnover of more than $3 million.
- A limited number of small business operators, including:
    - Private sector health service providers.
    - Businesses that sell and purchase personal information.
    - Credit reporting bodies.
    - Contracted service providers for Australian Government agencies.
    - Businesses that hold accreditation under the Consumer Data Right system.
    - Businesses that have opted-in to the Privacy Act
    - Businesses that are related to businesses that are covered by the Privacy Act.

A "small business operator" is defined as an individual, body corporate, partnership, unincorporated association, or trust that carries on one or more small businesses and does not carry on any other businesses. A small business is a business with an annual turnover of AUD$3,000,000 or less.

The Privacy Act does not apply, generally speaking, to:

- State or Territory government agencies.
- Individuals acting in a private or domestic capacity.
- Public universities and schools.
- The handling of employee records in some situations.
- The majority of small business operators.
- Media organizations which have publicly committed to privacy standards acting in the course of journalism.
- Registered political parties and political representatives.

The Spam Act applies to the sending of commercial email and other types of commercial electronic messages (such as instant message, SMS, and MMS).

Application to Digital Advertising

The Privacy Act applies to members of the digital advertising ecosystem that are APP entities including Australian Government agencies, private sector organizations with an annual turnover of more than $3 million,

and businesses that sell and purchase personal information.

The Spam Act applies to members of the digital advertising ecosystem who send commercial emails and other types of commercial electronic messages.

2.2 Jurisdictional Reach

Overview

The Privacy Act applies to acts done, or practices engaged in, in Australia. It also applies to acts done, or practices engaged in, outside Australia and the external territories by Australian Government agencies and by private sector organizations or small business operators with an "Australian link". Section 5B of the Privacy Act provides that an organization or small business operator has an Australian link if it:

- Is a partnership formed, trust created or body incorporated in Australia or an external Territory.
- Is an unincorporated association that has its central management and control in Australia or an external Territory.
- Carries on business in Australia and the personal information was collected or held by the organization or small business operator in Australia or an external Territory, either before or at the time of the act or practice.

The application of section 5B of the Privacy Act was recently considered by the Federal Court in Facebook No 2, which concerned an application by Facebook Inc. to set aside service of an originating application on them by the OAIC in relation to proceedings brought against the social media platform regarding the Cambridge Analytica scandal. Justice Thawley dismissed the application by Facebook Inc., finding that the Commissioner had established an arguable case to warrant exposing Facebook Inc. to litigation in Australia, in part, on the basis that:

- Facebook Inc. carried on business in Australia within the meaning of s 5B(3), through its provision of services to Facebook Ireland.[1]
- Collected and stored information in Australia within the meaning of s 5B(3), through its installation and operation of cookies.[2]

With respect to the notion of "carrying on business in Australia", it was held in *Australian Securities and Investments*

[1] *Australian Information Commissioner v Facebook Inc (No 2)* [2020] FCA 1307, at [119].

[2] Ibid, at [175].

Commission v ActiveSuper Pty Ltd (No 1) [2012] FCA 1519 (***ActiveSuper***), that:

Provided that there are acts within Australia which are part of the company's business, the company will be doing business in Australia although the bulk of their business is conducted elsewhere and it maintains no office in Australia.[3]

The Spam Act regulates the sending of commercial electronic messages with an "Australian link". Commercial electronic messages will have an Australian link for the purposes of the Spam Act if:

- The message originates in Australia.
- The individual or organization who sent the message, or authorized the sending of the message, is:
    - An individual who is physically present in Australia when the message is sent.
    - An organization whose central management and control is in Australia when the message is sent.
- The computer, server or device that is used to access the message is located in Australia.
- The relevant electronic accountholder is:
    - An individual who is physically present in Australia when the message is accessed.
    - An organization that carries on business or activities in Australia when the message is accessed.
- If the message cannot be delivered because the relevant electronic address does not exist–assuming that the electronic address existed, it is reasonably likely that the message would have been accessed using a computer, server, or device located in Australia.

Application to Digital Advertising

Scenario 1 (The baseline): A user residing in Australia (determined by IP address or geo identifier) goes onto an Australian domain and is served an ad by an Australian advertiser. The advertiser uses the user data to build a user profile.

The Privacy Act will apply to both the serving of the ad to the user as well as the building of a user profile, but only to the extent that the user is identified or reasonably identifiable to each of those parties. The issue of when a user is identified under Australian law is discussed further below. In summary, there is currently some doubt as to whether an online identifier such as an IP address is sufficient to relevantly identify someone under Australian law,

[3] *Australian Information Commissioner v Facebook Inc (No 2)* [2020] FCA 1307, at [119].

and changes to the law have proposed which would make it clear that online identifiers are sufficient for the purpose of attracting the operation of the Privacy Act.

If the user is identified, or reasonably identifiable, the publisher will need to comply with APP 3 and APP 5 in relation to its collection of personal information, assuming that a first-party cookie is used. Assuming the publisher is a private sector organisation, APP 3 provides that it must not collect personal information unless it is reasonably necessary for one or more of its functions or activities. In the case of sensitive information, subject to limited exceptions, the individual must also consent to the collection. The publisher must also take such steps as are reasonable in the circumstances to notify the individual of certain matters prescribed in APP 5.

If the user is identified, or reasonably identifiable, the publisher and the advertiser will also both need to comply with the requirements of APP 7, which governs direct marketing including online behavioural advertising, in relation to the serving of the ad.

In the case of the publisher, who collects the information from the individual:

- The publisher must either obtain consent, or ensure that the individual must reasonably expect the publisher to use or disclose the information collected for the purpose of direct marketing.
- The publisher must provide a simple means by which the individual may opt out.
- The individual must not have made such a request.

In the case of the advertiser, who collects the information from the publisher:

- The individual must have consented to the use or disclosure of their personal information for the purpose of direct marketing unless obtaining such consent is impracticable.
- The advertiser must provide a simple means by which the individual may opt out.
- In each direct marketing communication, the advertiser must include a prominent statement that the individual may opt out or otherwise draw their attention to that fact.
- The individual must not have made such a request..

Sensitive information must not be used or disclosed for the purpose of direct marketing unless the individual has consented.

To comply with APP 6, the use of the data by the advertiser to build a profile of the user must be consented to by the individual or, alternatively, reasonably expected by the individual and related to the primary purpose for which it was collected. The advertiser will also need to comply with APP 3 and APP 5 in relation to the collection of any inferred personal information, meaning further information inferred about the user from the collected data, as part of build-

ing a profile of the user. Both the publisher and the advertiser will also have obligations under APP 11 to keep the information they hold about the user secure. This, once again, assumes that the user is identified or reasonably identifiable.

Scenario 2 (User outside Australia): A logged-on/signed-in user, known by the publisher to be an Australian resident, goes onto an Australian domain but the user's IP address or geo identifier indicates the user is outside Australia. An Australian advertiser serves an ad and uses the user data to build a user profile.

The same answer as Scenario 1 applies on the basis that all relevant collections, uses, and disclosures take place in Australia.

- **Q1**: Does the answer change if this is a signed-out user with no way of knowing where they are domiciled?

Scenario 3 (Publisher domain outside Australia): A user residing in Australia (determined by IP address or geo identifier) goes onto a domain outside of Australia. An Australian advertiser serves an ad and uses the user data to build a user profile.

With respect to the advertiser, the same answer as Scenario 1 applies on the basis that all relevant collections, uses and disclosures by them take place in Australia.

With respect to the overseas publisher, the Privacy Act will only apply to them in this scenario if they have an Australian link, in that they:

- Carry on business in Australia or an external territory; and
- Collected or held personal information in Australia or an external territory, either before or at the time of the act or practice.

With respect to the first criteria, based on the decision in Active Super mentioned above, it is likely that the publisher in this scenario carries on business in Australia by virtue of its sale of advertising to an Australian company. With respect to the second criteria, assuming that a first party cookie is used then, based on the decision in Facebook No 2 mentioned above, it is at least arguable that the publisher collects and stores personal information in Australia, through its installation and operation of cookies.

- **Q1**: Does the answer change if the site hosts content aimed at Australian residents (e.g., a news aggregator with a section on Australian current affairs)?

  No.

- **Q2**: Does the answer change if the advertiser is based outside of Australia?

  Yes.

With respect to the advertiser, if they are based outside Australia, then the same considerations apply to them as set out below in relation to Scenario 4. If the publisher and advertiser are both outside Australia, then consideration needs to be given to whether either of them "carry on business" in Australia and collect or hold personal information in Australia. If not, then they will not be subject to the extraterritorial operation of the Australian Privacy Act.

Scenario 4 (Advertiser outside Australia): A user residing in Australia (determined by IP address or geo identifier) goes onto an Australian domain and is served an ad by an advertiser based outside Australia. The advertiser uses the user data to build a user profile.

The same answer as Scenario 1 applies to the publisher on the basis that all the relevant collections, uses, and disclosures by them take place in Australia.

However, because the advertiser is based outside Australia, the publisher will also have additional obligations under APP 8, which governs the cross-border disclosure of personal information. To the extent that the individual is identified, or reasonably identifiable, APP 8 will typically require the publisher to take reasonable steps by way of contract to ensure that the overseas advertiser does not breach the APPs in relation to the personal information disclosed.

With respect to the overseas advertiser, the Privacy Act will only apply to them in this scenario if they have an Australian link, in that they:

- Carry on business in Australia or an external territory.
- Collected or held personal information in Australia or an external territory, either before or at the time of the act or practice.

For the reasons noted in *ActiveSuper*, it is likely the advertiser in this scenario carries on business in Australia by virtue of its having served advertising to an Australian consumer. However, unless the advertiser has collected or held personal information in Australia before or at the time of the relevant collections, uses, and disclosures, the Privacy Act will not apply to it. If a third-party cookie was set by the advertiser then, based on the decision in Facebook No 2 mentioned above, it is at least arguable that the advertiser collects and stores personal information in Australia, through its installation and operation of cookies.

- **Q**: Does the answer change if the advertiser has an affiliate/ group company based in Australia?

  No.

3. DEFINITIONS

3.1. Collect

An APP entity collects personal information only if the entity collects the personal information for inclusion in a record or generally available publication. The term "record" is defined as including a document or an electronic or other device.

The APP Guidelines provide that:

> *The concept of 'collection' applies broadly, and includes gathering, acquiring or obtaining personal information from any source and by any means, including from:*
>
> - *Individuals*
> - *Other entities*
> - *Generally available publications*
> - *Surveillance cameras, where an individual is identifiable or reasonably identifiable*
> - *Information associated with web browsing, such as personal information collected by cookies*
> - *Biometric information, such as voice or facial recognition*[4]

- **When a publisher allows an ad tech company's pixel on its page, who is deemed to "collect" personal information and incur legal obligations (e.g., controller/co-controller obligations under GDPR or "business" obligations under CCPA)—the publisher, the ad tech company or both?**

While not settled by a court or confirmed by the regulator, when a publisher allows an ad tech company pixel on its page, the ad tech company is likely to be considered the entity that collects personal information and incurs legal obligations under the Privacy Act (assuming the information is about an identified individual or an individual who is reasonably identifiable). That is because it is the ad tech company, via its pixel, that collects information about user activity and includes that information in an electronic or other device.

While this collection is enabled by the publisher, the publisher does not collect information about users in this scenario unless, of course, the ad tech company shares the information with them (in which case the publisher would also have to comply with the Privacy Act with respect to that information). In practice, ad tech companies will often pass the obligation to notify users and obtain necessary consents on to the publisher as part of the terms

[4] APP Guidelines, [B.27].

of use for their product or service.

3.2. Data Processing (i.e., collecting, capturing, retaining, recording, organizing, structuring, storing, altering, retrieving, consulting, using, disclosing, transmitting, disseminating, making available, aligning, combining, restricting, erasing, destroying, or otherwise processing)

The Privacy Act adopts collection, use, and disclosure as the key terminology pertaining to the handling of personal information. There is also a concept of holding personal information. The Privacy Act does not refer to "data processing."

3.3. Personal Information

"Personal information" is defined under the Privacy Act as information or an opinion about an identified individual or an individual who is reasonably identifiable:

- Whether the information is true or not.
- Whether the information or opinion is recorded in a material form or not.

Type of Information Collected	Does this Category Independently Constitute Personal Information? (Yes/No)	Qualifying Notes (if any)
IP Address	No.	There is considerable legal uncertainty on the issue of whether technical data collected in relation to individuals is within the scope of the definition of personal information. As a consequence, the ACCC has proposed that the definition of personal information in the Privacy Act be updated to clarify that it captures "technical data such as IP addresses, device identifiers, location data, and any other online identifiers that may be used to identify an individual." Until such reform, there remains doubt as to whether pseudonymous digital identifiers are considered personal information, particularly on their own.
Mobile Advertising IDs (IDFA, AAID)	No.	As above.
Consumer identifiers such as: • User device ID • Publisher persistent ID/Cross-publisher cookie ID • Household ID	No.	As above.

Hashed identifiers such as: • Hashed email • Hashed IP address	No.	As above.
User Agent such as: • Character string identifying the application • Operating system • Browser information, vendor, and/or version of the requesting user agent	No.	Assuming that this information is not sufficient to identify an individual, it will not independently constitute personal information.
Device Information such as: • Type, version, system settings, etc.	No.	As above.
Website Information such as: • Name • URL, etc.	No.	As above.
Advertisement Information such as: • Placement • Title • Creative ID, etc.	No.	As above.
Timestamps	No.	As above.
Metrics such as: • Counts • Amounts of time	No.	As above.

Event Data such as: (e.g., full URL including query string, referral URL)	No.	As above.
Precise geolocation (latitude, longitude)	No.	As above.
General geolocation (city, state, country)	No.	As above.

- **Are pseudonymous digital identifiers by *themselves* personal information (e.g., IDFA, cookie IDs, proprietary IDs, IP addresses, etc)? Please provide context to the above chart.**

  Pseudonymous digital identifiers will only be considered personal information for the purposes of the Privacy Act if the individuals to whom they relate are identified, or reasonably identifiable, to a publisher or an advertiser.

  Guidance from the OAIC in relation to when information will be about an "identified" individual is:

  > *Generally speaking, an individual is 'identified' when, within a group of persons, he or she is "distinguished" from all other members of a group. For the purposes of the Privacy Act, this will be achieved through establishing a link between information and a particular person.*
  >
  > *This may not necessarily involve identifying the individual by name. Even if a name is not present other information, such as a photograph or a detailed description, may also identify an individual. The key factor to consider is whether the information can be linked back to the specific person that it relates to.*[5]

  Guidance from OAIC in relation to when an individual is "reasonably identifiable" is:

  > *This answer to this question will depend on the relevant context the information is being handled in. Certain information may be unique to a particular individual, and therefore may (in and of itself) establish a link to the particular person. However, for an individual to be "identifiable," they do not*

[5] https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information/.

necessarily need to be identified from the specific information being handled. An individual can be "identifiable" where the information is able to be linked with other information that could ultimately identify the individual.

The inclusion of the term "reasonably" in the definition of personal information means that where it is possible to identify an individual from available information, the next consideration is whether the process of identification is reasonable to achieve. This is determined by asking whether, objectively speaking, it is reasonable to expect that the subject of the information could be identified. Even though it may be technically possible to identify an individual from information, if doing so is so impractical that there is almost no likelihood of it occurring, the information would not generally be regarded as "personal information."

Determining whether a person is "reasonably" identifiable will require a contextual consideration of the particular circumstances, including:

a. *The nature and amount of information*
b. *Who will hold and have access to the information.*
c. *The other information that is available, and the practicability of using that information to identify an individual.*[6]

To be considered personal information, the pseudonymous digital identifier must also be considered information "about" a person, meaning that the individual is the subject matter of the information. It was for this reason that, in Telstra, the Federal Court of Australia upheld a decision by the Administrative Appeals Tribunal that information relating to the IP address allocated to a mobile device which an individual used was not personal information.

In its report in relation to the *Digital Platforms Inquiry*, the Australian Competition and Consumer Commission (**ACCC**) acknowledged that there was "considerable legal uncertainty on the issue of whether technical data collected in relation to individuals is within the scope of the definition of personal information." As a consequence, ACCC has proposed that the definition of personal information in the Privacy Act be updated to clarify that it captures "technical data such as IP addresses, device identifiers, location data, and any other online identifiers that may be used to identify an individual."

Until such reform, there remains doubt as to whether pseudonymous digital identifiers are considered personal information, particularly on their own.

[6] https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information/.

- **If the answer to the above question is "no," if a Company possesses a persistent digital identifier in Database 1 and has that same identifier in Database 2 with directly identifying information, does that render the pseudonymous information in Database 1 as personal information?**

  The possession by the company of directly identifying information in Database 2 is likely to render the persistent digital identifier in Database 1 personal information provided that the persistent digital identifier is considered information "about" a person (see commentary on the effect of *Telstra* above). Even if the persistent digital identifier is not considered to be information about a person, information linked to that persistent digital identifier (such as information about the activity of that user on the website of a publisher) is likely to be rendered personal information by the directly identifying information in Database 2.

- **Is a Company's possession of a pseudonymous identifier plus other non-directly identifying data (e.g., age, gender, precise or imprecise geolocation, user agent string, timestamps) considered "personal information"?**

  Only if the individual to whom the pseudonymous identifier relates is identified or reasonably identifiable by reference to the combined data.

- **Is a Company's possession of a pseudonymous identifier "personal information" if it can hire a service provider or otherwise engage in a transaction with a third party where the identifier *could* be matched to the person *but* the Company chooses *not* to hire such service provider or undertake such transaction? Is the mere fact that this service is *potentially* available to match to the person sufficient to render that pseudonymous identifier as "personal information"?**

  Guidance from OAIC relevantly includes the following:

  > *Where it is technically possible to identify an individual by referencing it against other available information, entities should also consider the likelihood that this would occur. The time (and in some cases, the cost) that would be involved in identifying the person, and the resources and operational capacity of the entity that holds the information, all contribute to the likelihood that identification would occur. For example, an individual is more likely to be reasonably identifiable from information held by an entity when the entity's staff have access to, or can easily obtain, other information about the individual. By contrast, where the process of identifying the individual is so impractical that there is almost no likelihood of it occurring, the available information would not generally be regarded as 'reasonably' identifying the individual.*

  The mere availability of services that match pseudonymous digital identifiers with specific individuals should not render those pseudonymous digital identifiers personal information in circumstances where an entity does not use such services. However, this question has not been tested in Australia and, based on the guidance above, OAIC could well reach a different view.

Another important consideration would be the process by which these services "match" pseudonymous digital identifiers with specific individuals. Pseudonymous digital identifiers may often be associated with multiple individuals within the same household, something which may make such matching difficult to achieve with any degree of certainty. There is also some doubt as to whether pseudonymous digital identifiers are information "about" a person, as explained above.

- **What level of geolocation is personal information (precise vs. approximate)? Does it need to be associated with an identifier to be considered PI?**

  Whether or not geolocation data is considered personal information for the purposes of the Privacy Act does not depend on its level of precision. Rather, the question is whether the geolocation data is information about an identified individual, or an individual who is reasonably identifiable. If a member of the digital advertising ecosystem holds geolocation data, together with other identifying information about an individual such as their name, then the geolocation data is likely to be considered personal information.

  The use of tracking devices to obtain geolocation information is subject to separate regulation under State surveillance laws in New South Wales, Victoria, Western Australia, South Australia, and the Northern Territory.

- **Is a household identifier personal information?**

  Household identifiers will only be considered personal information for the purposes of the Privacy Act if the individuals to whom they relate are identified, or reasonably identifiable. If a publisher or an advertiser holds a household identifier alongside information identifying the members of that household, the household identifier is likely to be considered personal information.

- **Is a hashed identifier personal information?**

  Hashed identifiers will only be considered personal information for the purposes of the Privacy Act where the individuals to whom they relate are identified, or reasonably identifiable. If a member of the digital advertising ecosystem holds a hashed email address, together with an email address that includes the name of that individual, then the hashed email address is likely to be considered personal information.

- **Is probabilistic information considered personal information?**

  Probabilistic information will only be considered personal information for the purposes of the Privacy Act where the individuals to whom it relates are identified, or reasonably identifiable, to member of the digital advertising ecosystem.

3.4. Sensitive Data

"Sensitive information" is defined under the Privacy Act as:

- Information or an opinion about an individual's:
    - Racial or ethnic origin;
    - Political opinions;
    - Membership of a political association;
    - Religious beliefs or affiliations;
    - Philosophical beliefs;
    - Membership of a professional or trade association;
    - Membership of a trade union;
    - Sexual orientation or practices; or
    - Criminal record;
- Health information about an individual;
- Genetic information about an individual that is not otherwise health information;
- Biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
- Biometric templates.

3.5. Pseudonymous Information

- **Is pseudonymous information considered personal information?**

  Pseudonymous information is not defined under the Privacy Act.

  However, APP 2 requires that, subject to certain exceptions, individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity. The APP Guidelines, in the chapter relating to APP 2, define a pseudonym as "a name, term or descriptor that is different to an individual's actual name."[7]

[7] APP Guidelines, at [2.6].

The use of a pseudonym does not necessarily mean that an individual cannot be identified. If a publisher or an advertiser holds pseudonymous information, together with other identifying information such as the name of the individual, the pseudonymous information may be personal information.

- **Are persistent digital identifiers pseudonymous information (e.g., IDFA, cookie IDs, proprietary IDs, IP addresses, etc.)?**

  Pseudonymous information is not defined under the Privacy Act. However, persistent digital identifiers may be considered pseudonyms for the purpose of APP 2 in the sense that they are descriptors that are different to an individual's actual name.

- **Does the law subject pseudonymous information to fewer obligations than "regular" personal information?**

  Yes. Unless the individual to whom pseudonymous information relates is identified, or reasonably identifiable, the pseudonymous information will not be subject to any of the obligations under the Privacy Act that apply to personal information. However, if the individual to whom the pseudonymous information relates is identified, or reasonably identifiable, it will be subject to the obligations under the Privacy Act that apply to personal information. As mentioned above, there is considerable legal uncertainty in Australia on the issue of whether technical data collected in relation to individuals is within the scope of the definition of personal information. There has also been a proposal that the definition of personal information in the Privacy Act be updated to clarify that it captures "technical data such as IP addresses, device identifiers, location data, and any other online identifiers that may be used to identify an individual."

  Until such reform, if an ad tech company collects information about a user by reference to a persistent digital identifier such as a device identifier or a cookie identifier, we consider it arguable that this information is not personal information on the basis that the individual to whom it relates is not reasonably identifiable. However, if the ad tech company possesses other information that identifies the individual, such as their email address, this is likely to render the information collected about the user personal information. If the information collected about the user is disclosed to other members of the ad tech ecosystem, whether or not the information will need to be treated as personal information by each of those companies will depend on whether the user is reasonably identifiable to them based on the other information they possess.

3.6. Anonymized/De-identified Information

- **Is there a difference between anonymized or de-identified data?**

  Yes.

  The Privacy Act uses the term "de-identified" and provides that personal information is de-identified if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.

In other words, information will be de-identified where the risk of re-identification is very low having regard to the relevant data access environment. De-identified information is not "personal information" and, as a result, is not subject to any obligations under the Privacy Act.

This is different from the concept of "anonymization" present in the privacy laws of certain other jurisdictions, which requires the irreversible treatment of information such that no individual is capable of being identified, including by the holders of the information.

- **What common data categories are passed between publishers, advertisers, and ad tech companies that fall into this category when no persistent identifier is present (e.g., browser type, device type, operating system, app name, publisher site)?**

  If no persistent identifier is present, none of the data categories referred to above would be considered personal information or pseudonymous information.

3.7. Data Controller

The Privacy Act does not distinguish between "data controllers" and "data processors" and does not use these terms.

3.8. Joint Controller/Co-Controller

The Privacy Act does not include a concept of "joint controllers" or "co-controllers" and does not use these terms.

3.9. Data Processor/Service Provider (i.e., an entity that is qualified as a processor or service provider under the law because it meets certain requirements and processes data pursuant to a permissible purpose on behalf of a controller/business)

As above, the Privacy Act does not distinguish between "data controllers" and "data processors" or "service providers" and does not use these terms.

3.10. Third Party (i.e., a third party that receives data from a business for non-business purposes and does not necessarily have specific requirements under the law as to such data, such as a third-party under the CCPA)

The Privacy Act does not distinguish between "service providers" and "third parties" and does not use these terms.

4. DATA CONTROLLER RIGHTS AND RESPONSIBILITIES

4.1. Overview

The Privacy Act, and specifically APPs, impose various obligations on APP entities in relation to their handling of personal information. This includes requirements in relation to the collection, use and disclosure of personal information, as well as specific requirements in relation to direct marketing, which are of particular relevance to the digital advertising ecosystem.

Proposed amendments announced by the Australian Government in March 2019, if implemented, would also require online platforms to stop using or disclosing personal information of individuals upon request, and impose specific rules to protect the personal information of children and other vulnerable groups.[8]

4.2. Accountability

4.2.1. Overview

APP entities are accountable for their handling of personal information under the Privacy Act, as well as the acts and practices of their employees. Under s 16C of the Privacy Act, subject to limited exceptions, APP entities who have disclosed personal information to an overseas recipient are also held accountable for the handling of such information by that overseas recipient. APP entities who engage in serious or repeated interferences with privacy face fines of up to $2.1 million.

4.2.2. Application to Digital Advertising

Members of the digital advertising ecosystem subject to APPs will therefore be held accountable for their handling of personal information under the Privacy Act, as well as the acts and practices of their employees. They will also be held accountable, and liable under s 16C, for the handling of personal information by any overseas recipients they disclose personal information to, unless an exception applies.

4.3. Notice

4.3.1. Overview

APP 5 requires entities collecting personal information to take reasonable steps to notify individuals of certain matters, or otherwise ensure that they are made aware of them, including:

- The entity's identity and contact details;

[8] https://webarchive.nla.gov.au/awa/20190808004414/https://www.attorneygeneral.gov.au/Media/Pages/Tougher-penalties-to-keep-australians-safe-online-19.aspx.

- The fact that the entity collects the information;
- Whether the collection is required or authorised by or under an Australian law or a court or tribunal order;
- The purposes for which the entity collects the information;
- The main consequences for the individual if some or all of the information is not collected;
- The entities, or types of entities, information of this kind is usually disclosed to;
- That the entity's privacy policy contains information about how individuals may access their information, seek a correction or make a complaint; and
- Whether the entity is likely to disclose the information to overseas recipients and, if so, the countries in which they are likely to be located.

The APP Guidelines provide that, if an entity collects personal information from another entity, ensuring that the other entity has notified or made the individual aware of the relevant APP 5 matters on its behalf (such as through an enforceable contractual arrangement) may constitute reasonable steps.[9]

In the context of digital advertising, while information will often be collected by a range of companies that are invisible to the user, such as SSPs and DSPs, it may be that the publisher provides the relevant APP 5 notice on behalf of those entities. However, the notice requirements in APP 5 will only apply in a digital advertising context if the information collected is about identified individuals or individuals who are reasonably identifiable.

- **Who must receive notice? When must notice be provided?**

APP entities must notify individuals about whom they collect personal information of the matters referred to above at or before the time, or as soon as practicable after, the information is collected.

In the context of digital advertising, given the legal uncertainty in Australia in relation to whether online identifiers are personal information, some publishers may take the view that an APP 5 notice is not required in the case of anonymous users of their website. Those publishers may instead only provide an APP 5 notice when users identify themselves by creating an account on their website, which frequently involves providing their name and email address. Publishers adopting a more cautious approach, and treating online identifiers as personal information, may provide an APP 5 notice to all users by way of a cookie banner that displays the first time a user visits their website.

[9] APP Guidelines, at [5.7].

- **Is there specific notice required for sensitive information?**

  No. However, what constitutes reasonable steps for the purpose of APP 5, will depend on the circumstances of the collection, including the sensitivity of the information collected. This means that, when sensitive information is being collected, more rigorous steps may be required than when collecting other types of personal information.

- **Are there any specific requirements for providing notice related to processing children's personal information?**

  The Privacy Act does not impose any specific notice requirements when collecting the personal information of children. However, the effect of the APP Guidelines is that, if it is not practicable to determine capacity on a case-by-case basis, entities are to presume that individuals under the age of 15 do not have capacity to make their own privacy decisions.[10]

- **Are there any requirements compelling vendors directly collecting personal information or those receiving it from others personal information to provide additional notices? Who is responsible for those notices? Publishers? The vendors?**

  In the context of digital advertising, where the information collected is considered personal information, each company that collects it will have an obligation to take reasonable steps to notify individuals of the relevant APP 5 matters. However, it is common practice for the publisher to provide such notices on behalf of the other members of the ad tech ecosystem, given that the publisher is the one with the relationship with the user. The other entities will typically ensure that any required notices are provided by the publisher by entering into an enforceable contractual arrangement with the publisher that passes this obligation onto them.

4.3.2. Application to Digital Advertising

- **Do third parties need to be named? For example, if a publisher gives privacy policy notice that it may share personal information with third parties for advertising purposes, does it have to specify which third parties? Do specific digital advertising activities or purposes need to be disclosed as well (e.g., TCF purposes)?**

[10] Ibid, at [B.58].

The APP Guidelines relevantly state:

> *If the personal information is usually disclosed to a particular APP entity (including a related body corporate), body or person, it should be named, unless it would be impracticable to include a long list of APP entities, bodies or persons. In that case, the "type" of APP entity, body or person should be described, for example, as "health insurers" or "State Government motor vehicle licensing authorities' or 'related bodies corporate."*[11]

In the digital advertising context then, if it would be impracticable to list all the entities that the collected information is usually disclosed to, it will likely be sufficient to list the types of entities, for example "third party advertisers," for the purposes of APP 5.

Neither APPs or APP Guidelines include an express requirement for privacy notices to distinguish between different types of digital advertising activities or purposes. Market practice also varies considerably with some players bundling together different activities under broad purposes like "targeted marketing" while others explain in a higher level of detail the different types of activities involved in digital advertising. The latter approach is more consistent with the objects of the Privacy Act, which include "to promote responsible and transparent handling of personal information by entities," as well as the guidance referred to below in relation to consent.

- **Are there specific requirements related to providing notice of data collection for digital advertising purposes?**

  Yes. Digital advertising is, as explained below, considered "direct marketing" for the purposes of APP 7.

  Private sector organisations are prohibited under APP 7 from using or disclosing personal information for the purpose of direct marketing unless an exception applies.

  One such exception, pursuant to APP 7.2, is where:

  - The organization collects the information from the individual.
  - The individual reasonably expects the organization to use or disclose the information collected for the purpose of direct marketing.
  - The organization provides a simple means by which the individual may opt out.
  - The individual has not made such a request.

[11] Ibid, at [5.25].

Accordingly, where an organization wishes to use or disclose personal information collected from an individual for the purpose of digital advertising, this should be included in the notice given.

Another such exception, pursuant to APP 7.3, is where:

- The organization collected the information from:
    - The individual and the individual would not reasonably expect the organization to use or disclose the information for that purpose.
    - someone other than the individual.
- Either:
    - The individual has consented to the use or disclosure of the information for that purpose; or
    - It is impracticable to obtain that consent.
- The organization provides a simple means by which the individual may easily request not to receive direct marketing communications from the organization.
- In each direct marketing communication with the individual:
    - The organization includes a prominent statement that the individual may make such a request.
    - The organization otherwise draws the individual's attention to the fact that the individual may make such a request.
- The individual has not made such a request.

Accordingly, where a private sector organization wishes to use or disclose personal information collected from someone other than an individual for the purpose of digital advertising, or in circumstances where this would not be reasonably expected, each digital advertisement must include a notice of the kind specified above. See, for example, the digital advertisements displayed on Facebook, each of which include a simple means by which an individual may easily request not to receive digital advertisements from that advertiser by choosing to "Hide all ads from this advertiser" and draws attention to the fact that the individual may make such a request via the "Why am I seeing this ad?" dropdown.

- **What is meant by "digital advertising purposes"?**

The phrase "digital advertising purposes" is not defined under the Privacy Act or the APP Guidelines.

However, "direct marketing" is defined in the APP Guidelines as follows:

> *"Direct marketing involves the use and/or disclosure of personal information to communicate directly with an individual to promote goods and services. A direct marketer may communicate with an individual through a variety of channels, including telephone, SMS, mail, email and online advertising."*[12]

There is no doubt that direct marketing includes online behavioural advertising for the purposes of APP 7, one of the examples given in the APP Guidelines being:

> *"…displaying an advertisement on a social media site that an individual is logged into, using personal information, including data collected by cookies relating to websites the individual has viewed…"*[13]

- **Does the law or guidance distinguish between (e.g.) analytics vs. direct sold campaigns vs. allowing third parties to build or enhance profiles?**

  No, neither APPs or APP Guidelines include an express requirement for privacy notices to distinguish between these types of activities. Market practice also varies considerably with some players bundling together different activities under broad purposes like "targeted marketing" while others explain in a higher level of detail the different types of activities involved in digital advertising. The latter approach is more consistent with the objects of the Privacy Act, which include "to promote responsible and transparent handling of personal information by entities," as well as the guidance referred to below in relation to consent.

4.4. Consent and Exceptions to Consent

4.4.1. Overview

- For what types of personal information or purposes of processing is consent required?
  Subject to certain exceptions, consent is required:
  - Under APP 3, for the collection of sensitive information.
  - Under APP 6, if an APP entity wishes to use or disclose personal information for a secondary purpose (does not apply to the use or disclosure of personal information by private sector organizations for the purpose of "direct marketing," including online behavioural advertising, which is governed by APP 7).

[12] Ibid at [7.9].

[13] Ibid, at [7.11].

- Under APP 7, for an organization to use or disclose personal information for the purpose of direct marketing, where:
  - The information is collected from the individual, but they would not reasonably expect the use or disclosure.
  - The information is collected from someone other than the individual.
  - The information is sensitive information about an individual.
- Under the Spam Act, before sending a commercial electronic message that has an Australian link.

- **How is valid consent manifested–express consent, opt-in, implied consent, or opt-out?**

Consent may be express or implied. APP Guidelines provide that:

> *Express consent is given explicitly, either orally or in writing. This could include a handwritten signature, an oral statement or use of an electronic medium or voice signature to signify agreement. Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the APP entity.*[14]

APP Guidelines describe four key elements of consent for the purpose of APPs:

- The individual is adequately informed before giving consent.
- The individual gives consent voluntarily.
- The consent is current and specific.
- The individual has the capacity to understand and communicate their consent.[15]

APP Guidelines also state that use of an opt-out mechanism to infer consent will only be appropriate in limited circumstances, as the individual's intention in failing to opt-out may be ambiguous.[16]

One relevant circumstance where an opt out mechanism is permissible for private sector organizations, pursuant to APP 7.2, is where:

- The organization collects the information from the individual.
- The individual reasonably expects the organisation to use or disclose the information

[14] Ibid, at [B.36] to [B.37].

[15] Ibid, at [B.35].

[16] Ibid, at [B.40].

collected for the purpose of direct marketing.

- The organization provides a simple means by which the individual may opt out.
- The individual has not made such a request.

Another relevant circumstance where an opt out mechanism is permissible for private sector organizations, pursuant to APP 7.3, is where:

- The organization collected the information from:
  - The individual and the individual would not reasonably expect the organization to use or disclose the information for that purpose.
  - Someone other than the individual.
- Either:
  - The individual has consented to the use or disclosure of the information for that purpose.
  - It is impracticable to obtain that consent.
- The organization provides a simple means by which the individual may easily request not to receive direct marketing communications from the organization.
- In each direct marketing communication with the individual:
  - The organization includes a prominent statement that the individual may make such a request.
  - The organization otherwise draws the individual's attention to the fact that the individual may make such a request.
- The individual has not made such a request.

- **Is specific notice required as part of the consent?**

  No. The same APP 5 notice requirements detailed above apply to the collection of personal information whether or not consent is required.

- **Does the consent obligation require granularity (i.e., consent for distinct processing activities) similar to GDPR? Or is the consent obligation more generalized (e.g., requiring consumers to opt-in to "online behavioural advertising" more broadly, without having to consent to each constituent processing activity/party)?**

  The consent obligation is often treated as more generalized by organizations carrying on business in Australia. However, APP Guidelines do warn against bundled consent as having the potential to

undermine the voluntary nature of consent.[17]

This position was affirmed by the recent decision *Flight Centre*, in which the Australian Information Commissioner held that any purported consent to Flight Centre's Privacy Policy was not voluntary because the policy:

> *"…'bundled' together information about a wide range of possible collections, uses and disclosures of personal information, without giving customers the opportunity to choose which collections, uses and disclosures they agreed to, and which they did not."*[18]

- This decision, together with the OAIC guidance referred to above, indicates that a more granular consent of the kind contemplated by the TCF is required in Australia, even though current market practice does not always reflect this.

- **Is consent different for different uses or types of data (e.g., sensitive data, profiling, automated decision making, etc.)? Please provide details.**

  APP Guidelines state that an APP entity should generally seek express consent from an individual before handling the individual's sensitive information, given the greater privacy impact this could have.[19] Market practice, in a digital context, is often to obtain express consent via a checkbox.

  There are no distinct consent requirements for profiling or automated decision making.

- **Can personal information be processed for secondary purposes (i.e., differing purposes from which it was collected)?**

  Yes. APP 6 permits the use or disclosure of personal information for secondary purposes if:

  - The individual has consented to the use or disclosure.
  - The individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:
    - If the information is sensitive information–directly related to the primary purpose.
    - If the information is not sensitive information–related to the primary purpose.

[17] Ibid, at [B45]-[B.46].

[18] *Flight Centre Travel Group (Privacy)* [2020] AICmr 57, at [56].

[19] APP Guidelines, at [B.41].

- The use or disclosure is required or authorised by or under an Australian law or a court or tribunal order.
- A "permitted general situation" exists in relation to the use or disclosure (see definition below).
- APP entity is an organization and a "permitted health situation" exists in relation to the use or disclosure (see definition below).
- The entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

"Permitted general situations" include:

- Lessening or preventing a serious threat to the life, health, or safety of any individual, or to public health or safety.
- Taking appropriate action in relation to suspected unlawful activity or serious misconduct.
- Locating a person reported as missing.
- Asserting a legal or equitable claim.
- Conducting an alternative dispute resolution process.
- Performing diplomatic or consular functions.
- Conducting specified Defence Force activities.

"Permitted health situations" include:

- The collection of health information to provide a health service.
- The collection of health information for certain research and other purposes.
- The use or disclosure of health information for certain research and other purposes.
- The use or disclosure of genetic information.
- The disclosure of health information for a secondary purpose to a responsible person for an individual.

However, APP 6 does not apply to the use or disclosure of personal information for the purpose of direct marketing, which likely includes online behavioural advertising, by a private sector organisation. This is instead governed by APP 7.

- **Are there any rules compelling downstream recipients/processors of personal information to provide additional notices?**

  No. In a digital advertising context where the information collected is considered personal information, each company that collects said information will have an obligation to take reasonable steps to notify individuals of the relevant APP 5 matters. However, it is common practice for the publisher to provide such notice on behalf of the other companies in the ad tech ecosystem, given that the publisher is the one who has a relationship with the user. The other entities will typically ensure that any required notices are provided by the publisher by entering into an enforceable contractual arrangement with the publisher who passes this obligation on to them.

- **Are there any issues concerning the timing of consent?**

  Yes, in that consent must be current and specific. APP Guidelines explain that this means, when an individual gives consent at a particular time and for specific circumstances, an entity cannot assume that their consent continues indefinitely.[20]

- **Are there distinct consent requirements for sensitive personal information?**

  Yes. APP 3.3 provides that an APP entity must not collect sensitive information about an individual unless, among other criteria, the individual consents to the collection of the information.
  There are exceptions to this, including if:

  - The collection of the information is required or authorised by or under an Australian law or a court or tribunal order.
  - A permitted general situation exists in relation to the collection of the information.
  - APP entity is an organization and a permitted health situation exists in relation to the collection of the information by the entity.
  - The APP entity is an enforcement body and certain other criteria apply.
  - The APP entity is a non-profit, and certain other criteria apply.

  APP 7.4 provides that sensitive information cannot be used or disclosed for the purpose of direct marketing unless the individual consents to the use or disclosure of the information for that purpose.

[20] Ibid, at [B.49].

- **Are there distinct consent requirements for profiling consumers?**

  No.

- **Are there distinct consent requirements for automated decision making?**

  No.

- **Are there any age restrictions related to consent? Are there distinct consent requirements around processing children's personal information?**

  The Privacy Act does not impose any age restrictions related to consent. However, the effect of APP Guidelines is that, if it is not practicable to determine capacity on a case-by-case basis, entities are to presume that individuals under the age of 15 do not have capacity to make their own privacy decisions.[21]

- **Can consent, however manifested, be revoked?**

  Yes. APP Guidelines provide that individuals can withdraw consent at any time and that this should be an easy and accessible process.[22]

  APP 7 also requires private sector organizations using or disclosing personal information for the purpose of direct marketing to provide them with the ability to opt out.

4.4.2. Application to Digital Advertising

Under APP 3, subject to certain exceptions, consent must be obtained by members of the digital advertising ecosystem before collecting sensitive information about an individual. This means that if, for example, an advertiser builds a profile about a user that profile must not include any "sensitive information" inferred from their online behaviour unless the individual has consented to the collection of such information.

Under APP 7, subject to certain exceptions, consent must be obtained by members of the digital advertising ecosystem before using or disclosing personal information for the purpose of direct marketing, in circumstances where:

- The information is collected from the individual, but they would not reasonably expect the use or disclosure.

[21] Ibid, at [B.58].

[22] Ibid, at [B.51].

- The information is collected from someone other than the individual.
- The information is sensitive information.

The obligation to obtain the relevant consent is frequently managed by imposing an obligation to obtain consent on the publisher by way of contract. Given the legal uncertainty in Australia in relation to whether online identifiers are considered personal information, some publishers take the view that consent is not required in the case of anonymous users of their website. Those publishers would instead only obtain consent when users identify themselves by creating an account on their website, which frequently involves providing their name and email address. Publishers who adopt a more cautious approach by treating online identifiers as personal information, would obtain consent from all users (typically by way of a cookie banner that displays the first time a user visits their website).

Under APP 6, subject to certain exceptions, consent must be obtained by members of the digital advertising ecosystem before using or disclosing personal information for a purpose other than the purpose for which it was collected. However, APP 6 does not apply to the use or disclosure of personal information for the purpose of direct marketing, which likely includes online behavioural advertising, by private sector organizations. This is instead governed by APP 7.

Under the Spam Act, subject to certain exceptions, consent must be obtained by members of the digital advertising ecosystem before sending commercial email and other commercial electronic messages that have an Australian link.

4.5. Appropriate Purposes

4.5.1. Overview

Under APP 3, organizations must not collect personal information unless the information is reasonably necessary (or, in the case of Australian Government agencies, directly related to) one or more of their functions or activities. In the case of sensitive information, subject to limited exceptions, the individual must also consent to the collection.

Under APP 6, entities are prohibited from using or disclosing personal information about an individual for purposes other than that for which the personal information was collected, unless the individual consents or another exception applies. However, APP 6 does not apply to the use or disclosure of personal information for the purpose of direct marketing, which likely includes online behavioural advertising, by private sector organizations. This is instead governed by APP 7.

APP 7 prohibits the use or disclosure of personal information for the purpose of direct marketing by private sector organizations unless an exception applies. The relevant exceptions are summarized below.

4.5.2. Application to Digital Advertising

- **Does the law or legal guidance require a specific legal basis for specific digital advertising activities? Clarify for each activity (suggest using TCF/IAB CCPA "purposes") ("profiling" must be addressed here).**

  Not for specific digital advertising activities. The effect of APP 7, which governs the use and disclosure of personal information by private sector organizations for the purpose of direct marketing, is summarized below.

- **If yes, what are the legal bases (e.g., consent, legitimate interest)? Are there any requirements related to lawful basis (need a valid legal basis to process)/fairness (scope of processing is fair)/transparency (transparent about the processing activity to the consumer and the lawful basis)?**

  Pursuant to APP 7.2, personal information (other than sensitive information) may be used or disclosed for the purpose of direct marketing (which likely includes online behavioural advertising) by private sector organizations where:

  - The organization collects the information from the individual.
  - The individual reasonably expects the organization to use or disclose the information collected for the purpose of direct marketing.
  - The organization provides a simple means by which the individual may opt out.
  - The individual has not made such a request.

  Pursuant to APP 7.3, personal information (other than sensitive information) may also be used or disclosed for the purpose of direct marketing (which likely includes online behavioural advertising) by private sector organizations where:

  - The organization collected the information from:
    - The individual and the individual would not reasonably expect the organization to use or disclose the information for that purpose.
    - Someone other than the individual.
  - Either:
    - The individual has consented to the use or disclosure of the information for that purpose.
    - It is impracticable to obtain that consent.
  - The organization provides a simple means by which the individual may easily request not to receive direct marketing communications from the organization.

- In each direct marketing communication with the individual:
  - The organization includes a prominent statement that the individual may make such a request.
  - The organization otherwise draws the individual's attention to the fact that the individual may make such a request.
- The individual has not made such a request.

Pursuant to APP 7.4, sensitive information may be used or disclosed for the purpose of direct marketing (which likely includes behavioural advertising) by private sector organizations if the individual has consented to the use or disclosure of the information for that purpose.

Finally, pursuant to APP 7.5, personal information (other than sensitive information) may be used or disclosed for the purpose of direct marketing (which likely includes behavioural advertising) by private sector organizations where:

- The organization is a contracted service provider for a Commonwealth contract (meaning a contract, to which the Commonwealth or an agency is or was a party, under which services are to be, or were to be, provided to an agency).
- The organization collected the information for the purpose of meeting (directly or indirectly) an obligation under the contract.
- The use or disclosure is necessary to meet (directly or indirectly) such an obligation.

- **Does the law address processing for secondary purposes/differing purposes from which it was collected?**

  Yes. See explanation of APP 6, which governs the use and disclosure of personal information for secondary purposes, above. In short, personal information must not be used or disclosed for purposes other than the primary purpose for which it was collected unless the individual has consented, or an exception applies. However, APP 6 does not apply to the use or disclosure of personal information for the purpose of direct marketing, which likely includes online behavioural advertising, by private sector organizations. This is instead governed by APP 7.

4.6. Safeguards

4.6.1. Overview

APP 11.1 provides that if an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:

- From misuse, interference, and loss.
- From unauthorized access, modification, or disclosure.

APP 11.2 provides that if:

- An APP entity holds personal information about an individual.
- The entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under the APPs.
- The information is not contained in a Commonwealth record.
- The entity is not required by or under an Australian law, or a court or tribunal order, to retain the information.

The entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

4.6.2. Application to Digital Advertising

Considering the above, if a member of the digital advertising ecosystem holds personal information about an individual, they must take such steps as are reasonable in the circumstances to protect the information from the matters referred to in APP 11.1. Furthermore, if a member of the digital advertising ecosystem holds personal information, and the other criteria in APP 11.2 are met, they must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified or destroyed at the appropriate time (see above). Personal information will likely no longer be needed by a member of the digital advertising ecosystem, with the result that the company must take reasonable steps to destroy the information or to ensure that the information is de-identified, if the individual opts out from receiving targeted advertising.

5. DATA SUBJECT RIGHTS/EXEMPTIONS

5.1. Overview

In most cases, the Privacy Act does not provide individuals with rights comparable to those available under the GDPR. The main exceptions to this are that individuals do have the right to request access to, or correction of, their personal information. For reasons explained below, there are also strong indications that the Australian government may introduce concepts similar to the right to erasure and the right to data portability in the near future.

5.2. Access

If an APP entity holds personal information about an individual, APP 12 requires the entity to, on request by the individual, give the individual access to the information unless certain exceptions apply.

The exceptions to access for Australian Government agencies are if the entity is required or authorized to refuse to

give the individual access by or under the *Freedom of Information Act 1982* (Cth) or another Act that provides for access to documents.

Private sector organizations are exempt from the requirement to give individuals access to their personal information to the extent that:

- The entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety.
- Giving access would have an unreasonable impact on the privacy of other individuals.
- The request for access is frivolous or vexatious.
- The information relates to existing or anticipated legal proceedings between the organization and the individual, and would not be accessible by the process of discovery in those proceedings.
- Giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations.
- Giving access would be unlawful.
- Denying access is required or authorized by or under an Australian law or a court or tribunal order.
- Both of the following apply:
    - The organization has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to its functions or activities has been, is being, or may be engaged in.
    - Giving access would be likely to prejudice the taking of appropriate action in relation to the matter.
- Giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body.
- Giving access would reveal evaluative information generated within the organization in connection with a commercially sensitive decision-making process.

5.3. Rectify

If an APP entity holds personal information about an individual, and the individual requests that the entity correct the information, APP 13 requires the entity to take such steps as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant, and not misleading.

If an APP entity corrects personal information about an individual that it has previously disclosed to another APP

entity, and the individual requests that the entity notify the other APP entity of the correction, APP 13 requires that the APP entity must also take such steps as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

5.4. Deletion/Erasure

There is no comparable right under Australian law to the right to erasure. The Federal Government is currently, as part of its review of the Privacy Act, considering whether a right to erasure should be introduced.

While there is currently no right to erasure in Australia, in the circumstances set out in Section 4.6 above, APP 11 requires entities to take such steps as are reasonable to destroy personal information they hold or to ensure that the information is de-identified.

5.5. Restriction on Processing

There is no comparable right under Australian law to the right to restrict processing under the GDPR.

5.6. Data Portability

There is no comparable right under Australian law to the right to data portability with application to the digital advertising ecosystem.

However, the *Consumer Data Right* (**CDR**) was introduced in Australia in July 2020, which allows consumers in certain sectors to direct that their data be shared with an accredited provider of their choice. The CDR has initially been introduced in the banking sector but is expected to roll out across other sectors of the Australian economy, starting with energy and telecommunications.

In its interim report in relation to the *Digital Advertising Services Inquiry*, the ACCC also announced that it is "considering measures aimed at increasing data portability and interoperability, to reduce barriers to entry and expansion and promote competition in the supply of ad tech services." With regard to data portability, the report states:

> *Data portability measures refer to tools that increase data mobility at the consumer's request, such as requiring firms with a significant data advantage to provide consumers with an easy interface in which to move or share their data from that firm to a third-party at the consumer's request. Examples of how this could work in practice include a user instructing Google and Facebook to make data on their interactions with platforms available to a publisher, or to another social network.*[23]

[23] Digital Advertising Services Inquiry Interim Report, page 80.

The CDR may be the vehicle through which such measures are introduced.

5.7. Right to Object

There is no comparable right under Australian law to the right to object under the GDPR.

However, under the Spam Act, every commercial electronic message must contain a functional unsubscribe facility and entities must honour unsubscribe requests within 5 days. To the extent that the Spam Act does not apply, APP 7 also requires organizations using or disclosing personal information for the purposes of direct marketing to provide individuals with the ability to opt out.

5.8. Right Against Automated Decision-Making

There is no comparable right under Australian law to the rights related to automated decision making under the GDPR.

5.9. Responding to Consumer Rights Requests

Requests for access to, or correction of, personal information under the Privacy Act may be made in any format.

APP Guidelines require APP entities to satisfy themselves that a request for access to personal information has been made by the individual concerned, or by another person authorised on their behalf.[24] The steps appropriate to verify identity will depend on the circumstances of the request. APP guidelines refer, in particular, to whether the individual is known to or readily identifiable by the entity, the sensitivity of the information and the possible adverse consequences for the individual of unauthorised disclosure.[25]

The timelines for dealing with requests for access to, or correction of, personal information is within 30 days in the case of Australian government agencies and within a reasonable period in the case of private sector organisations. An APP entity must give access to personal information in the manner requested by the individual if it is reasonable and practicable to do so or, if not, take reasonable steps to give access in a way that meets the needs of the entity and the individual.

If APP entities refuse to give access, or to give access in the manner requested by the individual, they must give the individual a written notice that sets out the reasons for the refusal and the mechanisms available to complain. Likewise, if entities refuse to make a correction, they must give the individual a written notice that sets out the reasons

[24] APP Guidelines, at [12.15].

[25] Ibid, at [12.17].

for the refusal and the mechanisms available to complain. If entities refuse to make a correction, individuals may also request that they associate with the information a statement that it is inaccurate, out-of-date, incomplete, irrelevant, or misleading. If such a request is made, the entity must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information.

Where an access request is refused, or not given in the manner requested, the APP Guidelines provide that the reasons for refusal should explain, where applicable:

- That the entity does not hold the personal information sought.
- The ground of refusal.
- That access cannot be given in the manner sought, and the reasons why.
- That the steps necessary to give access in a way that meets the needs of the entity and the individual are not reasonable in the circumstances.[26]

Where a correction request is refused, the APP Guidelines provide that the reasons for refusal should explain, where applicable:

- That the entity does not hold the personal information.
- That, having regard to the purposes for which it is held, the entity is satisfied that the personal information is accurate, up-to-date, complete, relevant, and not misleading.
- That the steps necessary to correct the personal information are not reasonable in the circumstances.[27]

5.10. Record Keeping Concerning Rights Requests

There is no requirement under the Privacy Act, or APP Guidelines, to keep records concerning requests for access to, or correction of, personal information.

5.11. Is Providing Consumers with These Rights Required by Law or Mere Suggestions?

Compliance with the Spam Act and APPs referred to above is required by law for the entities those laws apply to.

---

[26] Ibid, at [12.83].

[27] Ibid, at [13.55].

5.12. Application to Digital Advertising

Considering the above, if a member of the digital advertising ecosystem holds personal information for the purposes of the Privacy Act, they may be required to deal with requests for access to, or correction of, that information. The Privacy Act does not otherwise provide individuals with rights comparable to those available under the GDPR in relation to digital advertising.

However, as stated above, the Australian Government is currently, as part of its review of the Privacy Act, considering whether a right to erasure should be introduced. If introduced, this would create another type of request that members of the ad tech ecosystem may be required to deal with.

As further stated above, the Australian Government is also considering measures aimed at increasing data portability in the supply of ad tech services. According to the interim report published by the ACCC, this could allow users to instruct platforms like Google and Facebook to make data on their interactions with those platforms available to a publisher or to another social network.

6. DATA CONTROLLER AND PROCESSOR AGREEMENTS

6.1. Overview

There is no concept of "data controllers" or "data processors" under our laws and generally no requirement that such parties enter into agreements.

However, usual practice between participants in the digital advertising ecosystem who are sharing personal information is to enter into agreements that govern its handling.

6.2. Data Controller Outsourcing of Processing

"Data controllers" and "data processors," to adopt the terminology of the GDPR, are subject to the same obligations under the Privacy Act to the extent that they collect, use, or disclose personal information.

Data controllers and data processors will also each have obligations under the Privacy Act to the extent that they hold personal information. An APP entity holds personal information if it has physical possession of the personal information or, as is the case in relation to outsourcing arrangements, if the entity has the right or power to deal with the personal information.

Information may be collected, used, and disclosed by various members of the digital advertising ecosystem, including service providers, such as SSPs and DSPs, that act as intermediaries between publishers and advertisers.

To the extent that the information being handled is about an identified individual or an individual who is reasonably identifiable, each of the entities that handles it will have obligations under APPs. However, the agreements between members of the digital advertising ecosystem will often manage this issue by contractually requiring publishers to provide relevant notices and obtain relevant consents.

6.3. Data Processor Rights and Responsibilities

See Section 6.2 above.

6.4. Application to Digital Advertising

As mentioned above, it is usual practice for members of the digital advertising ecosystem who are sharing personal information to enter into agreements that govern its handling. Those agreements typically allocate responsibility for obtaining consents and giving notices as well as requiring all parties to take reasonable steps to keep the personal information secure.

Such agreements will also typically require all parties to comply with the APPs. This will be particularly important where the recipient of the personal information is located overseas, in order to ensure compliance with APP 8. In this scenario, agreements will typically also provide the disclosing party recourse against the overseas recipient in relation to its liability under s 16C of the Privacy Act, as further explained in Section 7 below.

It is also common for agreements that involve the sharing of personal information to allocate rights and responsibilities in the event of a data breach.

7. DATA TRANSFER & OUTSOURCING

7.1. Overview

APP 8.1 requires that, before an APP entity discloses personal information about an individual to an overseas recipient, the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs.

Entities that disclose personal information to overseas recipients that are not subject to APPs are, subject to certain exceptions, accountable for any acts or practices of those overseas recipients that would be a breach of APPs if they had applied (s 16C).

APP 8.1 will not apply if the entity reasonably believes that:

- The recipient of the information is subject to a law, or binding scheme, that has the effect of protecting information in a way that, overall, is at least substantially similar to the way in which

the APPs protect the information.

- There are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme.

There are other exceptions to the requirement in APP 8.1, including where:

- The individual consents to the disclosure having been informed that, if they do so, APP 8.1 will not apply.
- The disclosure is required or authorized by or under an Australian law or a court or tribunal order.
- A permitted general situation exists (see definition in Section 4 above).
- The disclosure is required or authorized by or under an international agreement relating to information sharing to which Australia is a party.
- The disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

7.2. Application to Digital Advertising

Considering the above, if one member of the digital advertising ecosystem that is an APP entity (for example, an SSP) discloses personal information to another member of the digital advertising ecosystem based overseas (for example, a DSP), APP 8.1 gives rise to a general expectation that the SSP will enter into an enforceable contractual arrangement with the DSP, which requires them to handle the personal information in accordance with the APPs.

In that scenario, even where the SSP has taken reasonable steps to ensure that the DSP complies with the APPs, it will still be held liable for the acts or practices of the DSP under Section 16C of the Privacy Act unless one of the exceptions referred to above applies or the SSP has an "Australian link" (as defined in Section 2 above).

These provisions will not apply to the cross-border disclosure of information that is not personal information for the purposes of the Privacy Act. For the information to be considered personal information it must be information about an identified individual or an individual who is reasonably identifiable (see Section 3 above).

8. AUDIT/ACCOUNTABILITY

8.1. Overview

APP entities do not have audit rights over their vendors in Australia that are dictated by law. Nor are there record keeping requirements that are dictated by law for vendors to demonstrate that they are complying with their privacy obligations.

However, audit rights clauses are commonly included in agreements between parties that are sharing personal information. These types of clauses typically contemplate, either expressly or impliedly, that vendors will keep records to demonstrate compliance.

8.2. Application to Digital Advertising

Considering the above, for the purposes of Australian law, if members of the digital advertising ecosystem wish to have audit rights in relation to vendors, this will need to be dealt with in their agreements with those vendors.

9. DATA RETENTION

9.1. Overview

APP 11 requires an APP entity, subject to limited exceptions, to take reasonable steps to destroy or de-identify personal information if it no longer needs the information for any purpose for which it may be used or disclosed under the APPs.

An APP entity may, therefore, retain personal information it holds if the information is still necessary for the purpose of direct marketing and its use or disclosure for that purpose is permitted under APP 7. An APP entity may, otherwise, retain personal information it holds if the information is still necessary for the primary purpose of collection or for a secondary purpose that is permitted under APP 6 (see Section 4 above).

The requirement to destroy or de-identify does not apply to Commonwealth records or if the entity is required by or under an Australian law, or a court or tribunal order, to retain the information.

9.2. Application to Digital Advertising

Considering the above, members of the digital advertising ecosystem subject to APPs will need to have systems in place to ensure that, once personal information is no longer needed for any lawful purpose, that information is destroyed or de-identified.

10. DATA PROTECTION AUTHORITY | REGULATORY AUTHORITY

10.1. Overview

The OAIC is the main regulator for privacy in Australia and the Privacy Act confers a range of powers on the Commissioner, from powers to work with entities to facilitate compliance, to investigative and enforcement powers.

10.2. Main Regulator for Data Protection

The OAIC is the main regulator for privacy in Australia.

10.3. Main Powers, Duties, and Responsibilities

The Privacy Act confers a range of regulatory powers on the Commissioner, including powers to:

- Develop enforceable codes or request that entities do the same.
- Monitor or conduct assessments of whether entities are maintaining and handling personal information as required by law.
- Direct entities to notify individuals about eligible data breaches.
- Investigate and conciliate privacy complaints.
- Commence investigations on their own initiative.
- Require information or documents to be produced.
- Require persons to answer questions under oath or affirmation.
- Accept enforceable undertakings and bring proceedings to enforce them.
- Make determinations and bring proceedings to enforce them.
- Report matters to the Minister in certain circumstances, such as following an investigation or assessment.
- Seek injunctions.
- Apply to the court for civil penalty orders.

10.4. Application to Digital Advertising

Members of the digital advertising ecosystem who are subject to APPs may, depending on their conduct, become subject to any of the regulatory action referred to above.

11. SANCTIONS

11.1. Overview

Significant penalties apply for serious and repeated interferences with privacy, as well as for breaches of the Spam Act, in Australia. The Australian Government has also announced plans to significantly increase the penalties applicable for serious and repeated interferences with privacy.

11.2. Liability

An APP entity that engages in a serious or repeated interference with the privacy of one or more individuals is liable

for a civil penalty under section 13G of the Privacy Act, which exposes them to a maximum penalty of $2.1 million.

The Australian Government has announced plans to increase this maximum penalty to the greater of $10 million, three times the value of any benefit obtained through the misuse of the information or 10 percent of the company's annual domestic turnover.

With respect to the Spam Act, a company that contravenes a civil penalty provision twice or more in one day is liable for up to $444,000 if the company has no prior record, and up to $2,220,000 if the company has a prior record.

11.3. Enforcement and Market Practice

Under the current framework under the Privacy Act, the Commissioner must attempt to resolve complaints by conciliation, failing which they may make binding determinations including awards of compensation.

The OAIC received 3,306 privacy complaints during the 2018-2019 financial year, 64.5 percent of which were resolved by its early resolution process. Only when the Early Resolution team is unable to resolve a privacy complaint, will the matter be investigated and/or conciliated by the OAIC.[28]

The main remedies agreed in conciliation in 2018-2019 included correction of records, access to records, apologies, compensation, changed procedures, and staff training or counselling. The majority of compensation awards were between $1000 and $5000, with nine compensation awards exceeding $10,000.[29]

The power to investigate matters on their own initiative was only exercised by the Commissioner on 15 occasions in 2018-2019 and is typically reserved for systemic issues involving incidents of significant community concern.[30]

Complainants or the Commissioner may apply to the Federal Court or the Federal Circuit Court for an order enforcing a determination made by the Commissioner. However, only three privacy determinations were made by the Commissioner in 2018-2019.[31]

As mentioned above, the Commissioner also has the power to apply to the Federal Court or the Federal Circuit Court for a civil penalty order, where an entity is alleged to have engaged in a serious or repeated interference with the

---

[28] OAIC, Annual Report 2018-2019 (Report, 12 September 2019), 12 and 57.

[29] Ibid, 161.

[30] Ibid, 65.

[31] Ibid, 60.

privacy of one or more individuals. This power had not been used prior to March 2020, when the Commissioner commenced proceedings against Facebook in relation to the Cambridge Analytica scandal.

In addition to the above, the Australian Government has announced plans to introduce new infringement notice powers and penalties of up to $63,000 for companies that fail to cooperate with efforts to resolve minor breaches.

With respect to the Spam Act, the Australian Communication and Media Authority (**ACMA**) is responsible for enforcement and may respond to breaches of the law by:

- Providing formal and informal warnings.
- Issuing infringement notices.
- Accepting enforceable undertakings.
- Applying to the Federal Court for civil penalty orders and injunctions.

11.4. Remedies

As set out above.

11.5. Private Right of Action

Currently, individuals do not have a right of action in Australia enabling them to apply directly to a court to seek compensation for an interference with their privacy. However, the Australian Government is currently considering, as part of its review of the Privacy Act, a recommendation by the ACCC that a direct right of action be introduced enabling individuals to bring actions or class actions. The introduction of a statutory tort for invasion of privacy is also being considered as part of the same review.

11.6. Digital Advertising Liability Issues

Considering the above, members of the digital advertising ecosystem that engage in serious or repeated interferences with the privacy of individuals, or that are otherwise liable for them under s 16C, currently face maximum penalties of up to $2.1 million. These maximum penalties are expected to increase to the greater of $10 million, three times the value of any benefit obtained through the misuse of the information or 10 percent of the company's annual domestic turnover. Members of the digital advertising ecosystem who breach the Spam Act twice or more in one day also face penalties of up to $444,000 if they have no prior record, and up to $2,220,000 if they have a prior record.

12. NOTIFICATION | CERTIFICATION | REGISTRATION

12.1. Overview

APP entities are not required to notify or register with OAIC or ACMA, and Australia does not currently have any privacy certification schemes in place.

12.2. Requirements and Brief Description

Australia has applied to participate in the Asia-Pacific Economic Cooperation (**APEC**) Cross-Border Privacy (**CBPR**) System, a regional certification scheme that requires businesses to demonstrate compliance with a commonly understood set of privacy standards. It is a voluntary scheme which assesses personal information handling practices of entities seeking certification, through an audit of their privacy practices and procedures undertaken by an APEC-certified Accountability Agent.

However, in order to implement the APEC CBPR System in Australia, its requirements would need to be incorporated, and an Accountability Agent would need to be appointed. The Australian Government is currently considering, as part of its Privacy Act review, whether it should implement the APEC CBPR System. As part of the same review, the Australian Government is also considering whether, in addition to implementing the APEC CBPR System, it should develop a domestic certification scheme.

12.3. Application to Digital Advertising

There are no requirements for members of the digital advertising ecosystem to notify or register with the OAIC or the ACMA and no privacy certification scheme currently that would apply to them.

13. DATA PROTECTION OFFICER

13.1. Overview

In Australia, Privacy Officers are responsible for managing privacy including handling internal and external privacy enquiries, complaints, and requests for access to and correction of personal information. Privacy Officers are typically the primary point of contact for advice on privacy matters in an agency or organization.

13.2. DPO–Compulsory Appointment (Yes/No)

The appointment of a Privacy Officer is compulsory for Australian Government agencies under the Privacy (Australian Government Agencies–Governance) APP Code 2017 (the **Agency Code**).

The appointment of a Privacy Officer is not compulsory for private sector organizations. However, the appointment

of a Privacy Officer is commonplace and is recommended by the OAIC, in its Privacy Management Framework, as good practice for APP entities generally, as part of embedding a culture of privacy.

13.3. Requirements

The Agency Code requires agencies to ensure that the following Privacy Officer functions are carried out:

- Handling internal and external privacy enquiries, privacy complaints and requests for access to and correction of personal information under the Privacy Act.
- Maintaining a record of the agency's personal information holdings.
- Assisting with the preparation of privacy impact assessments.
- Maintaining the agency's register of privacy impact assessments.
- Measuring and documenting the agency's performance against a privacy management plan at least annually.

There are no such requirements imposed on the private sector but guidance from the OAIC, in its Privacy Management Framework, suggests that Privacy Officers should, at a minimum, be responsible for handling internal and external privacy enquiries, privacy complaints, and requests for access to and correction of personal information under the Privacy Act.

13.4. Application to Digital Advertising

Considering the above, the only members of the digital advertising ecosystem that are legally required to appoint a Privacy Officer are publishers who are also Australian Government agencies for the purposes of the Privacy Act. Such publishers will also be required to ensure that the Privacy Officer functions outlined in above are carried out.

However, based on the guidance from the OAIC, members of the digital advertising ecosystem should appoint a Privacy Officer whether legally required to or not. Those Privacy Officers should, at a minimum, be responsible for handling internal and external privacy enquiries, privacy complaints and requests for access to and correction of personal information under the Privacy Act.

14. SELF-REGULATION

14.1. Overview

The Association for Data-Driven Marketing & Advertising (**ADMA**) Code of Practice is one relevant example of self-regulation in Australia.

The ADMA Code of Practice:

> *…was developed to set standards of conduct for the marketing, media and advertising industry, to minimise the risk of breaching regulatory obligations, to promote a culture of best practice, to increase confidence in doing business with ADMA Members who are bound by the provisions of the Code and to serve as a benchmark for settling disputes.*[32]

The objectives of the ADMA Code of Practice are to establish best practice standards:

- *For collection and handling of Personal Information for marketing purposes across all online and offline marketing channels.*
- *That are channel, platform and technology neutral.*
- *That apply to industry participants generally, and to Members specifically, for the purposes of self-regulation and to deter the need for further government regulatory intervention.*
- *That promote lawful, open and transparent data-driven marketing and advertising.*
- *To increase community trust and consumer confidence in the marketing, media, analytics and advertising industry generally, and with respect to ADMA Members specifically.*
- *To promote pragmatic regulatory compliance by Members and industry participants generally to minimise or eliminate any risk of non-compliance.*[33]

ADMA members are bound to follow both the ADMA Code, and any ADMA Code guidelines in force at the time, as a condition of their membership of ADMA. The ADMA Code is overseen and administered by the Code Authority, an independent body which is empowered to investigate complaints from consumers and make determinations about compliance with the ADMA Code.

Another important self-regulatory program, which is endorsed by the OAIC, is Your Online Choices, a tool which allows individuals to do a blanket opt-out of targeted advertising for organizations that have signed up.

[32] ADMA Code of Practice, page 2.

[33] Ibid, page 4.

15. PENDING PRIVACY BILLS

15.1. Overview

In response to the *Digital Platforms Inquiry*, the Australian Government committed to undertake a review of the Privacy Act with a view to ensuring that it empowers Australian consumers, protect their data, and best serve the Australian economy.

The review will examine and, if necessary, consider options for reform in relation to:

- The scope and application of the Privacy Act.
- Whether the Privacy Act effectively protects personal information and provides a practical and proportionate framework for promoting good privacy practices.
- Whether individuals should have direct rights of action to enforce privacy obligations under the Privacy Act.
- Whether a statutory tort for serious invasions of privacy should be introduced into Australian law.
- The impact of the notifiable data breach scheme and its effectiveness in meeting its objectives.
- The effectiveness of enforcement powers and mechanisms under the Privacy Act and how they interact with other Commonwealth regulatory frameworks.
- The desirability and feasibility of an independent certification scheme to monitor and demonstrate compliance with Australian privacy laws.

An Issues Paper was released by the Australian Government in October 2020, calling for submissions in response to various questions related to the above matters.

15.2. Application to Digital Advertising

Proposed reforms to the Privacy Act likely to have particular impact for members of the digital advertising ecosystem, if implemented, include proposals from the ACCC to:

- *"Update the definition of 'personal information' in the Privacy Act to clarify that it captures technical data such as IP addresses, device identifiers, location data, and any other online identifiers that may be used to identify an individual."*[34]

[34] Digital Platforms Inquiry Final Report, page 34.

- *"Require all collection of personal information to be accompanied by a notice from the APP entity collecting the personal information (whether directly from the consumer or indirectly as a third party), unless the consumer already has this information or there is an overriding legal or public interest reason."*[35]
- *"Require consent to be obtained whenever a consumer's personal information is collected, used or disclosed by an APP entity, unless the personal information is necessary for the performance of a contract to which the consumer is a party, is required under law, or is otherwise necessary for an overriding public interest reason."*[36]
- *"Require APP entities to erase the personal information of a consumer without undue delay on receiving a request for erasure from the consumer, unless the retention of information is necessary for the performance of a contract to which the consumer is a party, is required under law, or is otherwise necessary for an overriding public interest reason."*[37]
- *"Give individuals a direct right to bring actions and class actions against APP entities in court to seek compensation for an interference with their privacy under the Privacy Act."*[38]
- *"Increase the penalties for an interference with privacy under the Privacy Act to mirror the increased penalties for breaches of the Australian Consumer Law."*[39]

[35] Ibid, page 35.

[36] Ibid, page 35.

[37] Ibid, page 35.

[38] Ibid, page 35.

[39] Ibid, page 35.

iab.

Brazil

Cross-Jurisdiction Privacy Project

1. THE LAW

1.1. Overview & Key Acts, Regulations, and Directives

- **The Brazilian General Personal Data Protection Law** ("Law No. 13.709/2018" or "LGPD") entered into force on September 18th, 2020, as a result of the sanction of the Conversion Bill ("PLV") No. 34/2020 by the President of the Republic. However, the administrative sanctions set out by the LGPD will only be applicable by the Brazilian National Data Protection Authority ("ANPD"), which is responsible for supervising and editing rules on the processing of personal data, on August 1, 2021 (Law No. 14.010/2020).
- Notwithstanding, even though the ANPD has only recently been established and the administrative sanctions are not yet enforceable, other bodies such as the Federal Prosecutors Office of the Federal District and Territories (MPDFT), the consumer protection bodies (PROCON), and the National Consumer Secretariat (SENACON) are already enforcing data protection and privacy principles in Brazil.

The purpose of this regulation is to boost economic and technological development in Brazil, providing greater legal certainty to operations involving the processing of personal data, and harmonizing other sectoral laws and statutes in Brazil that also address privacy and data protection rights. While the LGPD was heavily inspired by the General Data Protection Regulation (the "GDPR"), the Brazilian legislation presents several peculiarities and reflects specific issues related to the country's culture and reality.

In that sense, the LGPD differs from the GDPR regarding other privacy-related topics, such as the different legal bases for data processing[1] , the timeframe for responding to data subjects' requests, cybersecurity, direct marketing, prior consultation, retention practices, among others. Thus, it is clear that complying with the GDPR is not enough to guarantee compliance with the LGPD and vice versa.

Notwithstanding, given Brazil's importance as a digital economy, the LGPD's entry into force represented an important development for companies carrying out direct marketing activities online, while also impacting offline marketing.

1.2. Guidelines

Not applicable.

[1] The LGPD provides for the possibility of processing personal data for the purposes of credit protection, a legal basis that is not foreseen by the GDPR: *Art. 7 Processing of personal data shall only be carried out under the following circumstances: (...) X – for the protection of credit, including as provided in specific legislation*.

1.3. Case Law

The LGPD has only recently entered into force, which is the reason why there are very few rulings regarding the matter. Notwithstanding, there are several foundation cases with respect to the enforcement of the LGPD.

One recent case is the decision of the Brazilian Federal Supreme Court ("STF") on the Referendum on the Precautionary Measure ("PM") in the Direct Action of Unconstitutionality No. 6,389 from the Distrito Federal[2] , which suspended PM No. 954. The decision concerned the sharing of personal customer data of phone carriers with the Brazilian Institute of Geography and Statistics ("IBGE") for use in official statistics. By 10 votes to one, the STF plenary endorsed the preliminary injunction previously granted by Justice Rosa Weber, which forced telecom companies to grant IBGE access to the names, telephone numbers, and addresses of their individual and corporate consumers. IBGE intended to identify whether consumers made "home interviews" for job vacancies (i.e., interviews conducted remotely, not face-to-face), which would measure unemployment in the country. Considered personal data by Justice Weber, such information, if disclosed without prior authorization, could cause "irreparable damage to the privacy and therefore, constitutional rights of more than one hundred million users".

Another decision delivered by the Court of the State of Rio Grande do Norte ordered the reinstatement of a driver from a ride-sharing platform who was wrongfully excluded from the application because of an automated decision by the software. Even though the driver was well-rated by customers, the software removed him from the platform without giving him the opportunity to defend himself or even perform his right to have the decision reviewed. In that sense, the case reflects the principles established by Law no. 13.853/2019, which amended the LGPD, with regards to the possibility of reviewing an automated decision.

Additionally, one case was concerned with the conviction of a real estate development company that shared the personal data of one of its clients without their previous consent and for a different purpose than the one initially informed, which was-the purchase of a real estate. Hence, the judge ruled that the company violated not only the LGPD, but also the Federal Constitution and provisions of the Consumer Protection Code, reason why the company was deemed responsible for indemnifying the Plaintiff.

2. SCOPE OF APPLICATION

2.1. Who Do the Laws/Regulations Apply to?

The LGPD applies to any agent (individual, legal entity, or public agency) that performs data processing activities,

[2] Brasil. Superior Tribunal Federal. Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.389 Distrito Federal. Rel. Min. Rosa Weber. Data de julgamento: 24 abr. 2020. Voto Conjunto ADIs 6.389, 6.390, 6.393, 6.388 e 6.387 pelo Min. Gilmar Mendes. Available in: https://www.conjur.com.br/dl/pandemia-reforca-necessidade-protecao.pdf

a term defined in the Law as "any operation carried out with personal data," ranging from simple access to the data of employees, suppliers, and consumers to storage, transfer, classification, erasure, or any other handling of personal data (Articles 3 and 5, X, LGPD). Hence, the LGPD applies to all foreign businesses that offer services or products to Brazil or perform any processing activity in the Brazilian territory, regardless of whether such businesses have headquarters or data processing centers in Brazil.

Naturally, the LGPD is applicable to all actors involved in digital advertising (publishers, advertisers, DSP, SSP, etc.) whenever they process the personal data of people located within the Brazilian jurisdiction. Additionally, if a company is not located in Brazil but intentionally aims to collect the data of data subjects located in Brazil, the LGPD is applicable to that company's data processing activities.

On the other hand, from a legal entity perspective, the LGPD does not apply when the processing of data is carried out exclusively for journalistic, artistic, and academic purposes; public safety, national defense, or state security purposes; or investigating and prosecuting criminal offenses. The LGPD also provides for exceptions where the data processing originates outside Brazilian territory and is not subject to any further processing in Brazil, in such a manner that the data is only in transit through Brazil.

2.2. What Types of Processing Are Covered/Exempted?

Art. 5, X of the LGPD defines processing as any sort of operation carried out with personal data, such as collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, elimination, information evaluation or control, modification, communication, transfer, diffusion, or extraction.

The LGPD applies to any processing activity regardless of the means, the country in which the controller's headquarters is located, or the country in which the data is located, provided that:

- The processing activity is carried out in the Brazilian territory.
- The purpose of the processing activity is to offer or supply goods or services to individuals located in Brazil.
- The personal data has been collected in the Brazilian territory.

Personal data collected in the Brazilian territory is understood as personal data belonging to a data subject that is in the Brazilian territory at the time of the collection.

The following data processing activities are exempted from the scope of application of the LGPD:

- Processing carried out by a natural person, exclusively for private and non-economic purposes.
- Processing for journalistic and artistic purposes.
- Processing for academic purposes (but observing the rules set out by Articles 7 and 11 of the LGPD).

- Processing carried out with the exclusive purpose of public safety, national defense, state security, or investigation activities and prosecution of criminal offences.
- Processing activities of personal data originating outside of Brazil, from countries that provide an adequate level of data protection to the LGPD, are not subject to the LGPD, so long as this personal data is not shared or communicated with Brazilian processing agents.

2.3. Special Laws

With regard to Privacy and Data Protection in Brazil, the following Laws also apply:

Brazilian Federal Constitution of 1988	Establishes the right to privacy as a fundamental right and determines protection of intimacy, privacy, honor, image, and confidentiality of personal information and communications. In addition, the Constitutional Amendment Bill No. 17/2019, which is currently scheduled for voting in the Chamber of Deputies Plenary, seeks to include personal data protection as a fundamental right and establishes the Union's private competence to legislate on matters regarding personal data protection.
Civil Code (Law No. 10,406/2002)	States that the private life of the natural person is inviolable, as an inherent "personality right."
Internet Act (Law No. 12,965/2014 and Decree No. 8,771/2016)	Regulates the processing of personal data collected through the internet, especially by internet and connection services providers.
Consumer Protection Code (Law No. 8,078/1990)	Regulates the privacy and data protection of consumers, ensuring that consumers have full access to their information (Article 43).
Wiretap Act (Law No. 9,296/1996)	Determines that the wiretapping of communications can only occur when authorized by a court order for purposes of criminal investigation proceedings.
Telecommunications Act (Law No. 9,472/1997)	Regulates the consumers' rights to privacy in relation to telecommunications services.

2.4. Jurisdictional Reach

LGPD has an extraterritorial application. In other words, the LGPD is also applicable to entities that are not located in Brazil, when personal data is collected from individuals located in Brazil or when the processing activity aims to offer or provide goods or services to individuals located in the Brazilian territory.

Does the data subject need to be physically located within the Brazilian jurisdiction when the data is collected and processed? Is this only the case in certain contexts (e.g., where a company is outside of the territory of the EU, in the case of the GDPR)?

Yes, the data subject needs to be physically located in Brazil when the data is collected and processed, because the scope of application of the LGPD encompasses data "collected in the national territory"[3].

Hence, the LGPD is applicable regardless of the means, the country in which the headquarter of the controller is located, or the country where the data is located, provided that, alternatively: (i) the processing activity is carried out in the Brazilian territory; (ii) the processing activity aims to offer or provide goods or services, or to process the data of individuals located in Brazil; or (iii) the personal data being processed was collected in Brazil.

2.5. Application to Digital Advertising

Hypothetical situations to test concerns/jurisdictional reach.

Scenario 1: A user residing in Brazil (determined by IP address or geo identifier) goes onto a Brazilian domain and is served an ad by a Brazilian advertiser. The advertiser uses the user data to build a user profile.

The LGPD is applicable.

Scenario 2 (User outside Brazil): A logged-on/signed-in user, known by the publisher to be a Brazilian resident, goes onto a Brazilian domain but the user's IP address or geo identifier indicates that the user is located outside of Brazil. A Brazilian advertiser serves an ad and uses the user data to build a user profile.

LGPD is applicable since the personal data is being processed by a company located in Brazil (the advertiser). According to Art. 3 of the LGPD, (I), the law is applicable when the processing activity is carried out in the Brazilian territory.

[3] Pursuant to Article 3, paragraph 1, LGPD.

- Q1: Does the answer change if this is a signed-out user, with no way of knowing where they are located?

  No, given that the data was collected and used by a company (advertiser) in Brazilian territory.

Scenario 3 (Publisher domain outside Brazil): A user located in Brazil (determined by IP address or geo identifier) visits a website hosted outside of Brazil. A Brazilian advertiser serves an ad and uses the user data to build a user profile.

LGPD is applicable since the data was collected in Brazil, which triggers LGPD's territorial scope: when the personal data being processed has been collected in the Brazilian territory (according to Article 3, §1, personal data from a data subject located in Brazil at the time of collection is considered to have been collected in Brazil).

- **Q1**: Does the answer change if the site hosts content aimed at Brazilian residents (e.g., a news aggregator with a section on Brazilian current affairs)?

  No.

- **Q2**: Does the answer change if the advertiser is based outside of Brazil?

  No.

Scenario 4 (Advertiser outside Brazil): A user residing in Brazil (determined by IP address or geo identifier) goes onto a Brazilian domain and is served an ad by an advertiser based outside Brazil. The advertiser uses the user data to build a user profile.

The LGPD is applicable since data was collected in Brazil.

- **Q1**: Does the answer change if the advertiser has an affiliate/group company based in Brazil?

  No. The application of the LGPD is triggered by the fact that the processed data was collected in the Brazilian territory.

3. KEY DEFINITIONS | BASIC CONCEPTS

3.1. Collect

- When a publisher allows an ad tech company's pixel on its page, who is responsible for "collecting" personal information and incurring legal obligations, (e.g., controller/co-controller obligations under GDPR or "business" obligations under CCPA)—the publisher, the ad tech company, or both?

  This is still a "grey" area in Brazil, but there are two different interpretations applied by the advertising industry, each with their own risk level:

Interpretation A: Considering a literal interpretation of the controller and processor definitions and even the LGPD's scope of application, it is possible to argue that the publisher is not processing any personal data (in this particular processing activity), with the implication that all legal obligations will be applied only to the ad tech's company, as the sole controller.

This understanding lies in the fact that, in this scenario, the data flow goes from the data subject directly to the ad tech's web server, and the publisher has no influence or interference in the process itself and no access to the collected data, thus pushing away the controller or processor definition.

Interpretation B: Considering a holistic interpretation and taking into consideration the fundamentals of LGPD, Interpretation A above could be questioned because it could be difficult for the data subject to exercise their data protection rights.

In this scenario, since the publisher allows data collection through its web page, it is in its power to manage the data collection and it should therefore be considered a data controller. The ad tech's company is also a data controller since it will be in charge of making all subsequent decisions about the processing activity. Many practitioners view this as the more conservative interpretation.

Bear in mind that, in this scenario, the publisher is the one deciding to use ad tech on its own site, and that decision is enough to put it into a data controller position even if it does not apply to subsequent processing by the ad tech company.

3.2. Data Processing (i.e., collecting, capturing, retaining, recording, organizing, structuring, storing, altering, retrieving, consulting, using, disclosing, transmitting, disseminating, making available, aligning, combining, restricting, erasing, destroying, or otherwise processing)

Any operation carried out with personal data, such as collection, production, reception, classification, using, accessing, reproduction, streaming, distribution, processing, storing, deletion, assessment or controlling of information, modifying, disclosing, transferring, diffusion, or extraction.

3.3. Personal Information

Information related to an identified or identifiable natural person.

Type of Information Collected	Does this Category Independently Constitute Personal Information? (Yes/No)	Qualifying Notes (if any)
IP Address	Yes	
Mobile Advertising IDs (IDFA, AAID)	No	
Consumer identifiers such as: • User device ID • Publisher persistent ID/Cross-publisher cookie ID • Household ID	No	The identifier itself, when it does not carry any information that could identify an individual (e.g., the name, a phone number, or an SSN), is not personal information.
Hashed identifiers such as: • Hashed email • Hashed IP address	No	Hashed identifiers, which are considered pseudonymous information, will only be considered personal data if the controller has the additional information that enables the identification of the data subject.
User Agent such as: • Character string identifying the application • Operating system • Browser information, vendor, and/or version of the requesting user agent	No	
Device Information such as: • Type, version, system settings, etc.	No	

Website Information such as: • Name • URL, etc.	Yes	This information will be considered personal data if it contains personal identification such as name and surname, or combined personal data (i.e., first name and place of work).
Advertisement Information such as: • Placement • Title • Creative ID, etc.	No	
Timestamps	No	
Metrics such as: • Counts • Amounts of time	No	
Event Data such as: • Full URL including query string • Referral URL	No	Query strings may contain tracking mechanisms, usernames, e-mail addresses, and other information about users. In those cases, query strings will be considered personal data.
Precise geolocation (latitude, longitude)	Yes	Provided that said data identify or potentially identifies a natural person.
General geolocation (city, state, country)	No	Unless said data identify or potentially identifies a natural person. Then, they will be considered personal data.

- **Are pseudonymous digital identifiers by *themselves* personal information (e.g., IDFA, cookie IDs, proprietary IDs, IP addresses, etc.)? Please provide context to the above chart.**

  The identifier itself, when it does not carry any information that could identify an individual (e.g., the name,

a phone number, or an SSN), is not personal information.

However, because the definition of personal data in LGPD is contextual (see example 1 below to illustrate this point), it is important to analyze the context of where this identifier is commonly used.

When, according to the context in which the identifier is commonly used, it is easy to link this identifier to the individual, then the identifier should be considered personal data (see example 2 below, to better clarify this point).

In this sense, considering that in the ad tech industry it is a regular practice to use more information aggregated with persistent identifiers aiming to identify an individual, cookie IDs, IDFA, proprietary IDs, IP addresses etc., should be considered personal data.

Example 1: The Apple Marketing ID (IDFA), initially, is not personal data for third parties (although it is from Apple's perspective), since only Apple can relate the IDFA to an individual. However, this identifier is usually shared with an advertiser when an Apple user clicks on an ad through their iPhone.

After clicking on this ad, the advertiser could use other identifiers (or collect other information from the data subject) that would allow for the identification of this specific user. Since this advertiser has information that could identify the user, it is now able to link the IDFA to an identified individual, which is now considered personal data.

Example 2: IP Address alone and per se cannot identify an individual (albeit that may change in the future depending on the roll out of IPv6), so from a strict perspective, it is not personal data. However, in Brazil, all ISPs should be able to identify the individual using an IP address (which could be disclosed, for example, with a judicial order or in a police investigation), which means that, in the Brazilian context, an IP address can easily be linked to an individual and is consequently considered personal data from LGPD's perspective.

- **If the answer to the above question is "no," if a Company possesses a persistent digital identifier in Database 1 and has that same identifier in Database 2 with directly identifying information, does that render the pseudonymous information in Database 1 as personal information?**

  From an LGPD perspective, Database 1 contains pseudonymized information and Database 2 contains personal data. However, LGPD does not differentiate personal data from pseudonymous data in regard to its obligations, which means that pseudonymous data is subject to the same obligations, principles and requirements applied to personal data. In other words, legal requirements applied to Database 2 should be applied to Database 1.

It is important to emphasize that this would not be the case if Database 1 and Database 2 were owned or controlled by two different companies and those companies did not share directly identifying information.

- **Is a Company's possession of a pseudonymous identifier plus other non-directly identifying data (e.g., age, gender, precise or imprecise geolocation, user agent string, timestamps) considered "personal information"?**

  Since pseudonymous information (as per LGPD's definition) is personal data, other data linked with this identifier is considered personal data.

- **Is a Company's possession of a pseudonymous identifier "personal information" if it can hire a service provider or otherwise engage in a transaction with a third party where the identifier *could* be matched to the person, but the Company chooses *not* to hire such service provider or undertake such transaction? Is the mere fact that this service is *potentially* available to match to the person sufficient to render that pseudonymous identifier as "personal information"?**

  No, in this case, the identifier will not be considered personal data. The mere fact that there is a service available that could identify an individual through a persistent identifier (such as IDFA) is not the determining factor for whether or not this identifier is considered to be personal data; this would only be the case if the company were to decide to use this service and "transform" the information into information related to a specific individual.

  Please, note that the definition of pseudonymous information in LGPD considers that the identifiers and the pseudonymous information are always held by the same controller.

- **What level of geolocation is personal information (precise vs. approximate)? Does it need to be associated with an identifier to be considered PI?**

  The geolocation itself and as isolated data, it is not personal data. But, if linked with more data, which could identify the individual from whom the geolocation refers to, it should be considered personal data.

  Also, as indicated above, the context of where geolocation is being used should be evaluated in order to define if this data is personal data or not.

- **Is a household identifier personal information? (Consider: If a company has a residential IP address (household level ID) and multiple unique device IDs (e.g., MAIDs for every mobile device in the house) associated with that IP address, would that affect whether the household identifier is considered personal information?)**

A HHID itself is not considered personal information, since it does not allow the identification of an individual per se.

In the context provided, the household information should be considered personal data, since IP address is personal data from a Brazilian perspective (please, see explanation on the first bullet of item 3.2. above), the aggregation of both identifiers transforms HHID in personal data.

- **Is a hashed identifier personal information? (Consider: there are commercially available services that will take batches of emails encrypted using standard hashes and return (often a high percentage) of clear emails from them. Does that affect whether they are considered personal information, if all a company has to do is pay for the commercial service?)**

  The hashed identifier could be considered the same as a persistent identifier, since it is often a unique hash linked to an individual. Considering this, since a hashed identifier does not contain personal information per se, and it is not possible to identify the individual linked to this hash, it is not considered personal data.

  Additionally, as stated below, anonymized data is defined as "data relating to a data subject who cannot be identified," considering the use of reasonable technical means available at the time of the processed thereof.

  Considering this, in the context provided, the technology used to hash these emails is clearly not "reasonable" to avoid the identification of an individual, so should be considered personal data.

- **Is probabilistic information considered personal information?**

  No, probabilistic information is not to be considered as personal data, unless it is not anonymous and may identify the data subject or is aggregated with other data that could lead to identification of the data subject.

3.4. Sensitive Data

Personal data concerning racial or ethnic origin, religious belief, political opinion, trade union or religious affiliation, philosophical or political organization membership, data concerning health or sex life, or genetic or biometric data, when related to a natural person.

3.5. Pseudonymous Information

Any information subjected to a pseudonymization process. Pseudonymization is the process by which data loses the possibility of direct or indirect association to an individual, except for the use of additional information kept separately by the controller in a controlled and safe environment.

- **Is pseudonymous information considered personal information?**

  Pseudonymous information is the data that loses the possibility to be associated, either directly or indirectly, to an individual, except by using additional information kept separately by the controller in a controlled and secure environment ; hence, at first sight, pseudonymous information shall be considered personal information, because they are related to an identifiable natural person.

  In other words, as per LGPD definition, pseudonymous information only exists in the environment of the same controller, since if the directly identifiers are held by different controllers (and not exchanged between then), these data are considered anonymized data.

  For example: the HR of a law firm shares a list of employees' names and their smartphone brand preferences with its IT team but, instead of giving the names themselves, they change this information to a unique hash. The IT team does not have the means to reverse the unique hashes to the names (and is therefore processing pseudonymous information). However, since HR has the key to link the hash with the employee's name, from a controller perspective, it is considered personal data.

  Yet, there are three possible scenarios, when assessing if pseudonymous information is, or not, personal information, depending on who the processing agent is, as follows:

  1. Data controller that has the keys to decrypt a given amount of data or the correct values to unhash a registry: the information will be considered personal data, because the controller can identify to whom the data belongs and, thus, identify the data subject.
  2. Processor that processes data on behalf of the data controller but does not have access to the keys or values to decrypt or unhash the registry: the information will not be considered personal data, because the processor is unable to associate, directly or indirectly, the information received to a natural person.
  3. Co-controller that also determines the purposes of processing but does not have the keys to decrypt a given amount of data or the correct values to unhash a registry: the information will not be considered personal data, because the controller cannot associate the information to a given natural person.

- **Does the law subject pseudonymous information to fewer obligations than "regular" personal information?**

  No. All the obligations and requirements applied to "regular" personal data also apply to pseudonymous data. Pseudonymization of personal data is only considered an internal technical mechanism to improve the security and protection of personal data.

3.6. Anonymized/De-identified Information

LGPD defines anonymized data as "data relating to a data subject who cannot be identified, considering the use of reasonable technical means available at the time of the processed thereof." Since anonymized data is not considered personal data, anonymized data does not fall within the scope of LGPD.

- **Is there a difference between anonymized or de-identified data?**

  LGPD does not have a specific definition for de-identified data, but in practice, considering the definition of anonymized data (mentioned above), it could be considered the same.

- **What common data categories are passed between publishers, advertisers, and ad tech companies that fall into this category when no persistent identifier is present (e.g., browser type, device type, operating system, app name, publisher site)?**

  Such information on its own may not be considered personal data, but when linked with information that could lead to the identification of the individual, it falls under the definition of personal data. The browser type linked to an IP address, for example, is considered personal data.

3.7. Data Controller

Natural person or legal entity, governed by public or private law, in charge of making decisions about the processing of personal data.

3.8. Joint Controller/Co-Controller

There is no specific definition or rules applied to joint controller or co-controller.

3.9. Data Processor/Service Provider (i.e., an entity that is qualified as a processor or service provider under the law because it meets certain requirements and processes data pursuant to a permissible purpose on behalf of a controller/business)

A natural person or legal entity, governed by public or private law, which processes personal data on behalf of the controller.

3.10. Third Party (i.e., a third party that receives data from a business for non-business purposes and does not necessarily have specific requirements under the law as to such data, such as a third-party under the CCPA)

There is no specific definition or rules applied to a Third Party.

3.11. Consent

free, informed, and unambiguous manifestation whereby the data subject agrees with the processing of their personal data for a given purpose.

3.12. Data Protection Officer

("DPO" or, in Portuguese, "Encarregado de Dados"): A person designated by the controller or processor to function as a communication channel between the data subjects and the National Data Protection Authority ("ANPD").

3.13. Household Level Information

There is no definition of household level information in LGPD.

3.14. International Data Transfer

A personal data transfer to a foreign country, or to an international entity of whom the country (Brazil) is a member.

3.15. Data Protection Impact Assessment

A controller's documentation which contains the description of personal data processing activities which could impose risks to civil liberties and fundamental rights, as well as the measures, safeguards, and mechanisms to mitigate those risks.

3.16. Profiling

The LGPD does not specifically define profiling and there is no precedent regarding this situation.

3.17. Automated Decision-making

There is no specific definition of automated decision-making, however, Article 20 of the LGPD states that the data subject has the right to request a review of decisions made solely based on automated processing of personal data related to their interests, including decisions intended to define their personal, professional, consumer and/or credit profile, or aspects of their personality.

4. DATA CONTROLLER RIGHTS AND RESPONSIBILITIES

Before assessing the main data controller characteristics, here are a few notes on marketing and digital advertising activities in Brazil.

4.1. Brief Notes on Marketing and Advertising in Brazil

Direct marketing is defined as the set of strategies employed to reach a targeted audience that has already shown some sort of interest in a product or service and is much more likely to convert that into a purchase, covering any

advertising or promotional material, not just commercial marketing. This is the case for advertisements carried out through online and offline means such as posts, email marketing, phone calls, SMS, messaging applications, social media, and web banners. Some online content is displayed without processing any personal data, for example, whenever the same content is displayed to everyone who visits a website, without targeting a specific audience/individual; in this case, data protection does not apply.

Unlike the GDPR, Brazilian law is silent in terms of the lawfulness of data processing for marketing and advertising purposes. Therefore, it is possible to carry out direct marketing and/or advertisement through either consent or *legitimate interests*.

If a company chooses to rely on consent for marketing and advertising purposes, they will generally obtain an individual's consent prior to sending marketing texts, emails, or making phone calls, and will also typically obtain consent in order to share customer details with another organization. Consent should be an informed, unambiguous, and a freely-given indication of the data subject's agreement to the processing of their personal data for marketing and advertising purposes.

The clearest way of obtaining consent for said purposes is to invite the customer to tick an opt-in box confirming that they wish to receive marketing communication through specific channels (post, email, phone call, SMS etc.). Opt-in, when available, is a best practice advisable to all organizations to adopt, since it provides a clear and prominent statement, apart from a general privacy policy, explaining that the positive action of "ticking the box" indicates consent to receive marketing communication from that organization, for instance.

Note that communications that are essential or legally mandatory to the provision of the goods or services per se are considered commercial communications and can be sent regardless of consent. That is the case of an e-mail sent to recover a password, or a communication reporting an error, or fraud detection. Providers need to be as clear as possible regarding which information is mandatory to the provision of the good or service and which information data subjects can choose to receive.

Therefore, one way to carry out direct marketing activities is to rely on consent and its general rules, including transparency and the data subject's rights to withdrawal their consent and to oppose further data processing from that point on.

However, some have subscribed to a more flexible interpretation of the Law on this point, based on arguments that consent requirements could significantly diminish companies' ability to advertise, communicate to the public, and launch new products on the market, and also based on the fact that advertising is an important tool for communicating with the public and has the power to escalate demand, widen competition, and even bolster innovation, playing an important role in economic development.

Therefore, it is also possible for companies to carry out marketing and advertising activities in Brazil based on legitimate interests instead of obtaining previous and express consent. The most important aspect of this scenario is respecting opt-outs, since this is when data subjects manifest their expectations in a clear manner. In other words, LGPD allows legitimate interest legal basis for marketing and advertising purposes, particularly when the processing of personal data aims to support the controller's activities or acts in the data subjects' benefit.

Bear in mind that "legitimate interest" cannot be used as a lawful basis for personal data processing sensitive personal data instead of receiving consent.

Despite the similarities between LGPD and GDPR, there is more flexibility in the Brazilian law when it comes to marketing and advertising activities. For example, there is no equivalent in LGPD to Article 21 (1) or (2) of GDPR, which allow the data subject to oppose processing based on legitimate interests or when carried out for marketing activities. There is also no equivalent in Brazil to the ePrivacy Directive, which requires consent for non-essential cookies.

Nevertheless, GDPR is influential in the Brazilian privacy landscape. European best practices are often applied in order to build understanding and arguments for some of the topics below.

That said, find, below, (i) the overview on the characteristics of the data controller as foreseen in the LGPD (item 4.2); (ii) a few notes on accountability (item 4.3); (iii) the requirements for the privacy notice (item 4.4); (iv) the specific analysis on consent and its exceptions (item 4.5); (v) the appropriate purposes (item 4.6); and (vi) the safeguards needed (item 4.7).

4.2. Overview

Responsibilities of the Data controller:

- Complying with all data subject rights.
- Complying with security incident notification obligations.
- Keeping a registry of the data processing activities.
- Implementing technical and administrative security measures to protect personal data from unauthorized access and illicit or accidental situations of destruction, loss, modification, communication, or any other form of inadequate or illicit processing.
- Developing data protection impact assessments when requested by the ANPD, or in situations where the processing activity imposes high risks to the data protection principles established in LGPD, as regulated by the ANPD.
- Appointing a DPO.

Another controller responsibility is to indicate the legal basis that authorizes the personal data processing. When it comes to digital advertising, usually, there will be two applicable bases: data subject's consent and legitimate interest. There is an opacity in the law about these two hypotheses and it will be addressed in topic 4.5.2.

How Data Controllers are Defined

Controllers and processors are defined according to how they are involved in the personal data processing activities. Controllers are the entities in charge of making decisions about the processing of personal data.

The position of controller and processor should be defined for each data processing activity, which means that a single organization could have processes where it figures as a controller and other ones where it figures as a processor.

Liabilities of the Data Controller

It is worth noting that strict liability may be imposed upon the controller and the processor in relation to data processing activities, particularly when data subjects are consumers. In other cases, there is room for different kinds of liability; for example, if the processor goes against the controller's instructions, that processor alone will be liable in most circumstances.

Hence, personal data processing agents must ensure that processing is carried out in an adequate and proportional manner, and is limited to the minimum amount necessary for the fulfilment of a specific purpose. In addition to this requirement, LGPD also establishes a number of other obligations and liabilities associated with the processing of personal data.

Beyond that, according to the approved text, in addition to complying with the law, data processing agents are responsible for taking efficient measures that are effectively capable of demonstrating compliance and fulfilment of the rules. This obligation is part of the accountability principle that should be complied with by the processing agent.

Lawfulness of Processing

LGPD requires that controllers, or processors performing a processing activity following the instructions of the controller, have an appropriate legal basis to process regular or sensitive personal data. As explained below, the legal bases under which sensitive personal data may be processed are stricter than those established for personal data.

That said, according to the LGPD, the processing of regular personal data shall only be carried out under the following circumstances:

(i) With the consent of the data subject.

(ii) For compliance with a legal or regulatory obligation by the controller.

(iii) By the public administration, for the processing and shared use of data necessary for the execution of public policies provided in laws or regulations, or based on contracts, agreements or similar instruments.

(iv) For carrying out studies by research entities, ensuring, whenever possible, the anonymization of personal data.

(v) When necessary for the performance of a contract or preliminary procedures related to a contract of which the data subject is a party, at the request of the data subject.

(vi) For the regular exercise of rights in judicial, administrative or arbitration procedures.

(vii) For the protection of life or physical safety of the data subject or a third party.

(viii) To protect the health, exclusively, in a procedure carried out by health professionals, health services or sanitary authorities.

(ix) When necessary to fulfill the legitimate interests of the controller or of a third party, except when the data subject's fundamental rights and liberties which require personal data protection prevail.

(x) For the protection of credit, including as provided in specific legislation.

Except for the other nine bases in which data processing is allowed when relying on consent, the controller must obtain freely given, informed and unambiguous consent from the data subject, either in writing or by any other means that can ensure the data subject's consent to both processing and sharing of personal data with other companies. The data subject may withdraw such consent at any time.

Also, the national authority may request a data protection impact assessment ("DPIA") from the controller when processing is based on their legitimate interest, with commercial and industrial secrecy being observed.

As mentioned, however, sensitive personal data may only be processed under the legal bases set out by Article 11 of the LGPD, which exclude protection of credit, performance of a contract (even though it is possible to process data for the exercise of rights that stem from a contract) and legitimate interest, as follows:

I – When the data subject or her/his legal representative specifically and distinctly consents, for the specific purposes.

II –Without consent from the data subject, in the situations when it is indispensable for:

a) Controller's compliance with a legal or regulatory obligation.

b) Shared processing of data when necessary by the public administration for the execution of public policies provided in laws or regulations.

c) Studies carried out by a research entity, whenever possible ensuring the anonymization of sensitive personal data.

d) The regular exercise of rights, including in a contract and in a judicial, administrative and arbitration procedure, the last in accordance with the terms of Law No. 9,307, of September 23, 1996 (the "Brazilian Arbitration Law").

e) Protecting the life or physical safety of the data subject or a third party.

f) To protect the health, exclusively, in a procedure carried out by health professionals, health services or sanitary authorities (New Wording Given by Law No. 13,853/2019).

g) Ensuring the prevention of fraud and the safety of the data subject, in processes of identification and authentication of registration in electronic systems, respecting the rights mentioned in Art. 9 of this Law and except when fundamental rights and liberties of the data subject which require protection of personal data prevail.

Thereafter, similarly to the GDPR, before the processing activity, there shall be a legal basis that supports it.

4.3. Accountability

4.3.1. Overview

Accountability is one of LGPD's founding principles, defined in Article 6 – X as "*demonstration by the agent of the adoption of measures which are efficient and capable of proving the compliance with the rules of personal data protection, including the efficacy of such measures.*"

LGPD's rules regarding accountability are those establishing the liability of processing agents, which are addressed further below.

4.3.2. Application to Digital Advertising

There are no specific accountability requirements for the digital advertising industry.

For digital advertising industries, the main accountability measures that could be used are:

- When applicable, keep a register (e.g., logs) of the consent provided, including when and how it was provided (e.g., type of language used, where the consent disclaimer was inserted, etc.)
- Manage opt-outs in a quick fashion, particularly when relying on legitimate interests.
- Account for all third parties that had access to the data of all the data subjects impacted by their activities.

- Elaboration of LIAs/DPIAs of their most critical activities (e.g., use of third-party cookies; cross-device tracking technologies, aggregation of data bought from data bureaus etc.).

4.4. Notice

4.4.1. Overview

LGPD states that the data subject needs to be able to access clear, precise, and easily-accessible information regarding the data processing activities being carried out.

- **When must notice be provided? What must be in the notice in the digital advertising context? (Consider also, what notice needs to be provided when pixels fire on a webpage?)**

It is generally better to provide notice prior to the collection of personal data, or as soon as possible. For example, when using cookies or pixel tags that load before the homepage visualization (processing personal data before the possibility to display any information to the data subject), it is recommended to present the notice as soon as the website loads.

Nevertheless, what matters most is that information about the processing activities can be easily accessed by data subjects, which means links to privacy notices and similar documents should be easy to find. In the digital advertising context, it is generally better to give succinct information at first and link to the privacy policy so that data subjects can learn more.

It is important to note that LGPD does not foresee any specific way to disclose privacy notices or disclaimers for cookies (or any other tracking technology), so the example above is aligned with the general practice of Brazilian companies.

Generally, those cookie banners have a simple text with an indication of a link where the data subject could get more information. For example: "*This website uses cookies and other similar technologies to offer customized advertising. For more information, please check our Cookie Policy [or Privacy Policy].*"

If the website does not intend to collect consent to use pixel or cookies on the data subjects' browsers, it is important that this cookie banner does not have a button saying words like "I Accept" or "I authorize," or anything else that could imply an attempt to collect consent.

- **Is there a specific notice requirement for sensitive personal data?**

  No, there are no specific notice requirements for sensitive personal data.

- **Are there any specific requirements for providing notice related to processing children's personal information?**

  Yes. In order to process the personal information of children (0 - 12 years old) and adolescents (13 - 17

years old), Article 14 §6º of the LGPD requires that controllers provide notice in a simple, clear, and accessible manner to provide the necessary information to the parents or legal representative, and the notice must appropriate for children's understanding. Data processing should be carried out with the best interest of the children and adolescents in mind. Such notice must take into consideration the data subject's physical-motor, perceptive, sensorial, intellectual, and mental capabilities, using audiovisual resources when appropriate.

Beyond that, when processing children's personal information, controllers must make available the information about the types of data collected, the way it is used and the procedures for exercising the rights of data subjects. A reference to said information in the privacy policy suffices.

- **Are there any requirements compelling vendors directly collecting personal information or those receiving it from others to provide additional notices? Who is responsible for those notices? Publishers? The vendors?**

  LGPD establishes that "the data subject has the right to facilitated access to information concerning the processing," but it does not specify who is responsible for providing the notice. Despite that, the current understanding is that the controller which is collecting data from the data subject is responsible to provide notice. This understanding is based in the following points:

  - The transparency principle, the base of notice obligations on LGPD, requires data subjects to be informed about the processing activity and the processing agents (Article 6, VI). Only data controllers have the possibility to disclose which processing agents are involved in a processing activity.
  - The Controller is responsible for making decisions regarding the processing activity, especially the why and how. The information that should be made available in the notice (such as the purpose of the processing, controller's identification and contact information, form and duration of the processing etc.) can only be known, in the first place, by the controller.
  - Article 18, which defines the rights of the data subject, foresees that all rights should be obtained from the controller, including the right to access their data and information about public and private entities with whom the controller has shared data.

  This does not mean that controllers cannot rely on processors to provide notice to the data subject, but only that the final (and opposable to third parties) responsibility cannot be delegated.

  In this case, the publisher will be responsible to inform the data subject that his/her data is being collected and shared with SSPs, DSPs, Advertisers, etc.

  Nevertheless, Article 8 §6º of the LGPD determines that, if there is any change in the data processing activity, the controller shall inform the data subject, specifically highlighting the

content of the changes. Therefore, it is reasonable to assume that the controller will always be responsible for providing notices.

4.4.2. Application to Digital Advertising

- **Do third parties need to be named? For example, if a publisher provides privacy policy notice that it may share personal information with third parties for advertising purpose, does it have to specify which third parties? Do specific digital advertising activities or purposes need to be disclosed as well (e.g., TCF purposes)?**

LGPD assigns to the controller and the processor the duty of transparency towards the data subjects, which means that they shall guarantee to the data subjects clear, precise, and easily accessible information about the carrying out of the processing and the respective processing agents, subject to commercial and industrial secrecy (Article 6, VI, LGPD).

Along the same lines, for the purposes of LGPD compliance, it would suffice for the company processing the personal data to disclose their sharing of the collected data with third parties to the data subject in the privacy policy/notice, with no need to indicate the third parties by name, in addition to the marketing purposes.

In other words, companies need to disclose in their privacy notices the categories of third parties with whom they share data, not the actual company names of said third parties.

Note that is mandatory that companies disclose the purpose of sharing, as per the provision in Article 9, V, of LGPD:

> *"Article 9. The data subject is entitled to the facilitated access to information on the processing of her/his data, which should be made available in a clear, adequate, and ostensible manner, concerning, among other characteristics provided in regulation for complying with the principle of free access:*
>
> *V–information on the shared use of data by the controller and the purpose."*

That said, let's see an example:

» A marketing company collects data from data subjects located in Brazil for the purpose of offering marketing/advertising activities. When collecting the consent from the data subjects by means of an opt-in checkbox, the company presents a clear and prominent statement, indicating that the data provided by the user will be used for marketing/advertising purposes, which implies the sharing of personal data with third parties.

In the example above, it is necessary that the notice disclose to users that their data will be shared with third parties and that they can learn more about this sharing in the privacy notice.

However, ideally, considering that the legal basis adopted in the example was consent and that such legal basis shall refer to particular purposes (as per Article 8, paragraph four, of the LGPD), the company which will process the data shall point out all the purposes intended, as far as reasonably possible (i.e., use of the data for basic or personalized ads, cookies, tracking, etc.). This means that, if "marketing purposes" include other purposes, those purposes shall be specified and informed to the data subject, what does not mean that the controller will have to collect consent for each one of the purposes.

As per the need to name all the third parties, within the presented legal context, there would be no express legal obligation to do so, apart from the indication that the personal data processed will be shared with third parties.

Notwithstanding, if the company already has a list containing all the vendors or companies to whom the data subjects' data might be shared, this could be made available in the privacy notice in order to comply with the transparency principle, although this is not mandatory.

On the other hand, if the data subject exercises their right to access such information, requiring a full report on their data pursuant to Article 19, II, of the LGPD, then the company will be legally required to present the names of the third parties with whom they share the personal data. Please note that there may be some room for not providing the full list of third parties if this amounts to a trade secret.

Lastly, it should be highlighted that a lot of publishers in Brazil identify the third parties that have placed cookies or pixels on their website. This practice does not include the identification of the third parties involved in the next steps of the chain, so if a cookie was placed on a given website by a SSP that will later share the data subject's information with a DSP, the publisher is only required to disclose regarding the SSP and not the DSP.

Usually, publishers provide a general list of cookies/trackers placed their website, indicating the name of the cookie, its purpose, and its "owner," as in the example below:

The cookies we use in our website are:

Third Party	Purpose
Specific Media	Technology used to disclose customized messages and advertising in videos, based on your interaction with our website.

- **From an industry perspective it is common to distinguish data use for ad targeting vs. profile building vs. measuring ad campaigns. Does the notice requirement require separate disclosure of those things? Or is it enough to say something general like "advertising and related purposes"?**

There is no legal requirement to specifically mention these concepts, but LGPD states that processing must be done "for legitimate, specific, and explicit purposes of which the data subject is informed," which means that purposes need to be disclosed as clearly as possible.

However, the general practice within the market is not to be very specific on advertising purposes, disclosing only that the data collected will be used for "advertising and related purposes," a practice that could be questioned by Brazilian authorities. It is important to emphasize that we do not have any case or recent enforcement action contesting this practice.

4.5. Consent and Exceptions to Consent

4.5.1. Overview

- **For what types of personal information or purposes of processing is consent required?**

Consent legal basis is applicable to any type of personal data or sensitive personal data, provided that the consent is given in writing or by other means able to demonstrate the manifestation of the will of the data subject, referring to particular purposes. Hence, the LGPD prohibits the processing of personal data if the consent is defective and, also, considers void the consent that does not refer to particular purposes.

If the consent refers to multiple purposes, the company that is processing the personal data shall point them out to the data subject, as far as reasonably possible. Nonetheless, the LGPD does not establish an obligation to collect a specific consent for each one of the specific purposes, rather, only one consent, encompassing all the purposes.

Also, note that if the consent is given in writing, it should be included in a clause that stands out from the other contractual clauses and in a way that highlights all the purposes for the processing.

On the other hand, if there is a change in (i) the specific purpose of the processing; (ii) the type and duration of the processing, being observed commercial and industrial secrecy; (iii) the identification of the controller; or (iv) the information regarding the shared use of data by the controller and the purpose, the controller shall inform the data subject, specifically highlighting the content of the changes, in which case the data subject, if their consent is required, may withdraw said consent if they disagree with the change (as per Article 8, paragraph six, of the LGPD).

In sum, if there is any change to any of the information mentioned in (i), (ii), (iii) and (iv), the controller must notify the data subject and obtain new consent. This obligation does not apply, for instance, if the controller changes its contact information.

Also, it should be highlighted that, as a rule, the processing of children's personal data must be based on the parents' consent, especially for marketing and advertising purposes. On another note, when the processing is necessary in order to contact the parents or legal guardian, is used only once and without storage, or is for the child's protection, provided that the personal data is not transferred to third parties, under any circumstance. The consent of parents or legal representatives may be waived in the best interest of the child, which will prevail in said cases.

- **How is consent manifested – express consent, implied consent, or opt-out?**

Consent must always be obtained (i) by means of demonstrating the will of the data subject; (ii) prior to the processing activity; (iii) upon free choice of the data subject; (iv) after the data subject has received clear information about the processing activity; and (v) by means of a positive act by the user indicating his acceptance, i.e., by ticking an opt-in option, with a clear and prominent statement, apart from a general privacy policy, explaining that the positive action of "ticking the box" indicates consent to receive marketing or advertising from the company.

Beyond that, when consent is given in writing (e.g., in a contract), it must be included in a clause that stands out from the other contractual clauses.

- **Is specific notice required as part of the consent?**

Yes. However, the specific notice regarding the consent is implicitly required by the LGPD, because the consent must be informed, which means that the data subject should be aware of what they are consenting to.

- **Does the consent obligation require granularity (i.e., consent for distinct processing activities) similar to GDPR? Or is the consent obligation more generalized (e.g., requiring consumers to opt-in to "online behavioral advertising" more broadly, without having to consent to each constituent processing activity/ party)? Is consent different for different uses or types of data (e.g., sensitive data, profiling, automated decision-making, etc.) Please provide details.**

No. LGPD does not set forth specific requirements regarding the granularity of an opt-in. However, consent must relate to a specific purpose and LGPD explicitly determines that "generic authorizations for processing personal data shall be considered void." Considering this, it is highly recommended to be as specific as the situation allows. Moreover, there are three situations where LGPD establishes that consent must refer to one purpose distinguished from others: when consent is given for (i) processing of sensitive personal data, (ii) processing of children's data, and (iii) international transfer of data (if consent was chosen by controller as the transfer mechanism). These situations can be compared, but are not necessarily equivalent, to the concept of granularity.

It is important to note that these concepts have yet to be enforced by authorities, and the general practice in the market is to not be very specific regarding advertising purposes, disclosing only that the consent is for "advertising purposes." However, since LGPD does foresee the requirement of specific purpose for valid consent, this practice (to be generic regarding purpose), could be questioned by authorities.

The understanding stated above is valid for profiling, automated decision-making, etc. For sensitive personal data, LGPD is even more emphatic that there should be only specific consent for sensitive data. Therefore, if a processing activity will be using sensitive personal data, it is mandatory that specific consent be obtained for this type of data. For example:

( ) I consent to the use of my personal data (name, email, phone and geolocalization) to be processed for advertising purposes. For more information, please check our Privacy Notice.

( ) I consent to the use the use of my sensitive personal data (facial biometric) to be processed for advertising purposes. For more information, please check our Privacy Notice.

- **Can personal information be processed for secondary purposes (i.e., differing purposes from which it was collected)?**

  As a rule, processing for uninformed purposes is forbidden, as per the definition of the "purpose" principle, on LGPD's Article 6.

  Moreover, LGPD's Article 8 §6º establishes that, whenever there is a change in the specific purpose of the processing, the controller is obligated to inform the data subject about said change. If the legal basis of the processing is consent, the data subject has the right to withdraw it.

  However, LGPD sets out two situations where processing for secondary purposes is allowed: processing of publicly accessible personal data (Article 7º §3º), and processing of data manifestly made public by the data subject (Article 7º §4º).

  According to Article 7º §7º:

  "*The subsequent processing of the personal data referred to in paragraphs three and four of this article may be carried out for new purposes, provided that legitimate and specific purposes to the new processing and the preservation of the rights of the data subject are observed, as well as the grounds and principles set forth in this Law.*"

- **Are there any rules compelling downstream recipients/processors of personal information to provide additional notices?**

  No, there is no obligation to provide additional notices on behalf of the recipients/processors.

- **Are there any issues concerning the timing of consent?**

  There is no express rule concerning the timing of the consent other than it shall occur before the data processing/data collection.

- **How does the timing of consent affect pixels firing when the user lands on a page?**

  Considering that pixels are usually associated with cookies, the ideal would be to notify the user regarding the platform's use of cookies as soon as they access the website, and to offer the user the option to disable them, which, consequently, would also disable pixels, a priori. Beyond that, even though the LGPD does not require companies to do so expressly, Brazilian companies have been drafting a cookie policy that would inform the data subject as to how they are, or will be, handling cookies and pixels.

- **Are the requirements foreseen in Brazil regarding the notification of the users and the use of pixels equivalent to how companies do this for GDPR today or are the requirements materially more or less specific?**

  Overall, yes. Both the GDPR and the LGPD do not specifically regulate the use of cookies (the GDPR mentions "cookies" only once, in Recital 30, and the LGPD does not mention "cookies" at all).

  Note, however, that in the EU, cookie compliance is managed pursuant to the ePrivacy Directive (EPD) which, among other provisions, determines that the processing agent must, prior to using cookies, obtain the user's consent, document and store the received consents make it easy for users to withdraw consent, etc. Brazilian legislation is silent on the matter. However, the new e-Privacy Regulation, which is currently being discussed by the EU, will build upon the EPD and expand its definitions, so it is expected that the cookie compliance in the EU will demand further efforts from companies there, unlike Brazil, where EPD compliance must suffice until the Brazilian Supervisory Authority (ANPD) decides otherwise.

- **Are there distinct consent requirements for sensitive personal information?**

  For sensitive data, in addition to complying with the general criteria (free, informed, and unambiguous), consent must also be specific and highlighted.

- **Are there distinct consent requirements for profiling consumers? Consider: if a business gets consent to use personal data for "advertising and marketing" purposes, is a separate (or more specific?) consent required to build an advertising profile for advertising?**

  LGPD does not provide specific rules regarding profiling. As mentioned in the responses above, the best practice is to be more specific regarding how the data will be processed, (Article 9, II, foresee that the form of the processing activity should be disclosed to the data subject), including, at the moment, to collect consent. However, the market practice has been to not enter on these specificities, collecting consent "for marketing purposes" without informing details regarding how this will be performed on the consent disclaimer.

- **Are there distinct consent requirements for automated decision-making?**

  No, there are no distinct consent requirements for automated decision-making in the LGPD.

- **Are there any age restrictions related to consent? Are there distinct consent requirements around processing children's personal information?**

  Yes. Children cannot give consent on their own. In order to process data related to children, it is necessary to take the child's best interest into consideration, which may clash with the consent required from parents. The ANPD will clarify this issue in the future. Under Brazilian law, individuals under 12 years old are considered children.

- **Can consent, however manifested, be revoked?**

  Yes. consent may be withdrawn at any time, through the express request of the data subject via a process that is simple and free of charge, with processing carried out under the previously-given consent remaining valid as long as there is no request for deletion. There are no additional requirements for address this data subject directly on LGPD.

4.5.2. Application to Digital Advertising

There are no specific consent requirements for the digital advertising ecosystem.

4.6. Legitimate Interest

Legitimate interest is the most flexible lawful basis for processing personal data and can be applied in a wide range of circumstances since it is not limited to a particular purpose. Article 7(IX) of the LGPD recognizes that personal data can be processed:

> "Whenever necessary to serve the legitimate interests of the controller or of third parties, except in the event of prevalence of fundamental rights and freedoms of the data subject, which require protection of the personal data."

Despite that, legitimate interest cannot be used as a legal ground for processing sensitive personal data, as opposed to consent; This because, when processing sensitive personal data, the LGPD requires the adoption of guarantees that are additional to those to be implemented for processing general personal data.

That said, in compliance with the LGPD's principles, Article 10 of the LGPD establishes the following limitations to the use of legitimate interest as a lawful basis for processing personal data:

> "The legitimate interest of the controller can only support the processing of personal data for legitimate purposes on concrete situations, which include, but are not limited to:
>
> I - Support and promotion of the controller's activities; and

II - Protection, in relation to the data subject, of the regular exercise of his rights or provision of services that benefit him, respecting his legitimate expectations and fundamental rights and freedoms, under the terms of this Law.

§1 When the processing is based on the legitimate interest of the controller, only personal data strictly necessary for the intended purpose may be processed.

§2 The controller must adopt measures to guarantee the transparency of data processing based on its legitimate interest.

§3 The national authority may request from the controller a data protection impact assessment on the protection of personal data, when the processing is based on its legitimate interest, observing commercial and industrial secrets.

Despite its conceptual broadness, the LGPD provides some guidance on the authorized use of legitimate interest by data controllers when the interests of the company in regards to processing data are based on concrete situations that either support the controller's activities or act in the data subjects' best interest, provided that (i) the processed data is kept to a minimum, (ii) the data subject is aware and fully informed of the data processing and (iii) the controller keeps a record of data processing activities that rely on legitimate interests, establishing, for each data processing activity, the interests pursued, the anticipated impacts and the mitigating measures of such impacts, including security.

In view of that, controllers may rely on legitimate interests to process consumers' personal data in order to promote their products or services, including prospecting new customers. That said, companies must still make sure that the processed personal data is kept to a minimum, that the data subject has access to information about the data processing (especially when they do not provide their data directly but are instead impacted by online third-party behavioral advertising, for example), that the data is only used pursuant to the purpose of supporting and promoting the controller's activities, and that such data processing activities are appropriately recorded.

4.7. Appropriate Purposes

- **Does the law or legal guidance require a specific legal basis for specific digital advertising activities? Clarify for each activity (suggest using TCF/IAB CCPA "purposes") ("profiling" must be addressed here).**

  No, LGPD does not establish a specific legal basis for digital advertising activities.

  Brazilian law is silent on the matter of marketing/advertisement. Controllers must rely on a valid legal basis when processing data for digital advertising activities. In any case, the principles of the LGPD must be observed, especially transparency and the data subject's right to oppose the processing of data when using the legitimate interest legal basis.

Legitimate interest, according to LGPD, should observe all the following requirements at the same time:

- The processing activity needs to pursue the support and promotion of the controller's activities.
- The activity must protect the data subject's regular exercise of his/her rights OR provide a service that benefits them.
- Data subject's legitimate expectations should be taken into account but are not the deciding factor for the use of this legal basis.

Notwithstanding the general obligation to observe all principles foreseen in the law, LGPD emphasizes the need to comply with transparency and data minimization principles when processing personal data based on legitimate interests.

- **If yes, what are the legal bases (e.g., consent, legitimate interest)? Are there any requirements related to lawful basis (need a valid legal basis to process)/fairness (scope of processing is fair)/transparency (transparent about the processing activity to the consumer and the lawful basis)?**

  Despite the lack of a specific legal basis for digital advertising activities, usually the applicable legal basis is either consent, or legitimate interest (as long as no sensitive data is processed, and the circumstances presented on item 4.6 above are complied with).

- **Does the law address processing for secondary purposes/differing purposes from which it was collected?**

  Yes. LGPD does not allow processing data for purposes which are not informed to the data subject. Any secondary purposes, or changes in the primary purpose, must be informed to the data subject (but does not requires consent or approval, except when consent is the applicable legal basis).

4.8. Safeguards

4.8.1. Overview

LGPD determines the adoption of technical and administrative security measures to protect the personal data from unauthorized accesses and accidental or unlawful situations of destruction, loss, modification, communication, or any form of inappropriate or unlawful processing.

Also, there is an incentive for processing agents that implement rules for good practices and governance that set forth conditions of organization, a regime of processing requests regarding data processing activities including complaints and requests from data subjects, security norms, technical standards, specific obligations for the various parties involved in the processing, educational activities, internal mechanisms of supervision and risk mitigation, and other aspects related to the processing of personal data.

4.8.2. Application to Digital Advertising

There are no specific safeguard requirements relating to the digital advertising industry.

5. DATA SUBJECT RIGHTS/EXEMPTIONS

5.1. Overview

The LGPD establishes that the data subject is entitled to a series of rights that must be guaranteed by both processing agents–controller and processor. In addition, the processing agents are responsible for keeping the data subjects informed of their rights in a clear, objective, and accessible manner.

Thus, according to the LGPD, the data subject is allowed to exercise their rights by direct request to the controller or the processor (Article 18, paragraph three of the LGPD), or through their legally constituted representative. It should be noted that the data subject's request, based on the performance of the rights provided in the LGPD, shall be carried out free of charge and within the timeframe and terms provided for in the LGPD, as per Article 18, paragraph five.

Regarding the timeframes to be observed by the processing agent, the LGPD only regulates the term for answering the data subject's request to confirm or access personal data. Thus, the processing agent shall provide the information requested by the data subject (i) immediately, in a simplified format; or (ii) within a period of fifteen (15) days as from the date of the data subject's request, by means of a clear and complete declaration that indicates the origin of the data, the nonexistence of registration, the criteria used and the purpose of the processing, subject to commercial and industrial secrecy.

Beyond that, if there is a request for the correction, deletion, anonymization, or blocking of data, the controller must immediately inform the other processing agents with whom the data has been shared so that they can carry out the same procedure, except in cases in which this action is proven impossible or involves disproportionate effort, pursuant to Article 18, paragraph six, of the LGPD.

Therefore, the LGPD establishes that the data subject is entitled to, at any time and by means of a request, obtain the following from the controller:

- Confirmation of the existence of processing.
- Access to data.
- Correction of incomplete, inaccurate, or outdated data.
- Anonymization, blocking, or elimination of unnecessary or excessive data or of data processed in noncompliance with the provisions of the LGPD.

- Portability of the data to other service providers or suppliers of products, at the data subject's express request, according to the ANPD, and observing the protection of business and industrial secrets in the process.
- Elimination of the personal data processed with the consent of the data subjects, except in the cases set forth in Article 16 of the LGPD.
- Information on the public and private entities with which the controller has shared data.
- Information on the possibility of not providing consent and on the consequences of such denial.
- Withdrawal of consent, pursuant to the provisions of paragraph five of Article 8 of the LGPD.
- Review of decisions based on the processing of personal data carried out exclusively through automated means.

The rights of confirmation of the existence of processing and access to data can be addressed by the controller immediately when in a simplified format or up to 15 days when in a clear and complete declaration.

For the other data subject rights, the ANPD shall regulate the appropriate timeframe that should be observed by data controllers.

5.2. Access

LGPD provides the right to access personal data for every data subject. It is the controller's obligation to provide such access at any time upon request made by the data subject (or their legal representative).

There are two types of access requests set out by the LGPD: in a simplified format or in a complete declaration. The latter must indicate the origin of the data, the nonexistence of registration, the criteria used and the purpose of the processing (subject to commercial and industrial secrecy). Access requests in simplified format must be answered immediately, while requests in complete format must be provided within a period of 15 days from the date of the data subject's request.

5.3. Rectify

LGPD provides data subjects with the right to rectify any incomplete, inaccurate, or outdated personal data. It is an obligation of the controller to provide such rectification, at any time upon request made by the data subject (or his/her legal representative). Furthermore, if the controller has shared the data that received a correction request (or for deletion, anonymization, or blocking), the controller has the obligation to inform the agent (other controller or processor) who received the data, according to Article 19 §6º.

5.4. Deletion/Erasure

LGPD provides the right to deletion of personal data in two circumstances: (i) when the data is unnecessary, excessive, or processed in noncompliance with LGPD; and (ii) when the data is processed with consent of the data subject.

When the data is unnecessary, excessive, or processed in noncompliance, the data subject can request deletion, anonymization, or blocking, and the controller should evaluate if it is the case to comply with the request.

When the data subject requests deletion of personal data processed under the basis of consent, there is an exception: the controller can refuse to delete the data if it is processed for one of the purposes set out in LGPD's Article 16, as follows:

"Art. 16. Personal data shall be deleted following the termination of their processing, within the scope and technical limits of the activities, but their storage is authorized for the following purposes:
I – Compliance with a legal or regulatory obligation by the controller.
II – Study by a research entity, ensuring, whenever possible, the anonymization of the personal data.
III – Transfer to third parties, provided that the requirements for data processing as provided in this Law are obeyed.
IV – Exclusive use of the controller, with access by third parties being prohibited, and provided the data has been anonymized."

Furthermore, if the controller has shared the data that received a deletion request (or for correction, anonymization, or blocking), it has the obligation to inform the agent who received the data, as per Article 19 §6º:

"The controller shall immediately inform the processing agents with which she/he has carried out the shared use of data of the correction, deletion, anonymization, or blocking of data, so that they can repeat an identical procedure, except in cases in which this action is proven impossible or involves disproportionate effort."

5.5. Restriction on Processing

LGPD provides the right to restrict processing when it establishes the right to request the blocking of data. This right is set forth in Article 18 - IV, with the same requirements and guarantees as the right to deletion, that is (i) when the data is unnecessary, excessive, or not processed in compliance with LGPD; and (ii) when the data is processed with the consent of the data subject.

5.6. Data Portability

LGPD provides data subjects with the right to portability of the data to another service or product provider, by the means of an express request. The only exception to the right to portability is that it does not include data that has already been anonymized by the controller. There is no timeline established by LGPD for exercising this right. ANPD will regulate the right to data portability in the future.

5.7. Right to Object

When the data is processed with any legal basis other than consent, the data subject has the right to object to the processing if there is noncompliance with the provisions of LGPD. When the processing is based on consent, the right to object is compromised by the right to withdraw consent, regardless of noncompliance.

5.8. Right Against Automated Decision-Making

LGPD provides data subjects with the right to request a review of decisions made solely based on the automated processing of personal data affecting their interests. LGPD explicitly mentions that this includes "decisions intended to define her/his personal, professional, consumer and credit profile, or aspects of her/his personality."

Furthermore, LGPD imposes the following responsibility on the controller:

"§1º Whenever requested to do so, the controller shall provide clear and adequate information regarding the criteria and procedures used for an automated decision, subject to commercial and industrial secrecy.

§2º If there is no offer of information as provided in §1 of this article, based on commercial and industrial secrecy, the national authority may carry out an audit to verify discriminatory aspects in automated processing of personal data."

There is no timeline established by LGPD for the exercise of this right.

5.9. Responding to Consumer Rights Requests

There are no specific provisions in LGPD (nor the Consumer's Defense Code) addressing how to respond to consumer rights requests.

5.10. Record Keeping Concerning Rights Requests

There are no specific provisions in LGPD regarding record keeping concerning rights requests, although, considering the accountability principle, it is a processing agent obligation to keep evidence that its obligations are being observed.

5.11. Is Providing Consumers with These Rights Required by Law or Mere Suggestions?

All data subjects' rights are required by LGPD, not mere suggestions.

5.12. Application to Digital Advertising and Extent of the Duty to Answer the Data Subject

As explained in item 5.1 above, both the controller and the processor are compelled by the LGPD to make it possible for data subjects to exercise their rights. Along those lines, the LGPD foresees that the data subject may exercise their rights under the LGPD by means of a request, to be directed to the processing agent; that is, the LGPD

considers that both the controller and the processor are bound to answer to the data subject's request. However, the controller and the processor are allowed to regulate amongst themselves through a Data Processing Agreement ("DPA") in such that, if a data subject presents a request to the processor to execute one of their rights, the processor will immediately notify the controller and, under this circumstance, the processor will redirect the data subject's request to the controller and will assist the controller in complying with said request by adopting the appropriate technical and organizational measures.

6. DATA CONTROLLER AND PROCESSOR AGREEMENTS

6.1. Overview

There are no specific rules on controller and processor agreements under the LGPD. The only requirement for processors is that they follow the controllers' lawful instructions. Controllers are obligated to verify that their instructions comply with data protection regulations.

6.2. Data Controller Outsourcing of Processing

LGPD does not establish rules regarding outsourcing of processing, such as a requirement for written agreements. However, best practices in Brazil include having a written agreement providing certain rules for the outsourcing of processing, especially:

- **Limitation of Purpose:** Data processing agreements often contain a clause prohibiting the processor from using the personal data for purposes other than those established by the controller and informed to the Data Subjects.
- **Limitation of Transfer:** Agreements may prohibit the processor of transferring the personal data to third parties (except in cases of legal obligations) or condition such transfers to previous and written authorization by the controller.
- **Response to Data Subject Requirements:** Parties may agree on the responsibilities of receiving, responding, and fulfilling data subject rights requests. According to the LGPD, the Data Subject may present a requirement to any processing agent, but the controller is ultimately responsible for fulfilling it. It is common to set out in a Data Processing Agreement that the processor must assist the controller in responding to DSRs, for example by receiving requirements, sending a confirmation of receipt, and forwarding the requirement to the controller.
- **Incident notification:** Data Processing Agreements often establish the obligation of the processor to notify the controller in case of any Incidents involving the personal data. Parties may also define a

minimum content for the notification, its timeline, specific channel for communication (e.g., DPO's e-mail address) and an obligation for the processor to assess the controller with the notifications to the ANPD (Brazilian DPA) and Data Subjects affected.

- **Liability for damage compensations:** Parties may allocate their liabilities in case of damages caused by the processing of data–whether the damage is caused to Data Subjects or to one of the processing agents. This contractual allocation of liabilities is limited by LGPD's liability rules. Agreements often reinforce the right of recourse of the party paying compensations (in case such party is not solely responsible for the damages), defining the Agreement as an extrajudicial title of enforcement.
- **Audits:** Data Processing Agreements often establish the right of the controller to demand audits on the processor, to ensure compliance with data protection standards, and the details pertaining to such audits (for example, a minimum time of previous notice to the processor, confidentiality of audits, etc.).

6.3. Data Processor Rights and Responsibilities

Processors are the ones who process personal data in the name of the controller. Data processors are responsible for following the controller's instructions.

Furthermore, processors also have the following responsibilities:

- Keeping a registry of the data processing activities.
- Implementing technical and administrative security measures to protect personal data from unauthorized access and unlawful or accidental situations of destruction, loss, modification, communication, or any other form of inadequate or unlawful processing.

Data processors are also liable for any damage caused by their data processing activities when in violation of the LGPD.

6.4. Application to Digital Advertising

Since LGPD does not establish specific rules regarding the Data Processing Agreement, agents in the digital advertising industry have a wide margin of contractual freedom to negotiate the terms of their agreement, striking for a balance between the interests of the Advertisers and agents who usually act as processors–observing LGPD's liability rules.

7. DATA TRANSFER & OUTSOURCING

7.1. Overview

Data subjects have the right to access information in an easy way regarding shared use of data (which includes data transfers) by the controller, as well as the purpose of sharing.

LGPD imposes limitations on the transfer of sensitive personal data. Sensitive data relating to health cannot be shared between controllers with the purpose of obtaining economic benefits (except for the hypothesis allowed on LGPD). Furthermore, LGPD foresees that the ANPD may impose restrictions on the shared used of any sensitive data between controllers, with the purpose of obtaining economic benefits.

It is worth highlighting that, when the controller that has obtained consent in order to proceed with the processing activity needs to communicate or share personal data with other controllers and has not previously informed the data subject that this could happen, they must obtain specific consent from the data subject for this specific purpose, except when the need for such consent is exempted (i.e., when the controller needs to share the personal data in order to comply with a legal obligation foreseen in Brazilian legislation). However, any eventual dismissal of the consent requirement does not exempt processing agents from the other obligations provided by the LGPD.

7.2. International Data Transfer

The LGPD allows the international transfer of personal data to countries that are deemed by the ANPD to guarantee an adequate level of data protection, or when the controller offers and provides guarantees of compliance with the principles and the rights of the data subject and the regime of data protection provided for in the LGPD through the specific means set out by the law (i.e., SCC, BCR or stamps, certificates, and codes of conduct). However, since the ANPD is not yet operating, there is still no approved SCC or a list of countries with adequate levels of protection.

Therefore, the international transfer of personal data is permitted solely in the following cases (without any order of preference):

- To countries or international organizations that provide an appropriate level of protection of personal data provided for by the LGPD.
- When the controller provides and demonstrates guarantees of compliance with the principles and rights of the data subject and data protection regime established in the LGPD, in the form of:
    - specific contractual sections for a given transfer
    - Standard contractual sections.
    - Global Corporate rules.
    - Seals, certificates, and codes of conduct regularly issued.

- When the transfer is required for international legal cooperation between government intelligence, investigations, and police bodies, in accordance with international law instruments.
- When the transfer is required for the protection of life or physical integrity of the data subject or any third party.
- When the ANPD authorizes such transfer.
- When the transfer results in a commitment undertaken under an international cooperation agreement.
- When the transfer is required for the enforcement of a public policy or legal attribution of the public utility, upon disclosure of the provisions of item I of the main provision of Article 23 of the LGPD.
- When the data subject has provided specific and highlighted consent for such transfer, with prior information on the international nature of the operation, clearly distinguishing it from any other purposes.
- When required to meet the hypotheses established in items II, V, and VI of Article 7 of the LGPD.

There are no specific requirements on outsourcing. If it involves cross-border transfers of personal data, the rules under the LGPD must be observed.

7.3. Application to Digital Advertising

There are no specific restrictions related to transfer of data regarding digital advertising activities, since the sole restrictions imposed by the LGPD to the international transfer of data are those pointed out on item 7.2 above; thus, if the controller guarantees the compliance to any of those parameters, the international transfer will be lawful. To obtain specific and highlighted consent from the data subject, therefore, will only be another hypothesis under which the international transfer of data will be allowed (as per Article 33, VIII, of the LGPD), but it is not, per se, a requirement for the operation at hand.

Regarding the international transfer of data performed under consent, note that the LGPD does not clearly indicate the form in which this should be obtained. For instance, it is unclear in the legislation whether the same means for obtaining general consent (i.e., a checkbox linked to the privacy policy) can be used to obtain consent for international transfers–since it is clear and distinct–or whether it would be necessary to obtain consent through a different means (i.e., a second checkbox exclusively for that purpose) in order to configure specific acceptance. Nonetheless, this is the case when consent is a circumstance under which international transfer of data is allowed, pursuant to Article 33 of the LGPD.

On the other hand, if consent was the original legal basis adopted by the processing agent to collect the personal data in the first place, and at that time the controller did not inform the data subject about the possibility of their data being shared with a third party outside of Brazil, then the controller will have to notify the data subject and obtain new consent. Note that the need to obtain consent in this case stems from the fact that the original purpose of the processing changed and therefore, since consent was the original legal basis adopted, the LGPD determines that

the controller needs to obtain new consent that encompasses the new purpose (as per Article 8, paragraph six, and Article 9, I, of the LGPD). In that sense, consent here is not a requirement for the international transfer itself, but rather for the lawfulness of the consent provided by the data subject.

Finally, it is worth noting that consent is very rarely used as a transfer mechanism because of how impractical it is. If a data subject withdraws her consent, companies need to host her personal data within Brazil and cease to share it with third parties outside of the country.

8. AUDIT/ACCOUNTABILITY

8.1. Overview

Please see below.

8.2. Application to Digital Advertising

- Audit - What audit rights are dictated by law? (E.g., must companies have audit rights over their vendors? Does the classification of those vendors matter?)

  LGPD does not establish audit rights, except that audits may be carried out by the Brazilian National Data Protection Authority.

- Accountability - Must companies/vendors keep certain records to prove they have met certain requirements? What are those requirements?

  The law requires compliance with the principle of accountability, which requires the "demonstration, by the data processing agent, of the adoption of measures which are efficient and capable of proving the compliance with the rules of personal data protection, including the efficacy of such measures."

  Notably, controllers and processors are required to keep records of the personal data processing operations they carry out, "especially when based on legitimate interest." The burden of proof is also on the controller to demonstrate that the consent was duly obtained in compliance with LGPD provisions.

9. DATA RETENTION

9.1. Overview

LGPD's general rule for data retention is that all data should be deleted when the processing terminates. According to Article 15, termination of processing must occur when:

- The purpose has been achieved or the data are no longer necessary to achieve the purpose.
- The processing period ends.

- There is a communication by the data subject, including when exercising the right to revoke consent, subject to the public interest; or
- The ANPD requests the termination if it determines that there has been an LGPD violation.

Data retention is authorized, even after termination of processing, in the following cases (according to Article 16):

- Fulfillment of a legal or regulatory obligation by the controller.
- Study by a research entity (ensuring, whenever possible, anonymization of the personal data); transfer to third parties, as long as the LGPD requirements for data processing are obeyed.
- Exclusive use of the controller, with access by third parties being prohibited, and provided the data has been anonymized.

9.2. Application to Digital Advertising

There are no specific data retention rules to digital advertising industry.

10. DATA PROTECTION AUTHORITY | REGULATORY AUTHORITY

10.1. Overview

The regulatory body responsible for enforcement of data protection rules in Brazil is the ANPD (in Portuguese, "*Autoridade Nacional de Proteção de Dados*"). Despite the vetoes that the original bill suffered in 2018, which very much impacted the creation of the ANPD, on July 2019, with the sanction of Provisional Measure (MP) 869/2018 and its consequent conversion into law (Law No. 13,853/2019), the creation of the ANPD and the National Council for Data Protection and Privacy was finally enacted. The ANPD was created as an entity part of the federal public administration, pertaining to the Presidency of the Republic, as per Article 55-A of the LGPD.

Beyond that, the referred Law attributed a transitory legal nature to the ANPD, since it may, within 2 (two) years, be transformed by the Executive Branch into an Indirect Federal Public Administration entity, subject to a special autarchic regime and pertaining to the Presidency of the Republic, according to Article 55-A, §1°, of the LGPD.

Said possibility of changing in the ANPD's nature is beneficial to companies that transfer data to the European Union, since the GDPR requires the independence of supervisory authorities in relation to its government as one of the requirements to consider a country as having an adequate level of protection. To be perceived as a country with an adequate level of protection on the European Commission's list makes it easier to interact in the international data transfer scenario with the EU, without any eventual bureaucratic procedures involved in other legal basis provided by the GDPR.

In addition, the Federal Government published on August 27, Decree No. 10,474/2020, defining the structure of the ANPD as a body of the Presidency.

10.2. Main Regulator for Data Protection

The Brazilian data protection authority ("ANPD") is the main regulator. The ANPD is a body of federal public administration, member of the Presidency of the Republic, and is composed of:

- Board of Directors, as the highest body of direction
- National Board of Personal Data Protection and Privacy
- Internal Affairs Office
- Ombudsman
- Legal Advisory Body
- Other administrative and specialized units required for the enforcement of the LGPD

The Board of Directors of the ANPD is composed of five directors, including the chief executive officer, all of them nominated by the President of the Republic, according to the requirements for them to be Brazilians with an unblemished reputation, a high level of education, and a great reputation in the field of specialization of the position for which they will be nominated for.

10.3. Main Powers, Duties, and Responsibilities

The ANPD is responsible for the enforcement of the LGPD and has the following powers available to ensure the protection of individuals' data:

- Supervise the protection of personal data, including through the conduction of inspections, or the determination to their occurrence.
- Consider how trade secrets ought to be protected in the context of processing personal data and transparency.
- Develop guidelines for protection of personal data and a national privacy policy.
- Receive and process data subject claims against the controllers (after being submitted to the controller and not solved according to the LGPD).
- Decide how data processing agents could be transparent regarding the personal data processing activities.
- Request, from public authorities that carry out personal data processing activities, information regarding the scope and nature of the data and other details of the processing, with the possibility to issue technical opinions to ensure compliance with the LGPD.

- Amend privacy and personal data protection regulations and procedures, including regarding Data Protection Impact Assessments ("DPIAs").
- Listen to data processing agents and the society in matters of relevant interest.
- Collect and apply its funds and publish a detailed report regarding its expenses.
- Perform agreements with data processing agents in order to eliminate irregularities, legal uncertainties, or litigious situations in administrative proceedings.
- Enact rules, guidelines, and simplified procedures, including regarding deadlines, for small and micro companies, start-ups, and innovative businesses in order to help them achieve compliance with the LGPD.
- Ensure that processing activities of personal data from elderly people is carried out in a simple, clear, accessible and adequate manner to their understanding.
- Decide the interpretation and competencies of the LGPD at an administrative level in cases in which the law is silent.
- Implement simplified mechanisms, including by electronic means, for the registration of complaints about personal data processing activities that do not comply with the LGPD.
- Inspect and sanction cases of data processing activities that do not comply with the LGPD through administrative proceedings that ensure the right to adversary proceedings, full defense, and the right to appeal.
- Report to the appropriate authorities the criminal offences that come to their knowledge.
- Report to the internal affairs bodies any non-compliance with the LGPD by bodies and entities of federal public administration.
- Disseminate knowledge with the Brazilian people about the legal norms and policy surrounding personal data protection and its security measures.
- Encourage the adoption of standards for services and products that facilitate the control and the protection of personal data by their subjects, considering the specificities of the activities and the size of controllers.
- Prepare studies about national and international practices on personal data protection and privacy.
- Promote actions of cooperation with personal data protection authorities from other countries, of international or transnational nature.
- Draft management reports on yearly activities.

10.4. Application to Digital Advertising

ANPD has not yet provided any guidance or pronouncements regarding the digital advertising industry.

The Agency's regulatory schedule for 2021/2022 does not envisage specific regulations for this industry.

11. SANCTIONS

11.1. Overview

The LGPD provides for an escalated system of penalties, starting with a warning and ending with a fine. In that sense, failure to comply with the LGPD by data processing agents may result in several penalties, as per Article 52 of the LGPD, including: warnings; disclosure of the violation; blocking or deletion of the personal data to which the violation relates; daily fines, or simple fines of up to two percent (2 percent) of the sales of the corporate group in Brazil--limited to fifty million Reais (R$ 50,000,000.00) per violation; partial suspension of the functioning of the database for six months; suspension of the exercise of personal data processing activity for up to six months; and a partial or total prohibition of the exercise of data processing activities.

11.2. Liability

Regardless of the industry or the type of processing carried out, LGPD establishes that the processing agents (controller and processor) are obligated to redress any damages caused as a result of carrying out their activity of processing personal data, in violation of data protection legislation.

The distribution of liability between processing agents is established in Article 42, as follows:

> *"§1º In order to ensure the effective compensation to the data subject:*
> *I – Processors are jointly liable for damages caused by the processing when they do not comply with the obligations of data protection legislation or when they have not followed controller's lawful instructions. In this last case, the processor is deemed equivalent to the controller, save from cases of exclusion as provided in Art. 43 of this Law.*
> *II – Controllers directly involved in the processing from which damages resulted to the data subject shall jointly answer, save from cases of exclusion as provided in Art. 43 of this Law.*
> *[...]*
> *§4º Anyone who pays compensation for damages to the data subject has the right to demand compensation from the other liable parties, to the extent of their participation in the damaging event."*

Exceptions to liability are set forth in Article 43:

> *"Art. 43. Processing agents shall not be held liable only when they prove that:*
> *I – They did not carry out the personal data processing that is attributed to them.*
> *II – Although they did carry out the processing of personal data that is attributed to them, there was no violation of the data protection legislation; or*
> *III – The damage arises from the exclusive fault of the data subject or a third party."*

- **Scope of liability for publishers and advertisers for processing activities of ad tech companies.**

The controller or the processor that, as a result of carrying out their activity of processing personal data, cause material, moral, individual or collective damage to others, in violation of legislation for the protection of personal data, are obligated to redress it, pursuant to Article 42 of the LGPD.

For that purpose, processors will be jointly liable for damages caused by processing activities when they do not follow the controller's lawful instructions. The same applies to controllers that were directly involved in processing that resulted in damage to the data subject. This rule will not apply in the cases provided for in Article 43 of the LGPD presented above.

Also, it shall be highlighted that anyone who pays compensation for damages to the data subject has the right to demand compensation from the other liable parties to the extent of their participation in the damaging event.

For instance: a data processing activity carried out by a given company gave rise to material damages to the data subject, whose personal data was leaked. The controller, in said case, faced the payment of the indemnification to the data subject. However, the processor was, in fact, the one that gave rise to the damage. Under this circumstance, the controller is entitled to demand compensation from the processor.

Beyond that, the controller and/or the processor will be subject to the sanctions foreseen in the LGPD, if the processing of personal data failed to comply with the LGPD or if the processing agent involved—the controller or the processor—did not provide the security that its data subject can expect, considering the relevant circumstances of the processing (Article 44 of the LGPD), which may include (a) the way in which the processing was carried out; (b) the result and the risks that one can reasonably expect of it; and (c) the techniques for processing personal data available at the time it was carried out.

- **Scope of liability for ad tech companies for collection activities of publishers and advertisers.**

  Same as above.

- **Scope of liability for ad tech companies for other ad tech companies they enable to process data (either b/c they make the decision of pub or advertisers or agency dictates it).**

  Same as above.

11.3. Enforcement and Market Practice

- **How are claims raised under the law?**

  The claims regarding LGPD could be raised by the ANPD or any data subject. Hence, it shall be known that, even though the ANPD is the competent authority to enforce the sanctions, the judiciary and other entities can also enforce sanctions regarding damages or non-compliance with LGPD.

- **Who enforces them?**

  The main competence to enforce LGPD is from ANPD. Therefore, other entities (as Attorney General Offices, consumer protection bureaus etc.) could use LGPD as a legal basis to promote public civil actions and investigations. There is one precedent related to this kind of action specific to advertising activities: https://www.zdnet.com/article/sao-paulo-subway-facial-recognition-system-slammed-over-user-data-security-and-privacy/

- **What is their practice (quietly working with companies to fix, publicly coming out with large investigations? Fact specific?)**

  It still is hard to define how the ANPD will behave towards the administrative sanctions once the sanctions are not in force yet, and ANPD itself is not yet completely in action.

- **What guidance had been given to date on how to handle requirements in the ad ecosystem? Have the regulators been educated on how the ecosystem operates? Have compliance regimes been discussed with them? Has their feedback been solicited?**

  We do not have until this moment official guidance of how to handle requirements in the ad ecosystem. We are not aware of any feedback solicited from ANPD to this industry and the curriculum of its directors does not indicate that there is a background at the ad ecosystem.

11.4. Remedies

There is a broad range of sanctions that could be applied when an organization violates the law:

- Warning, with an indication of the time period for adopting corrective measures.
- Simple fine of up to two percent (2%) of a private legal entity's, group or conglomerate revenues in Brazil, for the prior financial year, excluding taxes, up to a total maximum of fifty million Reais (R$ 50,000,000.00) per violation.
- Daily fine, subject to the total maximum referred to in item II.
- Publicization of the violation once it has been duly ascertained and its occurrence has been confirmed.
- Blocking of the personal data to which the infraction refers to until its regularization.
- Deletion of the personal data to which the infraction refers to.
- Partial suspension of the operation of the database related to the violation for a maximum period of six (6) months, extendable for the same period, until the normalization of the processing activity by the controller.
- Suspension of the personal data processing activity related to the infraction for a maximum period of six (6) months, extendable for the same period.

- Partial or total prohibition of activities related to data processing.

These sanctions will enter into force only on August 1, 2021.

11.5. Private Right of Action

Data subjects can petition privately against processing agents on account of LGPD, through actions in civil courts or in administrative proceedings towards the ANPD. This is established in Articles 18 and 22, respectively:

> *"Art. 18 §1º The personal data subject has the right to petition, regarding her/his data, against the controller before the national authority."*

> *"Art. 22. The defense of the interests and rights of data subjects may be carried out in court, individually or collectively, as provided in pertinent legislation regarding the instruments of individual and collective protection."*

11.6. Digital Advertising Liability Issues

Liability issues that could especially concern digital advertising agents are those related to the controller's responsibility for the processor's actions (except when the processor alone violates the law and/or the controller's instructions).

It is the controller's obligation to define the processing activity's legal basis and purpose. Therefore, issues relating to consent and legitimate interest (e.g., when using cookies) need to be carefully assessed by the controller before sharing personal data with a processor.

11.7. Application to Digital Advertising

There are no specific liability or sanction rules for the digital advertising industry. Agents is this industry are subject to the general rules described above and should pay attention to particular issues involved in their activities in order to avoid sanctions.

12. NOTIFICATION | CERTIFICATION | REGISTRATION

12.1. Requirements and Brief Description

Notification or registration of databases with the ANPD is not required under the LGPD. Only data breach notification is mandatory.

13. DATA PROTECTION OFFICER

13.1. Overview

The Data Protection Officer ("DPO" or "*Encarregado*", in Portuguese) is the person named by the controller and processor to act as a channel of communication between the controller, the subjects of such data and the National Data Protection Authority (ANPD). Therefore, the LGPD establishes the controller's obligation to appoint a DPO, but there are not yet any exemptions from this obligation or even specific criteria regarding its eligibility conditions and liability.

13.2. DPO – Compulsory Appointment (Yes/No)

A DPO must be appointed by controllers.

The ANPD could exempt controllers from appointing a DPO according to the nature and the size of the entity or the volume of data processing operations. According to ANPD's recently published regulatory schedule, complementary rules and exemptions regarding DPOs will be addressed by the Authority, through a Resolution, in the first semester of 2022.

13.3. Requirements

The identity and contact details of the DPO must be publicly, clearly, and objectively disclosed, preferably on the controllers' website.

The activities of the DPO consist of the following:

- To accept complaints and communications from data subjects, provide clarifications, and take measures.
- To receive communications from the supervisory authority and take measures.
- To instruct the employees and contractors of the entity on the practices to be adopted in relation to personal data protection.
- To carry out any other duties established by the controller or in supplementary rules.

The ANPD may establish supplementary rules on the definition and duties of the DPO.

Even though there is no specific location requirement in the LGPD, it is recommended that the DPO be based in Brazil; if, on the other hand, the appointed DPO is not in Brazil, it is important that they be able to communicate with ANPD and with the data subjects in Portuguese, and be available to be in Brazil when necessary.

13.4. Application to Digital Advertising

There are no specific rules regarding the DPO for digital advertising organizations. Until further notice from the

ANPD, all digital advertising organizations should follow the general rules and appoint a DPO.

14. SELF-REGULATION

14.1. Overview

There are no self-regulation initiatives in place in Brazil regarding data protection in the online ecosystem. However, it is possible to adopt them, since LGPD encourages self-regulatory governance models.

Are there any industry self-regulatory schemes in place in the jurisdiction?

Not yet, but LGPD allows the implementation of self-regulatory models and code of conducts for organizations, economic sectors, etc.

Are there any signal-based programs used in the territory to assist with digital advertising compliance?

No. However, it would be possible to apply such signal-based programs, since LGPD encourages the adoption of best practices and compliance rules by self-regulatory associations, especially to address:

- Conditions of organization
- A regime of operation
- Procedures, including for complaints and petitions from data subjects
- Security norms
- Technical standards
- Specific obligations for the various parties involved in the processing
- Educational activities
- Internal mechanisms of supervision and risk mitigation and other aspects related to the processing of personal data

Therefore, a program similar to, for example, IAB's *Europe Transparency & Consent Framework Policies* would be applicable in Brazil. (Please note the applicability refers to the Framework's self-regulatory and signal-based characteristics, **not to its content**, since LGPD differs from the European e-Privacy Directive).

14.2. Application to Digital Advertising

Although there are no precedents of self-regulatory schemes and signal-based programs for data protection in Brazil, the digital advertising industry appears to be a good field of application for these initiatives, since the industry needs to adapt practices and technology to comply with LGPD.

15. PENDING PRIVACY BILLS

15.1. Overview

Currently in the Brazilian Congress there are few pending privacy bills, among which the only one worth mentioning is the Preliminary Draft of a Bill aiming to regulate the processing of personal data in criminal proceedings. The Preliminary Draft of the so called "Criminal LGPD" was presented by the Technical Commission, which was created by the Brazilian Federal Congress on November 5th, 2020, and intends to regulate the processing of personal data in the fields of public security, criminal investigations and the prosecution of criminal offenses. The preliminary draft is very much inspired by Directive 2016/680 of the European Parliament and of the Council of April 27th, 2016. There is a high likelihood that it will be enacted.

Beyond that, it is worth mentioning Constitutional Amendment Bill No. 17/2019, currently scheduled for voting in the Chamber of Deputies Plenary, which seeks to include the protection of personal data among the fundamental rights and guarantees provided for in the Federal Constitution and establishes the Union's private competence to legislate on the protection and treatment of personal data.

15.2. Application to Digital Advertising

There are no pending privacy bills with relevant impact to the digital advertising industry.

iab.

Canada

Cross-Jurisdiction
Privacy Project

1. THE LAW

1.1 Overview

The Canadian privacy regime is characterized by the co-existence of federal and provincial legislation as well as two distinct and comprehensive privacy regimes, one for the private sector and the other for the public sector. Canada has independent federal and provincial data protection authorities with investigative powers, the federal authority, the Office of the Privacy Commissioner of Canada (OPC) having jurisdiction over the private sector everywhere in Canada except for provincially regulated private organizations in British Columbia, Alberta, and Quebec. Canada protects the right to privacy as a fundamental right. In the context of the private sector, the right to privacy is balanced with the need of organizations to collect, use, or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

In addressing privacy issues under Canadian privacy law, the first step is to identify the applicable law, based on where the issue arises and on the industry sector concerned.

1.2. Key Acts, Regulations, and Directives

Federal and provincial governments in Canada have enacted data protection legislation to govern the collection, use, and disclosure of personal information. An asterisk notation is included for legislation likely applying to digital advertising transactions.

Federal Private Sector Privacy Law:

- *Personal Information Protection and Electronic Documents Act 2000 ('PIPEDA')

Provincial Private Sector Privacy Laws:

- *Personal Information Protection Act, SBC 2003 c 63 ('BC PIPA')
- *Personal Information Protection Act, SA 2003 c P-6.5 ('AB PIPA')
- *Act respecting the Protection of Personal Information in the Private Sector, CQLR c P-39.1 ('Quebec Private Sector Act')
- (Collectively, the provincial statutes are referred to as "Provincial Privacy Laws," and the federal and provincial statutes are referred to as "Canadian Privacy Laws").

Federal Anti-Spam Legislation:

- *Canada's Anti-Spam Legislation, SC 2010 c 23 ('CASL')

In addition, there are numerous other statutes relating to personal health information and personal information collected, used, and disclosed by public sector institutions. We have only identified the above privacy laws

applicable to the private sector during commercial activities.

1.3. Guidelines

The statutory framework in Canada is supplemented by a large and growing body of privacy commissioner findings and guidance at the provincial and federal levels. Below is a sample of available guidelines published by the Office of the Privacy Commissioner of Canada ('OPC') relevant to advertising:

- *Guidelines on Privacy and Online Behavioral Advertising
- *Guidelines for Obtaining Meaningful Consent
- Guidance on Inappropriate Data Practices: Interpretation and Application of Subsection 5(3)

1.4. Case Law

Data protection issues are increasingly being addressed in the courts in Canada. Four provinces have enacted statutory torts for invasion of privacy, and common law privacy torts have also been recognized. With the potential to obtain damages for breaches of privacy even in the absence of any pecuniary loss, claimants and class action counsel increasingly turn to the courts, not the privacy commissioners, for recourse in respect of privacy matters. In addition to torts of invasion of privacy, claimants also claim liability in contract, negligence, misrepresentation, waiver of tort, and other claims. Despite the recent recognition of these torts, there is no relevant case law specifically related to digital advertising practices.

1.5. Application to Digital Advertising

"Personal information" is defined very broadly in Canada. To the extent that digital advertising is based, in part, on personal information, the Canadian Privacy Statutes will apply. See below for a more detailed analysis.

2. SCOPE OF APPLICATION

2.1. Overview

Two salient points characterize scope of application of privacy law in Canada. First, Canada being a federated state, some provinces have chosen to adopt their own privacy legislation governing the private sector, with their own authorities as mentioned above. Territorial jurisdiction is generally defined as bringing provincially regulated companies under provincial privacy law in the three provinces that have them. Federally regulated companies and companies having pan-Canadian activities are generally considered to come under federal privacy law. That said, as will be addressed further, provincial authorities often claim jurisdiction over federally regulated companies.

Second, with respect to subject-matter scope of application, as in Europe, Canada includes indirect identifiers (e.g., IP address or device ID in the definition of personal information) therefore within the scope of privacy law.

2.2. Who Do the Laws/Regulationss Apply to and What Types of Processing Activities Are Covered/Exempted?

Canadian Privacy Laws apply to the collection, use (including storage and processing), and disclosure of personal information by organizations in the private sector during commercial activities.

2.2.1. Canadian Privacy Statutes

Overview

Generally speaking, Canadian Privacy Laws apply to the collection, use, and disclosure of personal information by private sector organizations in the course of commercial activities. The Provincial Privacy Laws have been deemed to be substantially similar to PIPEDA and apply instead of PIPEDA in those provinces that have enacted them (i.e., Alberta, British Columbia and Québec). Public sector organizations and health care providers are generally regulated by other federal and provincial privacy statutes which are outside the scope of this chapter.

Under Canadian Privacy Laws, the term "personal information" is broadly defined as "information about an identifiable individual." OPC has found that "consistent with relevant jurisprudence... information will be about an "identifiable individual" where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information." (PIPEDA Report of Finding, 2013-001) OPC's Guidelines on Privacy and Online Behavioral Advertising contemplate that unique identifiers used in the digital advertising ecosystem (even absent a name) can qualify as personal information:

> "[G]iven the scope and scale of information collected, the powerful means available for gathering and analyzing disparate pieces of data and the personalized nature of the activity, it is reasonable to consider that there will often be a serious possibility that the information could be linked to an individual."

Under PIPEDA, the term "organization" is defined broadly to include corporations, associations, partnerships, and sole proprietorships. PIPEDA defines "commercial activity" as any particular transaction, act, or conduct, or any regular course of conduct that is of a commercial character, including the selling, bartering, or leasing of donor, membership, or other fund-raising lists.

PIPEDA does not apply to:

- Personal information handled by federal government organizations listed under the Privacy Act, RSC 1985 c P-21 ('the Privacy Act').
- The collection, use, or disclosure of employee personal information, unless the organization is a federally regulated business contact information of an individual that the organization collects, uses, or discloses solely for the purpose of communicating or facilitating communication with the individual in relation to

their employment, business or profession.

- An individual's collection, use, or disclosure of personal information strictly for personal purposes.
- An organization's collection, use, or disclosure of personal information solely for journalistic purposes.

Application of Provincial Privacy Laws

Unlike PIPEDA, the Provincial Privacy Laws apply irrespective of whether an activity is commercial in nature, as well as applying to employee personal information within their respective provinces.

PIPEDA does not apply to the collection, use, or disclosure of personal information within the provinces of Alberta, British Columbia, or Quebec, unless:

- The organization is a federally regulated as defined in PIPEDA, e.g., banks, telecommunications companies.
- The personal information is disclosed outside of a province in the course of a commercial activity.

However, there is a degree of uncertainty around transborder data flows where provincial and the federal regulators often both claim jurisdiction over a given activity.

Many organizations may be subject to PIPEDA in respect of certain aspects of their operations, and the provincial laws in respect of other aspects. Although the requirements of PIPEDA and the provincial laws are substantially similar, there are a number of important differences which can arise in certain circumstances. Consideration engaging local counsel for additional clarity on this issue.

Application to Digital Advertising

Canadian Privacy Laws generally apply to digital advertising. Through OPC investigation findings, specific applicable rules have been established:

- Advertising on a free platform is reasonable and should be expected and therefore consent can be required as a condition of service. However, the platform should not collect, use, or disclose personal information beyond what is necessary to provide the free service.
- Advertisers and publishers cannot collect, use, or disclose personal information in violation of the privacy policy of the publisher.
- Profiles that are detailed and based on numerous data points constitute sensitive personal information and therefore require express consent. Please see sections 4.4.3 and 4.4.6 for more information on "sensitive" personal information and the forms of consent.
- Publishers are accountable for advertisers' compliance with their privacy policy.

2.2.2. CASL

Overview

CASL regulates (1) the sending of commercial electronic messages such as promotional and marketing messages, to and from Canada, irrespective of whether the recipient is an individual or an organization and (2) the installation of computer programs on another person's computer system.

Electronic Messages

The term "message" is defined broadly to include a message sent by any means of telecommunication, including a text, sound, voice, or image message, that by virtue of (i) its content, (ii) any hyperlinks to content on a website contained therein, or (iii) contact information contained therein, it would be reasonable to conclude that, among its purposes, it is aimed at encouraging participation in a commercial activity. It prohibits the sending of commercial electronic messages without express consent, implied consent, or an applicable exception, and contains prescriptive form/content and unsubscribe mechanism requirements. Substantial monetary penalties (e.g., up to CAD $10 million per violation) and other consequences can flow from violations of CASL, including extended liability for directors and officers.

Computer Programs

CASL prohibits, during commercial activity, installing, or causing to be installed, a "computer program" on any other person's computer system without express consent of the user or system owner. A "computer program" is defined to mean data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function.

CASL includes "a cookie," "HTML code," and "Java Scripts" as types of "computer programs" and deems express consent to exist for their "installation," provided that it is reasonable to believe that the user or system owner consented to the program's installation.

Application to Digital Advertising

Electronic Messages

To the extent that digital advertisers send a "commercial electronic message" ("CEMs") to an "electronic address" where there is a real and substantial connection to Canada, CASL will apply. For example, email and text messages to Canadian residents represent the classic examples of CEMs that are caught by CASL, but the definition of "electronic message" is broadly defined and non-exhaustive, and can include forms of messaging that are not traditionally considered in connection with anti-spam legislation including, for example, direct messages, and other forms of messaging that are sent to an address used in connection with an email account, instant messaging account, telephone account, or any similar type of account.

Computer Programs
To the extent that digital advertisers install cookies or incorporate JavaScript in their advertising, CASL applies. Practically speaking, websites are not required to display a banner or ask the user to proactively demonstrate their consent to the installation of cookies.

By way of background, under CASL, although it may seem contradictory, express consent is deemed to exist for the installation of these types of "computer programs" provided that it is reasonable to believe that the user consented to their installation. Guidance from the regulatory authority, the Canadian Radio-television and Telecommunications Commission (CRTC) indicates that they interpret this requirement such that "… if the person disables JavaScript in their browser, you would not be considered to have consent under CASL since their conduct would not indicate that they consent to that type of program. Similarly, if the person disables cookies in their browser, you would not be considered to have consent to install cookies" (see Section 2 of Canada's Anti-Spam Legislation Requirements for Installing Computer Programs).

2.3. Jurisdictional Reach

Overview

PIPEDA is silent with respect to its territorial reach. However, the Federal Court of Canada ("the Federal Court") has found that PIPEDA will apply to businesses established in other jurisdictions if there is a "real and substantial connection" between the organization's activities and Canada. An assessment of whether a "real and substantial connection" to Canada exists is based upon a fact-specific analysis of relevant connecting factors, including:

- Whether a foreign-based entity carries on business in Canada or has any physical presence in Canada, including the geographic location to which promotional efforts are targeted.
- Whether the foreign entity engages in marketing efforts directed at Canadian residents.
- The location of the end-user and intermediaries, and whether contracts will be entered into with Canadians.

For example, with respect to websites, relevant connecting factors include where promotional efforts are being targeted, the location of end-users, the source of the content on the website, the location of the website operator, and the location of the host server.

PIPEDA applies to commercial dataflows of personal information across inter-provincial and international borders. PIPEDA also applies to the commercial processing of personal information entirely within a Canadian province or territory, other than in those provinces where substantially similar legislation exists and takes precedence (British Columbia, Alberta, and Quebec). Organizations subject to a substantially similar provincial privacy law are generally exempt from PIPEDA with respect to the collection, use, or disclosure of personal information that occurs within that province.

PIPA BC, PIPA AB and the Quebec Privacy Act apply to personal information practices of organizations within their

respective provinces. Provincial privacy regulatory authorities are asserting their jurisdiction on matters where users reside in the province, but the personal information flows are cross-border in nature. For example, provincial privacy regulatory authorities are often claiming concurrent jurisdiction with the Office of the Privacy Commissioner of Canada over apps and websites that are located outside of Canada but have users within the geographic territory of their jurisdiction.

Does the data subject need to be physically located within the jurisdiction when the data is collected and processed? Is this only the case in certain contexts (e.g., where a company is outside of the territory of the EU, in the case of the GDPR)?

No, the application of Canadian Privacy Laws does not turn on the physical location at the time of data collection. For the regulators to exercise jurisdiction over an organization, there must be a "real and substantial connection to Canada." (Lawson v Accusearch Inc. et al, 2007 FC 125). This connection can be grounded in the residency of individuals, or establishment of the organization or even the presumed impact on Canadian residents as in PIPEDA Report of Findings #2019-002.

Application to Digital Advertising

Hypotheticals to test concerns/jurisdictional reach

Scenario 1 (The baseline): A user residing in Canada (determined by IP address or geo identifier) goes onto a Canadian domain and is served an ad by a Canadian advertiser. The advertiser uses the user data to build a user profile.

- Assuming the initial serving of the ad is not based on personal information (e.g., no retargeting or tailoring of the ad based on information about the user), Canadian Privacy Laws would generally apply to the disclosure of personal information by the publisher to the advertiser, the advertiser's corresponding collection of such personal information and the advertiser's use to build the profile.
- Both the publisher and the advertiser would be required to comply with the Canadian Privacy Laws, including providing appropriate notice and obtaining consent (though for clarity, the same notice and opt-out process would be used by both the publisher and the advertiser).
- Opt-out consent may be appropriate, provided that it meets the criteria set out in the Office of the Privacy Commissioner of Canada's Guidelines on privacy and online behavioral advertising ("OBA Guidelines"), and specifically that:
    - "Individuals are made aware of the purposes for the practice in a manner that is clear and understandable–the purposes must be made obvious and cannot be buried in a privacy policy.

Organizations should be transparent about their practices and consider how to effectively inform individuals of their online behavioral advertising practices, by using a variety of communication methods, such as online banners, layered approaches, and interactive tools.

  - » Individuals are informed of these purposes at or before the time of collection and provided with information about the various parties involved in online behavioral advertising.
  - » Individuals are able to easily opt-out of the practice - ideally at or before the time the information is collected.
  - » The opt-out takes effect immediately and is persistent.
  - » The information collected and used is limited, to the extent practicable, to non-sensitive information (avoiding sensitive information such as medical or health information).
  - » Information collected and used is destroyed as soon as possible or effectively de-identified."
- To the extent sensitive information is used, express consent (opt-in) would be required.

Scenario 2 (User outside Canada): A logged-on/signed-in user goes onto a Canadian domain, but the user's IP address or geo identifier indicates the user is outside Canada. A Canadian advertiser serves an ad and uses the user data to build a user profile.

- Assuming the initial serving of the ad is not based on personal information (e.g., no retargeting or tailoring of the ad based on information about the user),it is likely that a real and substantial connection to Canada would be found to exist in this context, and that Canadian Privacy Laws would generally apply to the disclosure of personal information by the publisher to the advertiser, the advertiser's corresponding collection of such personal information, and the advertiser's use to build the profile.
- Both the publisher and the advertiser would be required to comply with the Canadian Privacy Laws, including providing appropriate notice and obtaining consent as outlined above.
- **Q1:** Does the answer change if this is a signed-out user, with no way of knowing where they are domiciled?
  - » No, since a real and substantial connection would likely be deemed to exist because a Canadian publisher would still be disclosing personal information to a Canadian advertiser, who would still be collecting it and building a profile, all using a Canadian domain.

Scenario 3 (Publisher domain outside Canada): A user residing in Canada (determined by IP address or geo identifier) goes onto a domain outside of Canada. An advertiser outside Canada serves an ad and uses the user data to build a user profile.

  - » Assuming that the domain outside Canada does not target users in Canada and there were no other indicia of a connection to Canada, it is possible that a real and substantial connection to Canada would not be found, and that Canadian Privacy Laws would therefore not apply.

- **Q1:** Does the answer change if the site hosts content aimed at Canadian residents (e.g., a news aggregator with a section on Canadian current affairs)?
  - » Yes, it is likely that a real and substantial connection to Canada would be found to exist in connection with the publisher's targeting of Canadian residents, and that Canadian Privacy Laws would generally apply to the publisher's collection and disclosure of personal information for its own use and the use of the advertiser.
  - » Both the publisher and advertiser would likely be required to comply with the Canadian Privacy Laws, including providing appropriate notice and obtaining consent as outlined above.

Scenario 4 (Advertiser outside Canada): A user residing in Canada (determined by IP address or geo identifier) goes onto a Canadian domain and is served an ad by an advertiser based outside Canada. The advertiser uses the user data to build a user profile.

- Assuming the initial serving of the ad is not based on personal information (e.g., no retargeting or tailoring of the ad based on information about the user), it is likely that a real and substantial connection to Canada would be found to exist in this context, and that Canadian Privacy Laws would generally apply—at minimum—to the disclosure of personal information by the publisher to the advertiser.
- To the extent that a case can be made that the advertiser has a real and substantial connection to Canada (e.g., advertises and sells goods/services to Canadian residents), Canadian Privacy Laws would apply to the advertiser as well.
- The publisher (and, if applicable, the advertiser) would be required to comply with the Canadian Privacy Laws, including providing appropriate notice and obtaining consent as outlined above.

Q: Does the answer change if the advertiser has an affiliate/group company based in Canada?

- The analysis would be fact-specific, but yes, to the extent that the affiliate/group company is involved in the advertising, there would be a stronger real and substantial connection to Canada and Canadian Privacy Laws would likely therefore apply to the advertiser by virtue of their presence and involvement in Canada.

3. DEFINITIONS

3.1. Collect

The term is used but not defined under Canadian Privacy Laws and therefore must be understood according to the commonsense of the word. It is used to refer to the process of gathering personal information (either directly or through a service provider) for the organization's own purposes.

- **When a publisher allows an ad tech company's pixel on its page, who is deemed to "collect" personal information and incur legal obligations (e.g., controller/co-controller obligations under GDPR or "business" obligations under CCPA) – the publisher, the ad tech company, or both?**

In circumstances where a publisher allows an ad tech company's pixel on its page: (i) if the ad tech company is collecting personal information through the pixel solely on behalf of (i.e. as a service provider to) the publisher, the personal information collected through the pixel would be collected by the publisher (even if the collection is actually done by the ad tech company on behalf of the publisher); and (ii) if the ad tech company is collecting personal information through the pixel for its own use (for example, to facilitate the provision of services to other publishers or other parties), it would be viewed as collecting the personal information.

3.2 Data Processing (i.e., collecting, capturing, retaining, recording, organizing, structuring, storing, altering, retrieving, consulting, using, disclosing, transmitting, disseminating, making available, aligning, combining, restricting, erasing, destroying, or otherwise processing)

The terms "data processing" or "processing" are not used in Canadian Privacy Laws. Canadian Privacy Laws regulate the collection, use, disclosure, and protection of personal information. All processing activities noted above, would fit within one of these actions. For example, storing, consulting, and retrieving would be considered "uses" of personal information, and making available, disclosing, or transmitting are likely to be considered "disclosures," depending on the circumstances (for example, making personal information available to employees within a single organization would be a use rather than a disclosure). It is important to note that a transfer of personal information to a service provider for processing solely on behalf of the organization (and not for its own purposes) is considered a "use" of the personal information by the organization and not a disclosure to the service provider.

Express Consent:

Express consent is not specifically defined by Canadian Privacy Laws but is generally understood to mean that some express, active indication of consent is given by the individual. For example, failing to take an action to opt-out of a proposed collection, use or disclosure of personal information would not constitute express consent, but taking an action to actively opt-in to a proposed collection, use or disclosure of personal information would be. In all cases, consent is only valid if sufficiently informed.

Note that Canada's Anti-Spam Legislation contains prescriptive requirements for express consent.

Implied Consent:

Implied consent may be available if the personal information to be collected, used, or disclosed is not sensitive, the proposed collection, use and disclosure is consistent with the individual's reasonable expectations and the collection, use or disclosure does not create a meaningful residual risk of significant harm. It is only reasonable to imply consent in these cases, if the purposes for which personal information will be collected, used, and disclosed, and the nature of the personal information that will be collected, used, and disclosed, would be obvious to a reasonable person.

Note that under Canada's Anti-Spam Legislation, implied consent is only available in certain specified circumstances.

3.3. Personal Information

In general terms, "personal information" means information about an identifiable individual. This definition is given a broad interpretation. Information is generally considered to fit the definition of "personal information" where there is a serious possibility that the individual could be identified through the use of the information, alone or in combination with other information (even if not in the organization's immediate possession).

Type of Information Collected	Does this Category Independently Constitute Personal Information? (Yes/No)	Qualifying Notes (if any)
IP Address	No	IP address can be personal information in some cases (e.g., a home-based IP address vs a workplace IP address where everyone browses from the same IP address).
Mobile Advertising IDs (IDFA, AAID)	Yes	
Consumer identifiers such as: • User device ID • Publisher persistent ID/Cross-publisher cookie ID • Household ID	Yes	

Hashed identifiers such as: • Hashed email • Hashed IP address	Yes	
User Agent such as: • Character string identifying the application • Operating system • Browser information, vendor, and/or version of the requesting user agent	No	To the extent the user agent can be used alone or in combination with other data elements (e.g., fonts, keyboard layout, etc.) this could become personal information.
Device Information such as: • Type, version, system settings, etc.	No	See above.
Website Information such as: • Name • URL, etc.	No	
Advertisement Information such as: • Placement • Title • Creative ID, etc.	No	
Timestamps	No	
Metrics such as: • Counts • Amounts of time	No	

Event Data such as: (e.g., full URL including query string, referral URL)	No	
Precise geolocation (latitude, longitude)	Yes	
General geolocation (city, state, country)	No	Assuming sufficiently general

- **Are pseudonymous digital identifiers by themselves personal information (e.g., IDFA, cookie IDs, proprietary IDs, IP addresses, etc.)? Please provide context to the above chart.**

  Yes. Canadian privacy regulatory authorities have found IP addresses (in some circumstances), computer name, hashed telephone numbers, subscriber IDs, or User IDs pertaining to an ISP's customers, and the type of application used by the subscriber to be personal information. Cookies may not be personal information in and of themselves, but when cookies are used to store unique identifiers for the purpose of profiling a user to target advertisements based on inferred interests, the information would be information about an identifiable individual.

- **If the answer to the above question is, "no," if a Company possesses a persistent digital identifier in Database 1 and has that same identifier in Database 2 with directly identifying information, does that render the pseudonymous information in Database 1 as personal information?**

  n/a (answer to question above is yes)

- **Is a Company's possession of a pseudonymous identifier plus other non-directly identifying data (e.g., age, gender, precise or imprecise geolocation, user agent string, timestamps) considered "personal information"?**

  Yes. The pseudonymous identifier is personal information (as a unique identifier) and the other information is about the individual. So, the information is about an individual who could be identified from the information in combination with other information.

- **Is a Company's possession of a pseudonymous identifier "personal information" if it can hire a service provider or otherwise engage in a transaction with a third party where the identifier *could* be matched to the person, *but* the Company chooses *not* to hire such service provider or undertake such transaction. Is the mere fact that this service is *potentially* available to match to the person sufficient to render that pseudonymous identifier as "personal information"?**

  Yes

- **What level of geolocation is personal information?**

  Personal information is defined under the Canadian Privacy Laws as "information about an identifiable individual." To the extent that any level of geolocation information is "about" an identifiable individual—alone or in combination with other information—it will be deemed to be personal information.

  For example, a geoIP lookup that maps back to a city—on its own—would not be personal information. But when that city is combined with other information (e.g., a user ID, browsing habits, and an email address), the city would be deemed to be personal information. Similarly, an individual's precise location at specific times of the day, combined with other data (such as a residential address directory) could identify the individual and would likely be considered to be sensitive personal information.

- **What level of geolocation is personal information (precise vs. approximate)? Does it need to be associated with an identifier to be considered personal information?**

  Please see the response immediately above.

- **Is a household identifier personal information? (Consider: If a company has a residential IP address (household level ID) and multiple unique device IDs (e.g., MAIDs for every mobile device in the house) associated with that IP address, would that affect whether the household identifier is considered personal information?)**

  An identifier that connects to a specific household would likely be deemed to be personal information, because it is about one or a small group of identifiable individuals (who are likely also related).

- **Is a hashed identifier PI? (Consider: there are commercially available services that will take batches of emails encrypted using standard hashes and return (often a high percentage) of clear emails from them. Does that affect whether they are considered personal information, if all a company has to do is pay for the commercial service?)**

  Hashed identifiers can be personal information to the extent that they are about an identifiable individual. The mere act of hashing personal information does not generally—in and of itself—render it non-identifiable.

3.4. Sensitive Data

Sensitive Data: "Sensitive data" is not defined under PIPEDA or provincial data protection statutes. However, PIPEDA provides that "any information can be sensitive depending on the context" and also stipulates that the collection of sensitive personal information generally requires express consent, which involves the positive action of the individual. PIPEDA also provides that some information (for example, medical records and income records) is almost always considered to be sensitive, and that any information can be sensitive, depending on the context. Sensitive information is also required to be safeguarded by a higher level of protection. It is important to note that personal information that is not—in and of itself—sensitive in nature may become sensitive when it is associated with a substantial amount of other non-sensitive personal information. For example, building a user profile based on non-sensitive information may result in sensitive personal information by virtue of its granularity in what it reveals about the individual.

3.5. Pseudonymous Information

Pseudonymous information: Canadian Privacy Laws do not include a definition of pseudonymous information. For the purposes of this section, we have assumed that pseudonymous information may be re-identified with the data subject when combined with other data (even if the other data is not in the immediate possession of the organization).

- **Does the law subject pseudonymous information to fewer obligations than "regular" personal information?**

  While this can be fact-specific, generally speaking, there are no fewer obligations associated with pseudonymous information.

- **Are "digital identifiers" considered pseudonymous (e.g., IDFA, cookie IDs) or otherwise deemed to be personal information?**

  The Office of the Privacy Commissioner of Canada has found that pseudonymous data (such as hashed telephone numbers), as well as the content and details of sites visited by an

individual, such as that collected using first or third-party cookies and pixel tags, constitutes personal information.

3.6. Anonymized/De-identified Information

Anonymized/de-identified information: Canadian laws do not include a definition of anonymized data or de-identified data. The only reference to information "made anonymous" appears in relation to the limitation on retention, equating it to the information being destroyed. The French version refers to "dépersonnaliser" which means "de-identify." Proposed amendments would replace the notion of personal information "made anonymous" with the process to "de-identify" with a similar meaning but a different status. While under current Canadian law, as well as EU and US law, and proposed amendments to privacy law in Québec, the process to modify personal information to the point that it can no longer identify an individual alone or in combination with other information, is considered "anonymization," under proposed amendments it would be merely "de-identified" and remains personal information governed by privacy law. The consideration behind this amendment is that technologically, anonymization is no longer achievable.

For the purposes of this section, we rely on existing Canadian privacy law and have assumed that there is not a serious risk that anonymous information can be re-identified with the data subject, even where administrative controls (e.g., internal rules) are ignored. We have also assumed that de-identified information may be re-identified with the data subject.

Is there a difference between anonymized or de-identified data?

Based on the assumptions above, yes. Anonymized information would not be considered personal information (and therefore, would not be subject to the Canadian Privacy Laws) while de-identified information would generally still be deemed to be personal information, and therefore subject to the requirements of Canadian Privacy Laws.

The Canadian Anonymization Network is an industry-led initiative that is currently working to define a standard for anonymized and de-identified information.

What common data categories are passed between publishers, advertisers, and ad tech companies that fall into this category when no persistent identifier is present (e.g., browser type, device type, operating system, app name, publisher site)?

N/A

3.7. Data Controller

Data Controller: "Data controller" is not expressly defined under PIPEDA or provincial data protection laws. Canadian statutes refer to "organizations" which are considered to be in control of, and accountable for, compliance with privacy law requirements.

3.8. Joint Controller/Co-Controller

Canadian Privacy Laws do not have a concept of joint controller or co-controller.

3.9. Data Processor/Service Provider (i.e., an entity that is qualified as a processor or service provider under the law because it meets certain requirements and processes data pursuant to a permissible purpose on behalf of a controller/business)

"Data processor" is not defined under Canadian Privacy Laws, which generally use the term "service providers." A service provider is generally understood to be an organization that processes personal information solely on behalf of the accountable organization and not for its own purposes.

Non-controller/processor/service provider (i.e., an entity that is qualified as a processor or service provider under the law because it meets certain requirements and processes data pursuant to a permissible purpose on behalf of a controller/business): In a Canadian context, this is called a service provider. A service provider processes personal information solely on behalf of the accountable organization and not for its own purposes.

In Canadian law, the term arises in the following contexts:

1. Service provider (for example in clause 4.1.3 of Schedule 1 of PIPEDA)
2. Another individual in the context of an individual access request which must be denied if it could disclose personal information about another individual without consent.
3. In relation to a service provider abroad, the OPC guidance on cross-border transfers of data specifically requires ensuring that the transfer of personal information to a service provider abroad does not compromise the protection of the personal information.

3.10. Third Party (i.e., a third party that receives data from a business for non-business purposes and does not necessarily have specific requirements under the law as to such data, such as a third-party under the CCPA)

Non-controller/third-party (i.e., a third party that receives data from a business for non-business purposes and does not necessarily have specific requirements under the law as to such data, such as a third-party under the CCPA): This concept is not contemplated by, and is potentially inconsistent with, Canadian Privacy Laws. Under Canadian Privacy Laws, there are accountable organizations that must only collect, use, and disclose personal information for appropriate purposes with meaningful consent (subject to limited exceptions) and service providers to accountable organizations.

3.11. Data Subject/Consumer

These terms are not defined or otherwise used under applicable law. Instead, PIPEDA refers to "individuals" without defining the term.

- **Does "household"-level information need to be protected similarly to a consumer's information? What are the differences?**

  There is no concept of "household information" in Canadian privacy law. However, household information is likely to constitute personal information since it reveals information about a small group of related and identifiable individuals.

3.12. Profiling

Canadian Privacy Laws do not specifically address profiling, but profiling involves the collection, use, and disclosure of personal information, so Canadian Privacy Law requirements will apply. This includes the requirement to obtain consent for the collection of sensitive personal information.

In relation to profiling, OPC found in its PIPEDA Report of Findings #2015-001 that profiling created sensitive information if it used all URLs visited by an individual to create a "highly detailed multi-faceted profiles" because "all" URLs inevitably includes sensitive URLs, such as health related searches. In those cases, profiling is subject to express consent.

3.13. Automated Decision Making

Not currently addressed under Canadian Privacy Laws.

4. DATA CONTROLLER RIGHTS AND RESPONSIBILITIES

4.1. Overview

PIPEDA requires organizations to comply with a set of legal obligations that are based on the following ten principles:

- Accountability
- Identifying purposes
- Consent
- Limiting collection
- Limiting use, disclosure, and retention
- Accuracy

- Safeguards
- Openness
- Individual access
- Challenging compliance

The Provincial Privacy Laws provide similar requirements.

4.2. Accountability

4.2.1. Overview

Canadian Privacy Laws hold organizations[1] accountable for information under their control and require the appointment of an individual or individuals who are responsible for the organization's compliance with the law.

Organizations are also required to implement policies and practices to address compliance, including:

- Implementing procedures to protect personal information.
- Establishing procedures to receive and respond to complaints and inquiries.
- Training staff and communicating to staff information about the organization's policies and practices.
- Developing information to explain the organization's policies and procedures.[2]

4.2.2. Application to Digital Advertising

With regard to online behavioral advertising ("OBA") in particular, Canadian data protection laws and OPC investigation reports point to the following relevant parameters:

- Using personal information to advertise in support of a free service constitutes a reasonable purpose supported by implied consent (PIPEDA Report of Findings #2009-008 on Facebook).
- Using personal information to advertise in the context of a paid service may require express consent depending on the circumstances (PIPEDA Report of Findings #2015-001 on Bell Canada).

---

[1] PIPEDA and provincial data protection law does not use the term "data controller." See section 3.6 above.

[2] See OPC Guidance on PIPEDA Fair Information Principle 1 – Accountability: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_accountability/

- Advertisers must comply with platforms' privacy policies and platforms are responsible to ensure compliance by advertisers (PIPEDA Report of Findings #2014-001 on Google).
- Openness principle requires that individuals be made aware of OBA upon collection of personal information (Guidelines on privacy and online behavioral advertising).
- Publishers must offer an ability to opt-out, effective immediately and persistently (as above).
- The personal information collected must not be sensitive (as above).
- Personal information must be destroyed or de-identified as soon as possible (as above).
- Tracking of web browsing activity must be done with knowledge and consent. If through cookies, there must be a function to disable them (Web Tracking with Cookies fact sheet).
- OBA to children should be avoided (Guidelines on privacy and online behavioral advertising).

In its 2015 Policy Position on OBA, OPC also interprets PIPEDA to:

- Apply to most of the information collected for OBA as personal information because it may be linked to an identifiable individual.
- Allow OBA as an appropriate purpose for the collection, use and/or disclosure of personal information but OBA should not be a condition of service.
- Allow OBA subject to mere opt out if:
    i. Individuals are made fully aware of the purposes for the OBA practices, and these cannot be buried in a privacy policy.
    ii. This occurs at or before the time of collection (see section 4.4.12 below regarding the requirements in connection with notice for OBA purposes).
    iii. Openness must include information about the various parties involved in OBA.
    iv. Opt-out is easy, immediately effective and always available.
    v. Personal information use and collection is minimal.
    vi. Information is not retained.

4.3. Notice

4.3.1. Overview

i. Who must receive notice? When must notice be provided? What must be in the notice in the digital advertising context? (Consider also, what notice needs to be provided when pixels fire on a webpage?)

PIPEDA requires organizations to explain, orally or in writing, the purposes for which personal information is

collected at or before the time the personal information is collected.[3]

Under the Alberta PIPA and guidance issued by OPC, before or at the time of collecting personal information from the individual, an organization must notify that individual in writing of:

- The purposes for which the personal information is collected.
- The name, position, or title of a person who is able to answer on behalf of the organization the individual's questions about the collection.[4]
- Where an organization transfers personal information outside of Canada, Canadian privacy regulatory authorities would generally expect the organization to provide notice of this trans-border data flow in their privacy policy.
- Where an organization uses a service provider outside Canada to use or store personal information for or on behalf of the organization and with the consent of the individual, or where an organization transfers personal information to a service provider outside of Canada, the organization must, before or at the time of collecting or transferring the personal information, notify the individual in writing or orally of:
    - The way in which the individual may obtain access to written information about the organization's policies and practices with respect to the service provider outside Canada.
    - The name, position or title of a person who is able to answer on behalf of the organization the individual's questions about the collection, use, disclosure or storage of Personal Information by the service provider outside Canada for or on behalf of the organization.[5]

Under the BC PIPA, before or at the time personal information is collected from an individual, an organization must notify that individual in writing or orally of:

- The purposes for which the personal information is collected.
- On request by the individual, the position or title and the contact information for an officer or employee of the organization who is able to answer the individual's questions about the collection.[6]

---

[3] PIPEDA, Schedule 1, 4.2.

[4] Alberta PIPA, s. 13.

[5] Alberta PIPA, s. 13.1.

[6] BC PIPA, s. 10.

Under the Quebec PPIPS, an organization who collects personal information from an individual must, at the time of collection, notify the individual of:

- The object or purpose of collecting the Personal Information.
- The use which will be made of the Personal Information.
- The categories of persons who will have access to it within the organization.
- The place where the Personal Information will be kept.
- The individual's rights of access and rectification.[7]

ii. Is a specific notice required for sensitive information?

No. There is a loose concept of sensitive data under Canadian Privacy Laws. However, no specific notice is prescribed for personal information which could be deemed or considered sensitive. See 3.3 above.

iii. Are there any specific requirements for providing notice related to processing children's personal information?

There are no specific requirements under Canadian Privacy Laws for providing notice related to processing children's personal information.

However, the OPC's 2015 Policy Position on OBA provides:

> "The most obvious type of information that should not be tracked involves children's information. Operators of websites that are targeted at children should not permit the placement of any kind of tracking technologies on the site. It is hard to argue that young children could meaningfully consent to such practices, and the profiling of youngsters to serve them online behaviourally targeted ads seems inappropriate in such circumstances. The Canadian advertising industry has indicated that it will require its members to not knowingly target children; this is a position that the OPC endorses and encourages."

iv. Are there any requirements compelling vendors directly collecting personal information or those receiving it from others personal information to provide additional notices? Who is responsible for those notices? Publishers? The vendors?

Accountability under Canadian Privacy Laws falls to the organization with control of the personal information at issue. In the digital advertising context, this would typically be the publisher or the advertiser. Service providers are not generally required to provide additional notice.

[7] PIPEDA, Schedule 1, 4.2.

4.3.2. Application to Digital Advertising

i. Are there specific requirements related to providing notice of data collection for digital advertising purposes? What must be in the notice in the digital advertising context? Do third parties need to be named? For example, if a publisher gives privacy policy notice that it may share personal information with third parties for advertising purposes, does it have to specify which third parties? Do specific digital advertising activities or purposes need to be disclosed as well (e.g., TCF purposes)?

See section 4.4.12 below regarding the requirements in connection with notice for OBA purposes.

OPC defines OBA as "tracking and targeting of individuals' web activities, across sites and over time, in order to serve advertisements that are tailored to those individuals' inferred interests." In its 2015 Policy Position on OBA, OPC described that there are a number of purposes for online tracking, profiling and targeting individuals, and various techniques for conducting such tracking.

There is no specific guidance on the placement of cookies or similar technology. However, OPC has issued guidance on the use of cookies and similar technology to collect personal information in the context of targeted advertising (Policy position on online behavioral advertising).

PIPEDA requires that the purposes for which an individual's information is to be collected, used, or disclosed be explained in a clear and transparent manner. OBA may be considered an appropriate purpose for the collection, use and/or disclosure of personal information from the perspective of the reasonable person. However, OBA should not be considered a term or condition for individuals to use the Internet generally. There are still other forms of advertising that web sites can rely on. There must also be meaningful consent, and there should be limitations on the types of information collected and used for profiling. Safeguarding the information is also vital, as is limiting the retention of the data to the least amount of time possible.

Regarding the transfer or disclosure of personal information to third parties, OPC's meaningful consent guidance sets out their expectation that third parties be identified "as [specifically] as possible" but that "[in] the case where third parties may change periodically or are too numerous to specify, organizations should at the very least specify the types of third parties information is shared with and then use other means (such as layering) to be more specific." In other words, a global vendor list is not required where the third parties change periodically or there are many of them.

The specificity required by TCF is not required under Canadian Privacy Statutes, however, Canadian Privacy Statutes generally require that organizations are only permitted to collect, use, and disclose personal information in a manner that a reasonable person would consider appropriate in the circumstances, and PIPEDA requires that for a consent to be valid, it must be reasonable for someone to understand the nature, purposes and consequences of their consent. In short, while the level of granularity provided by TCF is not specifically required, the overall practices

must be reasonable, appropriate, and users must be able to provide a valid consent.

iii. From an industry perspective it's common to distinguish data use for ad targeting vs. profile building vs. measuring ad campaigns. Does the notice requirement require separate disclosure of those things? Or is it enough to say something general like "advertising and related purposes"?

No separate disclosure required.

4.4. Consent and Exceptions to Consent

4.4.1. Overview

Except where an exemption is applicable (as described below) consent is required by Canadian Privacy Laws prior to the collection, use, and disclosure of personal information. Consent may be expressed or implied, depending on the circumstances, the intended collections, uses, and disclosures, and the level of sensitivity of the information. Implied consent is generally not appropriate for sensitive personal information, such as health information and financial information.

Moreover, consent under PIPEDA is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose, and consequences of the collection, use, or disclosure of the personal information to which they are consenting. In order to meet the requirement for valid consent, organizations must give consideration to, among other things, the disclosures which they make to individuals at the point of obtaining consent, which has been emphasized in OPC guidance regarding obtaining meaningful consent. These considerations are particularly important in respect of potentially vulnerable groups.

4.4.2 For What Types of Personal Information or Purposes of Processing is Consent Required?

PIPEDA requires informed consent and provides that consent is only valid if it is reasonable to assume that the individual understands the nature, purpose, and consequences of the collection, use, or disclosure to which they are consenting.[8]

PIPEDA acknowledges that the form of consent may vary depending on the circumstances, the reasonable expectations of the individual and the sensitivity of the Personal Information. According to the guidance from OPC, along with the Alberta OIPC and BC OIPC, called Guidelines for obtaining meaningful consent ("Consent Guidance")[9] , express consent (where an individual takes an active step to signify his/her consent, such as checking

[8] PIPEDA, s. 6.1 and Schedule 1, 4.3.

[9] https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/#_determining

a box) is required where the personal information may be considered sensitive, the collection, use, or disclosure is outside of the reasonable expectations of the individual or the collection, use or disclosure creates a meaningful residual risk of significant harm. Implied consent may be appropriate where the information is not sensitive and the proposed collection, use or disclosure would be obvious to the individual in the circumstances. Opt-out consent may be appropriate where the personal information is non-sensitive, the collection, use, or disclosure is within the reasonable expectations of the individual and the collection, use or disclosure does not create a meaningful residual risk of significant harm. See section 2.4 for a further discussion of opt-out consent.

Consent is not required in certain prescribed circumstances. For example, under PIPEDA, consent is not required if the collection is clearly in the interests of the individual, consent cannot be obtained in a timely way, and where it is reasonable to expect that the collection with the consent of the individual would compromise the availability of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the Canada's federal or provincial laws.

In addition, PIPEDA permits organizations to disclose personal information without consent to another organization to:

- Investigate a breach of an agreement or a law that has been, or is about to be, committed.
- Detect or suppress fraud, or to prevent fraud that is likely to be committed. These exemptions apply only where it is reasonable to expect that obtaining consent would compromise the investigation or the ability to prevent, detect or suppress the fraud, and are permissive only; they do not require an organization to disclose personal information.

Consent is not required for the collection, use, and disclosure of certain publicly available information, e.g., published information, court decisions, although some restrictions apply. In general terms, for the exemption to apply, the collection, use, or disclosure must be related to the purpose for which the information is publicly available.

The Alberta PIPA and BC PIPA specifically provide that consent is deemed if the purpose would be considered obvious to a reasonable person, the individual voluntarily provides the personal information to the organization for that purpose, and it is reasonable that an individual would voluntarily provide that information.[10]

The Alberta PIPA and BC PIPA also permit opt-out or negative option consent (e.g., a pre-checked box that the individual must uncheck to indicate that they do not consent) for the collection, use, or disclosure of personal

[10] Alberta PIPA, s. 8(2); BC PIPA, s. 8(1).

information for a particular purpose where:

> (a) The organization provides the individual with a notice, in a form the individual can reasonably understand, that it intends to collect, use, or disclose the individual's Personal Information for the particular purpose.
> (b) The organization gives the individual a reasonable opportunity to decline within a reasonable time to have their Personal Information collected, used, or disclosed for those purposes.
>
> (c) The individual does not decline within that time.
>
> (d) The collection, use, or disclosure of Personal Information is reasonable having regard to the sensitivity of the Personal Information.[11]

Though not specifically described as such, the Quebec PPIPS contemplates implied or deemed consent for the collection and use of personal information as long as the organization informs the individual at the time of collection of the "purpose for collecting the information and the use that will be made of the personal information."[12] Personal information may not be used for any purpose other than what has been identified to the individual, and many not be communicated to third persons, without consent that is "manifest, free and enlightened," which means that there is some express indication that consent is given.[13]

The Quebec PPIPS also provides for opt-out or negative option consent for the use or sharing of a "nominative list" (a list of names, telephone numbers, and/or physical/technological addresses), which in common terms may sometimes be referred to as a marketing list, for marketing purposes.[14]

4.4.3 Does the Consent Obligation Require Granularity (i.e., consent for distinct processing activities) similar to GDPR? Or is the consent obligation more generalized (e.g., requiring consumers to opt-in to "online behavioral advertising" more broadly, without having to consent to each constituent processing activity/party)? Is consent different for different uses or types of data (e.g., sensitive data, profiling, automated decision making, etc.) Please provide details.

The consent obligation requires that the individual know and understand the purposes for the collection, use or disclose of the personal information. When the personal information being collected is innocuous and the

---

[11] Alberta PIPA, s. 8(3); BC PIPA, s. 8(3).

[12] Quebec PPIPS, s. 8.

[13] Quebec PPIPS, s. 13, 14.

[14] Quebec PPIPS, s. 22 – 26.

purpose is straight forward, the consent principle allows for implied consent. When the personal information is more sensitive, explicit, and documented means of obtaining consent such as opt-in options are required. Consent for multiple purposes can be obtained through one request for consent.

4.4.4 Can Personal Information be Processed for Secondary Purposes (i.e., differing purposes from which it was collected)?

Yes, however, as a best practice, OPC Guidance provides that organizations should use the express (opt-in) form of consent for any intended disclosure of personal information to third parties or any other secondary purpose that customers would not reasonably expect to be involved as a matter of course in their purchase of a product or service from your organization.

4.4.5 Are there any Rules Compelling Downstream Recipients/Processors of Personal Information to Provide Additional Notices?

There is no requirement to provide information to an individual when personal information about the individual has been collected from another source. However, personal information may only be collected from another source with the individual's consent, which necessarily requires the individual to be provided with information necessary to obtain informed consent (unless an exception from the consent requirement applies).

When personal information is collected from another organization or from publicly available sources, privacy regulators would expect the organization receiving the personal information to exercise reasonable due diligence to ensure that all necessary consents have been obtained or that an exemption from the consent requirement applies.

4.4.6 Are there any Issues Concerning the Timing of Consent?

The Consent Guidance provides that information must be provided to individuals in manageable and easily accessible ways (potentially including layers) and individuals should be able to control how much more detail they wish to obtain, and when. Information provided to obtain meaningful consent should remain available to individuals as they engage with the organization. Consent choices are not made just once; at any time, individuals should be able to re-consider whether they wish to maintain or withdraw their consent, and full information should be available to them as they make those decisions. See also Section 4.4.12.

4.4.7 Are there Distinct Consent Requirements for Sensitive Personal Information?

See section 3.3 above. There is a loose concept of sensitive data which must be considered in relation to all the Canadian data protection laws, however, sensitive information is not defined. PIPEDA provides that some information (for example, medical records and income records) is almost always considered to be sensitive, but any information can be sensitive depending on the context.[15]

[15] PIPEDA, Schedule 1, 4.3.4.

Examples of information that is considered sensitive by OPC include health information, credit information, and credit score, social insurance number, criminal record data, biometric data, genetic data, employee performance data, video streaming of very young children, and precise geolocation information.[16]

No other categories of personal information are subject to enhanced or different requirements. Sensitive personal information should generally receive a greater degree of protection (e.g., stronger safeguards).[17] The sensitivity of the Personal Information is also relevant in determining the appropriate form of consent. PIPEDA specifically provides that an organization should generally seek express consent for the collection, use, or disclosure of sensitive personal information.[18]

4.4.8 Are there Distinct Consent Requirements for Profiling Consumers? If a Business gets Consent to use Personal Data for "Advertising and Marketing" Purposes, is a Separate (or more specific?) Consent Required to Build an Advertising Profile for Advertising?

There is no express obligation to obtain consent for "profiling" separate and apart from notice and consent obtained for marketing and advertising purposes.

Organizations should be aware that there is an overarching restriction on organizations to only process personal information for purposes that a reasonable person would consider to be appropriate in the circumstances (often referred to as an overarching "reasonableness" standard).[19] The following factors are used to assess "reasonableness" [20]:

- The degree of sensitivity of the personal information at issue.
- Whether the organization's purpose represents a legitimate need /bona fide business interest.
- Whether the collection, use, and disclosure would be effective in meeting the organization's need.

---

[16] See OPC Guidance on Safeguards here: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_08_sg/

[17] PIPEDA, Schedule 1, 4.3.4, 4.3.6 and 4.7.2; OPC, "Guidelines for processing personal data across borders" (January 2009), online: https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127/

[18] PIPEDA, Schedule 1, 4.3.4.

[19] PIPEDA, s. 5(3); Alberta PIPA, s. 11; BC PIPA, s. 11; Quebec PPIPS, s. 4 and 5.

[20] *Turner v. Telus Communications Inc.*, 2005 FC 1601 (CanLII).

- Whether there are less invasive means of achieving the same ends at comparable cost and with comparable benefits.
- Whether the loss of privacy is proportional to the benefits.

OPC has issued guidance on inappropriate data practices, which provides examples of inappropriate data practices including: collection, use, or disclosure that is otherwise unlawful (such as a collection, use or disclosure that violates credit reporting legislation), profiling, or categorization that leads to unfair, unethical, or discriminatory treatment contrary to human rights law, collection, use or disclosure for purposes that are known or likely to cause significant harm to the individual, publishing personal information with the intended purpose of charging individuals for its removal, requiring passwords to social media accounts for the purpose of employee screening and surveillance by an organization through audio or video functionality of the individual's own device.[21]

4.4.9 Are there Distinct Consent Requirements for Automated Decision Making?

In January 2020, OPC launched a consultation to seek comments on various proposals for amending PIPEDA to ensure appropriate regulation of artificial intelligence. See for example, Policy Proposals for PIPEDA Reform to Address Artificial Intelligence Report.

4.4.10 Are there any Age Restrictions Related to Consent? Are there Distinct Consent Requirements Around Processing Children's Personal Information?

OPC takes the view that in all but exceptional circumstances, 13 is the minimum age at which a child can provide meaningful consent; below that age, consent should be obtained from parents or guardians. There is no specific guidance on how consent should be obtained from parents or guardians, but in one reported decision from OPC, OPC determined that notifying parents by email that a child had opened an online account was not sufficient, and that the parent should have been required to take a step to authorize the opening of the account (such as clicking a link). For children over 13, organizations should be able to demonstrate that they have considered the level of maturity and adapted consent processes accordingly.

Canadian data protection laws do not prescribe specific circumstances in which parental consent is required nor do they prescribe specific steps that an organization must take to verify that the person providing consent holds parental responsibility (or equivalent). Organizations should be ready to demonstrate on demand that their chosen process leads to meaningful and valid consent.[22]

---

[21] See https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805/#fn9

[22] See Consent Guidance.

Personal Information relating to youth and children is seen by OPC as being particularly sensitive, and OPC recommends limiting the circumstances in which Personal Information of children is collected.

4.4.11 Can Consent, However Manifested, be Revoked?

Yes. PIPEDA and provincial data protection laws provide individuals with the right to withdraw or vary their consent to the collection, use or disclosure of their personal information, subject to contractual and legal restrictions and reasonable notice.

If the individual withdraws consent, further processing actions based on that consent must cease, subject to contractual and legal restrictions. For example, the individual cannot withdraw consent to any collection, use, or disclosure of personal information required to perform a contract in place between the individual and the organization, or to a disclosure of Personal Information required by law (e.g., disclosures to taxing authorities for income reporting purposes). Canadian data protection laws do not specify that the withdrawal of consent must apply to processing actions completed before consent was withdrawn.

4.4.12. Application to Digital Advertising

In OPC's 2015 Policy Position on OBA, it indicates that opt-out consent, meaning consent except when exercising the opt-out (i.e., a form of implied consent), may be acceptable provided certain conditions are met. The conditions are:

- Individuals are made aware of the purposes for the practice in a manner that is clear and understandable – the purposes must be made obvious and cannot be buried in a privacy policy. Organizations should be transparent about their practices and consider how to effectively inform individuals of their OBA practices, by using a variety of communication methods, such as online banners, layered approaches, and interactive tools.
- Individuals are informed of these purposes at or before the time of collection and provided with information about the various parties involved in OBA.
- Individuals are able to easily opt-out of the practice--
- ideally at or before the time the information is collected.
- The opt-out takes effect immediately and is persistent.
- The information collected and used is limited, to the extent practicable, to non-sensitive information (avoiding sensitive information such as medical or health information).
- Information collected and used is destroyed as soon as possible or effectively de-identified.

In practice, compliant notice for OBA purposes is provided in a variety of ways, including (i) above-the-fold (e.g., no scrolling) notice on each page where OBA-related personal information is collected, (ii) banners at the top of bottom of the page providing notice and enabling users to click through to obtain more information or opt-out, and (iii) pop-up windows that inform users about OBA-related personal information that may be collected and that require users to make a choice before proceeding.

4.5. Appropriate Purposes

4.5.1. Overview

Canadian data protection laws contain an overarching requirement that organizations may only collect, use, or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances. In other words, even with consent, there are certain activities which may be prohibited under PIPEDA. A similar restriction is applicable under provincial laws.

In assessing whether a reasonable person would find a purpose for collecting, using, and disclosing personal information to be appropriate, OPC and the Federal Court have applied the following four-part test in a number of cases:

- Is the activity demonstrably necessary to meet a specific need.
- Is the activity likely to be effective in meeting that need.
- Is the loss of privacy proportional to the benefit gained.
- Is there a less privacy-invasive way of achieving the same end.

Although the test will not be applicable in every case, it provides a useful guide for assessing activities, and has often been applied in the workplace and surveillance contexts in particular.

4.5.2. Application to Digital Advertising

i. Does the law or legal guidance require a specific legal basis for specific digital advertising activities? Clarify for each activity (suggest using TCF/IAB CCPA "purposes") ("profiling" must be addressed here).

See 4.3.2 above.

4.6. Safeguards

4.6.1. Overview

Organizations are required to use security safeguards to protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification.

PIPEDA and provincial data protection laws do not specify particular security safeguards that must be used.

However, they do require that the nature of the safeguards must be appropriate to the level of sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. Organizations must consider and implement, as appropriate: physical measures, such as locked cabinets and doors; organizational measures, such as access on a "need to know" basis and clean desk policies; and technological measures, such as passwords and encryption. Commissioner decisions and guidance materials provide additional direction regarding appropriate safeguards in particular circumstances.

Canadian data protection laws also require that organizations make their employees aware of the importance of maintaining the confidentiality of personal information, and that care be used in the disposal or destruction of personal information to prevent unauthorized parties from gaining access to the information.

4.6.2. Application to Digital Advertising

No specific or distinct application to digital advertising.

5. DATA SUBJECT RIGHTS/EXEMPTIONS

5.1. Overview

Canadian Privacy Laws provide individuals with rights of access and correction to their personal information and mechanisms to challenge compliance subject to certain limited exemptions.

5.2. Access

Under Canadian Privacy Laws, individuals have a general right to obtain access to their personal information held by organizations. Access requests must be processed in accordance with the applicable statute, within prescribed timeframes. Organizations are permitted to refuse access only in enumerated circumstances, and generally must sever exempt information from non-exempt information where possible. For example, under PIPEDA, organizations may refuse access to personal information where, among other exceptions, the information is protected by solicitor-client privilege or would reveal confidential commercial information.

Requests for access to personal information under private sector privacy statutes are relatively infrequent in Canada. However, they are often attempted to be used as a form of early litigation discovery by individual litigants and prospective litigants, including former employees. Organizations generally must process such requests, notwithstanding whether parallel litigation proceedings are in existence.

See section six below. In addition, individuals have the right to submit complaints to organizations, to withdraw consent (subject to some limitations), and to file complaints with OPC.

5.3. Rectify

Under Canadian Privacy Laws, if an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization must amend the information as required. Depending on the nature of the information challenged, this could involve correction, deletion, or addition of information. Where appropriate, amended information must be transmitted to third parties who have access to the information in question.

5.4. Deletion/Erasure

The Quebec PPIPS provides that an individual is entitled to have personal information that was collected other than in compliance with that law deleted. Individuals also have the right to have their name and contact details "deleted" from marketing lists. The Quebec Civil Code gives individuals the right to have obsolete personal information or personal information that is not required by the organization to be deleted.

The other Canadian Privacy Laws do not provide for a general right of erasure. However, the right to withdraw consent combined with the obligation not to retain personal information for longer than necessary can give rise to an obligation to delete personal information in certain circumstances.

5.5. Restriction on Processing

Canadian Privacy Laws do not currently provide a right of objection to processing. An individual may withdraw or refuse to provide consent to the collection, use or disclosure of Personal Information where applicable.

5.6. Data Portability

Canadian Privacy Laws do not currently provide a right of data portability.

5.7. Right to Object

Canadian Privacy Laws do not currently provide a right of objection to processing. An individual may withdraw or refuse to provide consent to the collection, use, or disclosure of Personal Information where applicable.

5.8. Right Against Automated Decision-Making

Canadian Privacy Laws do not currently provide a right against automated decision-making.

5.9. Responding to Consumer Rights Requests

Under Canadian Privacy Law, an organization is required to comply with an individual's access or rectification request where the request is in writing. An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of Personal Information and the information provided by the individual may only be used for this purpose.

The organization must provide any necessary assistance to enable an individual to make their request. The Alberta PIPA and BC PIPA require the organization to make a reasonable effort to respond to the individual as accurately and completely as reasonably possible.

Under PIPEDA, the BC PIPA and the Quebec PPIPS, organizations must exercise due diligence in responding to a request for access or rectification within a reasonable period of time and, in any event, within 30 days of receipt of the request. The time limit for responding to a request under the Alberta PIPA is 45 days from receipt of the request.

PIPEDA allows organizations to extend the time limit for responding to a request for access or rectification: (a) for a maximum of 30 days if meeting the time limit would unreasonably interfere with the organization's activities, or if meeting the time limit would be impractical having regard to any consultations required to be undertaken with third parties; or (b) for the period of time necessary to convert the Personal Information to an alternative format.

Under the Alberta PIPA and BC PIPA, an organization may extend the time limit for providing access to Personal Information for up to an additional 30 days (or for a longer period with the Alberta OIPC or BC OIPC's permission) if:

(i) The individual does not give enough detail to enable the organization to identify the Personal Information requested.
(ii) A large amount of Personal Information is requested or must be searched and (or in the case of the Alberta PIPA, or) meeting the time limit would unreasonably interfere with the organization's operations.
(iii) More time is needed to consult with another organization or public body before the organization is able to decide whether or not to give the individual access to the Personal Information requested (and under the Alberta PIPA, to decide whether or not to provide information about the use or disclosure of the personal information).

The Quebec PPIPS does not expressly provide for extensions.

If an organization fails to respond to a request for access or rectification within the applicable time period, the organization will be deemed to have refused the request and the individual may file a complaint with the relevant Commissioner.

5.10. Record Keeping Concerning Rights Requests

In general, where a request is not resolved to the satisfaction of the individual, the substance of the unresolved issue must be recorded by the organization and transmitted to third parties where appropriate.

5.11. Is Providing Consumers with These Rights Required by Law or Mere Suggestions?

Canadian Privacy Laws require providing individuals with these rights.

5.12. Application to Digital Advertising

Canadian Privacy Laws require organizations with control of personal information to pass requests pursuant to these rights down to their service providers. Generally speaking, such requests do not need to be passed to other accountable entities (e.g., other data controllers).

6. DATA CONTROLLER AND PROCESSOR AGREEMENTS

6.1. Overview

Each Canadian Privacy Law provides that where an organization with personal information under its control engages a third party to process the Personal Information on its behalf, the organization with personal information under its control is responsible for ensuring that the service provider complies with the requirements of the relevant law.

In a 2014 investigation report from OPC, OPC held that "an Organization's status as a third-party processor does not prevent it from being subject to [PIPEDA]. The Act applies to all organizations that have personal information in their possession or custody, so long as the information was collected, used, or disclosed in the course of a commercial activity that has a real and substantial connection to Canada" (PIPEDA Report of Findings #2014-004). A similar position was taken in a 2019 joint investigation report from OPC and BC OIPC. We are not aware of any similar decision from the Alberta OIPC or Quebec PPIPS, however, in our view, these Commissioners are likely to take a similar position.

6.2. Data Controller Outsourcing of Processing

Each Canadian Privacy Law provides that where an organization with personal information under its control engages a third party to process the personal information on its behalf, the organization with personal information under its control is responsible for ensuring that the service provider complies with the requirements of the relevant law. However, Canadian Privacy Laws do not specifically state that service providers have no obligations under Canadian Privacy Laws.

6.3. Data Processor Rights and Responsibilities

A service provider can generally rely on the organization to obtain consent or ensure other conditions for processing have been met. PIPEDA does not specify whether the service provider is responsible for ensuring that consent has been obtained or that other conditions for processing have been met. In a 2019 OPC investigation report, OPC held that PIPEDA allows organizations to process personal information on behalf of other organizations based on the consent given by the individual to the other organization but creates an obligation on the service provider to exercise due diligence in terms of determining whether consent has in fact been acquired for how they use personal information.

Under BC PIPA, the requirement to respond to data subject requests applies only to the organization that controls the personal information, and the Quebec PPIPS specifically provides that a service provider may refer such requests to the controller. The requirement to respond to data subject requests is not expressly limited to controllers under PIPEDA and the Alberta PIPA, but it is limited in this way in practice.

6.4. Application to Digital Advertising

Not applicable.

7. DATA TRANSFER & OUTSOURCING

7.1. Overview

An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. In general terms, organizations must use contractual or other means, which usually include technical measures, to provide a comparable level of protection while the information is being processed by a third-party service provider or other entity. Additional considerations, including notice to individuals, are applicable regarding the use of service providers located outside of Canada. Certain provincial privacy laws impose additional obligations in relation to cross-border transfers.

7.2. Application to Digital Advertising

Canadian private sector privacy laws set out fairly consistent obligations for private sector organizations that outsource the processing of personal information. These requirements are generally contained within the statutory-based principles of accountability, safeguards, and openness.

- Accountability: Under Canadian Privacy Laws, an "organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing" (see, for example, PIPEDA, Principle 4.1.3). Consequently, an organization that transfers personal information to a third party (including a corporate affiliate) for processing under an outsourcing arrangement remains accountable for the protection of the personal information it transfers. This includes cloud service providers.
- Safeguards: Canadian Privacy Laws contain safeguarding obligations that require an organization to implement reasonable technical, physical, and administrative measures in an effort to protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. These obligations apply to organizations when personal information is in the custody of a third-party service provider, including a cloud service provider.

- Openness: Canadian Privacy Laws require organizations to be transparent about their personal information handling practices, and organizations should there make information available about trans-border transfers of personal information and the use of third-party service providers.

To the extent that publishers and advertisers *transfer* personal information to a third-party service provider for the purposes of processing on the data on their behalf, such organizations should take steps to implement contractual accountability and safeguarding provisions (e.g., requirements to only process the personal information for the purposes set out in the agreement and to implement safeguards appropriate to protect the personal information from unauthorized access, use, disclosure, or modification. To the extent that publishers and advertisers *disclose* personal information to third parties located outside of Canada, publishers and advertisers should include a reference in their notice (e.g., online advertising notice or privacy policy) that third parties to whom personal information may be disclosed operate outside Canada.

8. AUDIT/ACCOUNTABILITY

8.1. Overview

Under Canadian Privacy Laws, organizations are generally accountable for the personal information in their custody and under their control (e.g., in the hands of a third-party service provider). While Canadian Privacy Laws are generally not prescriptive regarding the records that must be retained to evidence compliance, practically speaking, accountable entities should be imposing record-keeping requirements on third-party service providers in the event that the accountable entity is called upon to demonstrate their compliance.

In a commercial context, organizations that are accountable for personal information frequently negotiate audit rights where a service provider will have custody of a significant amount of personal information or where personal information may be sensitive in nature, all for the purposes of reviewing and confirming compliance with both contractual terms and Canadian Privacy Laws. Audit rights are not mandatory under commercial agreements, but organizations that are accountable for personal information must nonetheless consider how they will evidence compliance.

Under PIPEDA, OPC has the power to audit organizations on reasonable grounds and with reasonable notice. OPC has exercised this power in the context of both organization-specific audits and sectoral audits where systemic issues had been identified.

8.2. Application to Digital Advertising

In a digital advertising context, audit rights will need to be tailored to the commercial arrangement, taking into account the volume and sensitivity of personal information contemplated in the underlying data flows. The parties will also need to consider the breadth and scope of records that will need to be retained to evidence compliance by accountable entities.

9. DATA RETENTION

9.1. Overview

PIPEDA states that personal information must be retained only for as long as is necessary to fulfil the purposes for which it was collected, after which it should be securely destroyed, erased, or rendered anonymous. However, there are exceptions to this: an organization must retain information that is the subject of a request for access for as long as necessary to allow the individual to exhaust any recourse open to them in relation to the request; and information that has been used to make a decision about an individual must be retained long enough to allow the individual access to that information following the decision.

A specifically identified purpose is often a clear indicator of how long information needs to be retained. In some cases, determining the appropriate retention period may be complex as there is no "one-size-fits-all" retention period. For some organizations, there is a legislative requirement to keep information for a certain amount of time. In other instances, there may be no such requirement, and an organization needs to determine the appropriate retention period.

9.2. Application to Digital Advertising

Since Canadian privacy law requires that personal information that is no longer required to fulfil its purpose be "destroyed, erased, or made anonymous." Personal information collected to serve ads should be destroyed as soon as that purpose is fulfilled. Compliant ad tech mbed expiry of data according to the minimal retention times as necessary to provide their service.

10. DATA PROTECTION AUTHORITY | REGULATORY AUTHORITY

10.1. Overview

Private sector privacy law in Canada is regulated by four privacy regulatory authorities:

- Federally: Office of the Privacy Commissioner of Canada
- British Columbia: Office of the Information & Privacy Commissioner for British Columbia
- Alberta: Office of the Information & Privacy Commissioner of Alberta
- Québec: Commission d'accès à l'information du Québec

To the extent that representations are made in connection with the manner in which personal information is treated, the Competition Bureau of Canada may also enforce laws relating to false or misleading representations to the public.

10.2. Main Regulator for Data Protection

PIPEDA is administered by OPC. Provincial privacy commissioners administer the provincial privacy laws. While these provincial and territorial commissioners have their own unique mandates and powers under provincial laws, including order-making power, they often work collaboratively with OPC and one another on investigations and policy matters.

CASL is administered by CRTC, the Competition Bureau Canada, and OPC. Each regulatory authority has jurisdiction over particular aspects of CASL requirements and enforcement.

10.3. Main Powers, Duties and Responsibilities

One of the main roles of OPC is to investigate and attempt to resolve complaints, make findings, and issue non-binding recommendations. OPC is an ombudsperson and, as such, does not have the power to issue binding orders or fines, although such powers are being considered. It is notable that, unlike OPC, the provincial commissioners do have order-making powers.

Following the completion of an OPC investigation, individuals and OPC may seek binding enforcement and related relief in the Federal Court. OPC also initiates investigations, audits, and related enforcement activity even in the absence of a complaint.

In addition, OPC's mandate includes an important public education and guidance role. OPC has published many guidance documents, summaries of findings, and other resources for individuals and organizations.

10.4. Application to Digital Advertising

The Canadian privacy regulators outlined above have taken jurisdiction over the personal information data flows in the digital advertising ecosystem.

11. SANCTIONS

11.1. Overview

While Canadian privacy regulators have extensive enforcement powers, the sanctions to-date for contraventions of Canadian Privacy Laws have generally had a reputational impact. With anticipated changes to Canadian Privacy Laws expected in 2021/2022, however, the impact is expected to shift toward new financial penalties, though the precise scope of these penalties had not yet been finalized at the time of publication.

11.2. Liability

Please see 11.3, Enforcement and Market Practice.

11.3. Enforcement and Market Practice

Under Canadian Privacy Laws, individuals have a right to formally complain to the applicable regulatory authority. Privacy regulatory authorities have an express obligation to investigate complaints, save in some exceptional circumstances where they may decline to do so. Privacy regulatory authorities also have the authority to open investigations at their own initiative.

PIPEDA

Under PIPEDA, the Privacy Commissioner may initiate a complaint if satisfied that there are reasonable grounds to investigate a matter. Generally, the Commissioner must investigate complaints brought by individuals, unless they are of the opinion that:

- The complainant should first exhaust grievance or review procedures otherwise reasonably available.
- The complaint could more appropriately be dealt with, initially or completely, by means of a procedure provided for under another law of Canada or the laws of a province.
- The complaint was not filed within a reasonable period after the day on which the subject matter of the complaint arose.
- The act if proved would constitute a contravention of any of sections 6-9 of CASL or of section 52.01 of the Competition Act or reviewable conduct under section 74.011 of that Act (PIPEDA, s. 12(1) and 12(2)).

In the conduct of an investigation of a complaint, the Commissioner has the power to:

- Summon witnesses
- Administer oaths
- Compel production of evidence
- Enter premises
- Converse in private with any person in any premises entered
- Examine or obtain copies of relevant records found in premises

Following an investigation, OPC shall issue a report with findings and recommendations. Reports may be made public if the Commissioner believes it is in the public interest to do so.

After receiving OPC's report, a complainant (but not the organization subject to the complaint) may apply to Federal Court for a *de novo* review of the complaint and the court has broad remedial powers, including the power to:

- Order a correction of the organization's practices.

- Order publication of a notice of any action taken or proposed to be taken to correct its practices.
- Award damages to the complainant, including damages for any humiliation that the complainant has suffered (PIPEDA, s. 16).

A *de novo* review is different than a judicial review of the Commissioner's findings and recommendations pursuant to section 18.1 of the *Federal Courts Act*, which can be brought by either party on the grounds that the Commissioner:

- Acted without jurisdiction, acted beyond its jurisdiction or refused to exercise its jurisdiction.
- Failed to observe a principle of natural justice, procedural fairness or other procedure that it was required by law to observe.
- Erred in law in making a decision or an order, whether or not the error appears on the face of the record.
- Based its decision or order on an erroneous finding of fact that it made in a perverse or capricious manner or without regard for the material before it:
- Acted, or failed to act, by reason of fraud or perjured evidence; or
- Acted in any other way that was contrary to law.

Under PIPEDA, there is no private right of action. OPC can also pursue legal action before the Federal Court when matters are unresolved.

Provincial Privacy Laws

Under PIPA Alberta and PIPA BC, an investigation may be elevated to a formal inquiry by the Commissioner. Formal inquiries result in binding orders. Organizations are required to comply with orders within a prescribed time period or apply for judicial review.

In Alberta, an order made by the Commissioner may be filed with a clerk of the Court of Queen's Bench and, after filing, the order is enforceable as a judgment or order of that Court. A BC Commissioner's order cannot be automatically filed in the same way.

In both British Columbia and Alberta, once an order is final, an affected individual has a cause of action against the organization for damages for loss or injury that the individual has suffered as a result of the breach.

Similarly, under the Quebec Privacy Act, an order must be obeyed within a prescribed time period. An individual may appeal to a judge of the Court of Quebec on questions of law or jurisdiction with respect to a final decision.

Other Issues

- As noted above, publishers and advertisers should be aware that the Competition Bureau of Canada may seek to enforce representations about how personal information is collected, used, or disclosed to the extent that they are false or misleading in a material respect.
- Under PIPEDA, the Privacy Commissioner has the power to audit the personal information management practices of an organization or sector if they have reasonable grounds to believe that the organization/sector has contravened PIPEDA, provided that reasonable notice is given. The Privacy Commissioner also has the power to enter into compliance agreements with organizations if the Commissioner believes on reasonable grounds that an organization has committed, is about to commit, or is likely to commit an act or omission that could constitute a contravention of PIPEDA or a failure to follow recommendations in Schedule I to PIPEDA.

11.4 Remedies

OPC and the provincial privacy commissioners have issued many findings, touching on virtually every aspect of d ata protection law, including those described above. OPC has also recommended that in some cases an organization undertake an independent third-party audit to demonstrate that the organization is in compliance with PIPEDA. OPC now has the ability to enter into compliance agreements with organizations in the wake of investigations and complaints. However, OPC does not currently have the power to issue fines or penalties.

11.5. Private Right of Action

While historically privacy matters have less frequently been pursued in the courts, in recent years the landscape has changed dramatically in Canada. Courts have awarded damages for violations of PIPEDA in a number of cases, and there has been a sharp increase in tort claims and related civil litigation and class action proceedings. Claimants now frequently bypass privacy commissioners and proceed directly to court to seek damages and other relief in respect of privacy matters. In a number of cases, claimants have obtained damages for privacy breaches, and certification of class actions, even in the absence of any pecuniary loss flowing from a breach. The current volume of privacy-related litigation, and certifications of class proceedings, is unprecedented in Canada (see section 15, below).

11.6. Digital Advertising Liability Issues

In a digital advertising context, the primary enforcement-related issues to-date have had a primarily reputational impact in the form of adverse publicity about the manner in which personal information is being used by organizations in the digital advertising space in contravention of Canadian Privacy Laws. With updates anticipated to the Canadian Privacy Laws expected in 2021/2022, however, the penalties for non-compliance could increasingly shift toward financial penalties.

Canadian privacy regulators are generally quite well-versed in matters of the digital advertising ecosystem, and the Office of the Privacy Commissioner has a dedicated technology team that assists with detailed examinations of the technology underlying OPC's investigations.

12. NOTIFICATION | CERTIFICATION | REGISTRATION

12.1. Overview

Organizations are not required to notify or register with the regulatory authorities under privacy laws in Canada.

12.2. Requirements and Brief Description

N/A

12.3. Application to Digital Advertising

N/A

13. DATA PROTECTION OFFICER

13.1. Overview

Under Canadian law, every organization must designate an individual responsible for compliance with Canadian law. Note, the term Data Protection Officer is not used under Canadian law and no particular title is mandated.

13.2. DPO – Compulsory Appointment (Yes/No)

Yes, this individual ensures internal privacy compliance, although it is not required that they be called the "DPO" under Canadian law.

13.3. Requirements

Under PIPEDA and the privacy laws in British Columbia and Alberta, organizations are required to designate an individual or individuals responsible for compliance with PIPEDA. This individual does not need to be located in the jurisdiction, and the individual is conventionally known as the "Privacy Officer," although PIPEDA does not specify any particular nomenclature or that the individual be a corporate officer. However, there is no such requirement in Quebec. In Quebec, the *Charter of the French Language* may impose language requirements when communicating with consumers. Unlike the European Union's General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR") which provides extensive guidance for the position of a data protection officer, PIPEDA and the privacy laws of British Columbia and Alberta do not describe the duties of a Privacy Officer.

13.4. Application to Digital Advertising

Organizations must designate an individual who is responsible for privacy compliance. The contact information must be made available upon request.

14. SELF-REGULATION

14.1. Overview

Are there any industry-self regulatory schemes in place in the jurisdiction?

The Digital Advertising Alliance of Canada ("DAAC") launched a self-regulatory program for OBA to assist companies with their compliance obligations under Canadian Privacy Laws. The DAAC program is based on the Digital Advertising Alliance's program in the US.

Are there any signal-based programs used in the territory to assist with digital advertising compliance?

14.2. Application to Digital Advertising

The Principles apply to the collection of data over time and across multiple websites and/or apps for the purpose of using such data to predict web and/or app user preferences or interests to deliver online advertising in the Canadian online advertising ecosystem based on the preferences or interests inferred from such web and/or app viewing behaviors. The Principles include separate provisions for First Parties, Third Parties, and Service Providers that engage in OBA. Therefore, different Principles and different types of notice and choice may be applicable to each type of company and activity. The Principles do not apply to viewing behavior for a particular website and/or app, nor do they apply to contextual advertising (i.e., advertising based on the content of the webpage and/or app being visited, a consumer's current visit to a webpage, app, or a search query) or Ad Delivery. To the extent Ad Delivery and Ad Reporting (as defined by the Principles) include the collection or use of Personal Data, independent requirements under the Canadian Privacy Statutes may apply.

15. PENDING PRIVACY BILLS

15.1. Overview

The federal government and several provincial governments have signaled their intention to modernize their privacy legislation.

In February 2020, the B.C. government began a statutory review of the *Personal Information Protection Act*. The Office of the Information and Privacy Commissioner for British Columbia, along with other stakeholders, has put forth recommendations which include mandatory reporting requirements in the event of a cybersecurity breach.

In June 2020, the Quebec National Assembly tabled Bill 64 to modernize its privacy legislation. If Bill 64 is enacted, it would create a private-sector privacy statute in that province that is substantially similar to the GDPR.

In August 2020, the Ontario government launched a consultation on privacy law reform, with a view to implementing a provincial act regulating privacy in the private sector (and possibly other sectors like non-profits and charities). Currently, Ontario only has privacy laws that regulate the public and health sectors, though private-sector organizations in Ontario remain subject to the PIPEDA.

In November 2020, the federal government introduced the *Digital Charter Implementation Act, 2020*, which if enacted would repeal the parts of the PIPEDA that regulate the processing of personal information and enacting a new *Consumer Privacy Protection Act*.

15.2. Application to Digital Advertising

While C-11 remains a Bill that is subject to amendment, the following key issues in the proposed Bill may affect the digital advertising industry:

- **De-identification**: Bill C-11 includes de-identified information within the scope of privacy protections. The policy behind the provision is that technologists argue that it is no longer possible to anonymize information in the sense of making it impossible to trace the information back to an individual.
- **Cross-border data transfers**: Bill C-11 confirms the requirement in PIPEDA to ensure that the transfer of personal information to a service provider abroad is subject to the same level of protection.

iab.

China

Cross-Jurisdiction Privacy Project

1. THE LAW

1.1. Overview & Key Acts, Regulations, and Directives

China's data protection laws are in a period of change and there has been significant progress in the field of data protection legislation. A number of new laws have recently been enacted or will come into effect in 2021 including, most significantly, a draft comprehensive law governing the processing of personal information ("***Draft PIPL***"). This guidance document discusses generally applicable data protection requirements rather than sector-specific laws and regulations (such as requirements that govern telecommunications, finance and healthcare, etc.). It discusses data protection requirements in China as they stand today, as well as new laws that are expected to come into effect in 2021.

1.2. Key Acts, Regulations, and Directives

There is currently no single, comprehensive law that addresses data protection in China[1]. However, there are a number of different laws that, taken together, cover many of the individual components of a data protection regime. The laws and regulations governing data protection in China today include (with an asterisk notation included for those likely applying to digital advertising):

- *Civil Code of the People's Republic of China* (available in English here) (***"Civil Code"***).*
- *Cybersecurity Law of the People's Republic of China* (available in Chinese here and an unofficial English version available here) (***"CSL"***).*
- *Advertising Law of the People's Republic of China* (available in Chinese here and an unofficial English version available here) (***"Advertising Law"***).*
- *E-Commerce Law of People's Republic of China* (available in Chinese here and an unofficial English version available here) (***"E-Commerce Law"***).*
- *People's Republic of China's Criminal Law* (available in Chinese here and Amendment 9 here, and an unofficial English version available here) (***"Criminal Law"***).

Civil Code

The *Civil Code of the People's Republic of China* (***"Civil Code"***) became effective on January 1, 2021. The Civil Code is a comprehensive piece of law and addresses a variety of rights, including an express right to privacy and the protection of personal information (in Chapter VI of Part IV "Personality Rights").

[1] Please note that this guidance does not cover Hong Kong, Macau, or Taiwan, as these jurisdictions have their own data protection rules.

The provisions relating to the right to privacy and the processing of personal information are separate but may be overlapping. The Civil Code defines privacy as the "undisturbed private life of a natural person and his private space, private activities, and private information that he does not want to be known by others." It contains specific provisions relating to the right to privacy and the processing of "private information."

The Civil Code also regulates the processing of personal information more broadly, which includes the activities of collecting, storing, using, refining, transmitting, providing, and disclosing personal information. Moreover, the Civil Code adds three types of information to the definition of personal information under the CSL–email address, health information, and location information.

The Civil Code establishes the principles and conditions to lawfully process personal information in China and creates certain rights for individuals, such as the rights of access, correction, and deletion. It also requires "personal information processors" to implement technical and other necessary measures to ensure the security of personal information and protect information from data breaches. Personal information processes are prohibited from falsifying personal information or unlawfully providing personal information to others. The Civil Code generally requires consent to process personal information but provides certain exceptions when allowed by relevant laws and regulations.

Please see Section 2.1.1 for more information about the Civil Code and Section 3.7 for more information about the standard of consent.

Cybersecurity Law

The *Cybersecurity Law of the People's Republic of China* (***"CSL"***) became effective on June 1, 2017. It applies to all companies that operate a computerized information network system in China. CSL contains a data localization requirement, under which operators of critical information infrastructure ("CIIO") may not transmit "critical data" or "personal information" that they collect or generate within China in the course of operating their business to a destination outside of China, unless they first undergo (and pass) a security assessment.

CSL also sets out data protection requirements for "network operators." A "network" is defined broadly to include the internet, intranets, and industrial control systems–ultimately, any website or app that collects and processes personal information falls within the scope of CSL. Under CSL, network operators are subject to notice and consent requirements in respect to the collection and use of personal information, as well as requirements to comply with the principles of legitimacy, rightfulness, and necessity.

Network operators are also prohibited from providing personal information to third parties without the individual's consent, except in cases where personal information is depersonalized in such a way that it cannot identify the individual and the depersonalization cannot be reversed. When personal information has been disclosed due to a breach, or has been destroyed or lost, the network operator must promptly notify the individuals and report to

the relevant government agencies. The administrative penalties under CSL may include warnings, orders to rectify violations, fines, orders to suspend operations, and even revocation of business permits or licenses. At the time of writing, certain provisions of CSL still await clarification by way of implementing regulations or other rule-making.

Please see Section 2.1.2 for more information about CSL and Section 3.7 for more information about the standard of consent.

Advertising Law

The *Advertising Law of the People's Republic of China* (***"Advertising Law"***) became effective on September 1, 2015. On July 4, 2016, the State Administration for Industry and Commerce issued the *Interim Measures for the Administration of Internet Advertising* (***"Internet Advertising Measures"***).

Together, the Advertising Law and Internet Advertising Measures govern advertising activities conducted over the internet in China (for example, to address fairness and truthfulness in advertising). They do not specifically regulate data protection practices or the processing of personal information and are instead primarily focused on the content of advertising. For example, under the Internet Advertising Measures internet advertisements should be identifiable and clearly marked as an "advertisement" so that consumers can identify them as such. However, there are certain provisions relating to the form of advertising which may be relevant in the context of digital advertising.

Please see Section 2.1.3 for more information about the Advertising Law.

E-Commerce Law

The *E-Commerce Law of the People's Republic of China* (the ***"E-Commerce Law"***) became effective on September 1, 2019. It contains requirements regarding the protection of personal information in the e-commerce sector. E-commerce is defined as the "sale of goods or provision of services through the Internet or other information networks" (Article 2).

The E-Commerce Law applies to "e-commerce operators," which include e-commerce platform operators (e.g., Taobao or Jing dong), in-platform operators (e.g., online sellers of Taobao), and other operators that sell goods or services via self-built websites or other network services (e.g., via a public WeChat account in China). There are exceptions for financial and media products. The E-Commerce Law requires e-commerce operators to comply with the personal information protection requirements of other laws when processing their users' information. It also provides users with certain rights around their personal information.

Please see Section 2.1.4 for more information about the E-Commerce Law.

Criminal law

The Ninth Amendment to the *People's Republic of China's Criminal Law* (promulgated on August 29, 2015)

(***"Criminal Law"***) provides that all parties that sell or provide personal information to a third party in violation of the law may be subject to criminal liability, and that parties that sell or provide personal information obtained while providing services in violation of law may be subject to heavier punishment.

Hierarchy of laws

The Civil Code operates at a higher, more authoritative level and therefore takes precedence over the other laws discussed in this guidance. To be clear, the other laws continue to operate as valid law, but the requirements of the Civil Code will prevail in the event of any conflict.

In terms of the other laws, CSL, Advertising Law and E-commerce Law operate on the same level and we understand there should be no real conflict among these laws: the Advertising Law focuses on the content of advertisements (rather than personal information protection), while the E-Commerce law just supplements the requirements of CSL in the e-commerce sector (e.g., it gives users the right to cancel their account). This means that e-commerce operators must comply with the laws and regulations governing personal information protection when collecting and using personal information of their users.

1.3. Guidelines

App Operators

The Cyberspace Administration of China, Ministry of Industry and Information Technology, Ministry of Public Security and State Administration of Market Regulation have issued two sets of guidelines for app operators:

- *Announcement Launching a Special Crackdown Against Illegal Collection and Use of Personal Information by Apps* (only available in Chinese here) (***"Announcement for App Operators"***)
- *Measures for the Determination of the Collection and Use of Personal Information by Apps in Violation of Laws and Regulations* (only available in Chinese here) (the ***"Measures for App Operators"***).

The Announcement for App Operators set out how app operators should behave when they collect personal information online, and the Measures for App Operators clarify the kinds of behavior that will be considered unlawful under the Announcement. The Measures for App Operators are deemed binding rules for app operators.

Based on these guidelines, China also developed a working group called the Personal Information Protection Task Force on Apps which is charged with app privacy inspection and enforcement.

Please see Section 3.7 for more information about the standard of consent.

Children

On August 22, 2019, the Cyberspace Administration of China issued the *Measures on the Online Protection of Children's Personal Data* (***"Children's Measures"***). The Children's Measures provide further clarity around the

protection of children's personal data under CSL. They define a child as any person under 14 years of age. While they are often referred to as "China's COPPA," they have a broader scope than their US counterpart and include more prescriptive requirements that are designed to safeguard children's data online. The Children's Measures are deemed binding rules published by the Cyberspace Administration of China.

National Standards

Finally, there are also a number of national standards, such as the *Information Security Technology - Personal Information Security Specification* (***"Information Security Standards,"*** only available in Chinese here). These standards are recommended only and are not binding or enforced mandatorily.

1.4. Case Law

China is a civil code jurisdiction and therefore cases are not binding (they are useful for reference only). There are no recent cases relevant to digital advertising.

1.5 Application to Digital Advertising

China's current mandatory laws and regulations apply to digital advertising as follows:

- The **Civil Code's** personal information section applies to all personal information processing activities in China-including digital advertising. The Civil Code operates at a higher, more authoritative level than other the laws discussed in this guidance and therefore takes precedence.
- **CSL** applies to network operators within the context of digital advertising-for example, publishers, advertisers, advertisement operators, and agents that build, use, and/or maintain networks in China (i.e., Chinese domain name, language, ICP).
- The **Advertising Law** is primarily focused on the content of advertising rather than the form of advertising or privacy per se. However, it contains a very general requirement that the law also applies to advertising conducted over the internet and specific form requirements relating to pop-up advertisements.
- The **E-Commerce Law** applies to digital advertising that appears on e-commerce platforms websites. Depending on the scenario, therefore, e-commerce operators may be publishers, advertisers, and advertising operators.
- The **Criminal Law** applies to anyone (including organizations and persons in any sector) that seriously violates Chinese laws-including organizations that illegally collect, share, or sell personal information without individuals' consent.

As summarized above, China has at least five laws of general application that apply in certain circumstances to the way personal information is used for digital advertising. Taken together, and as a practical matter, these laws require operators of digital properties (like websites and mobile apps) to take the following steps:

1. Disclosure Requirements--end users must receive notice of the digital property's own relevant digital advertising activities before personal information is collected. For a website, notice may be provided in a privacy policy linked from the website. For an app, the notice must be explicit and provided when the user first downloads and uses the app. The app should display a pop-up that contains the main content of privacy policy, and additional pop-ups when the privacy policy is changed substantially. These requirements are attributable to the Civil Code and CSL. Please see Section 3.7 for how website and app operators comply with these requirements in practice in China.
2. Conditions for Processing--before using personal information for digital advertising, digital properties must obtain the user's consent to the processing of their personal information (unless the processing is otherwise required by laws and regulations). These requirements are attributable to the Civil Code and CSL. Generally speaking, consent for personal information processed through a website does not need to be expressed and may be implied. However, express consent is required for any processing of personal information by a mobile app. In addition, best practice favors obtaining express consent for websites as well.
3. Third Parties--the digital property must obtain consent to share personal information with third parties. This requirement is attributable to CSL.

The requirements summarized here are discussed in greater detail and specificity in the sections explaining each law below.

2. SCOPE OF APPLICATION

2.1. Who Do the Laws/Regulations Apply to and What Types of Processing Activities are Covered/Exempted?

2.1.1. Civil Code

The Civil Code applies to "personal information processors." The Civil Code does not clearly define a personal information processor but generally speaking any organization or person that processes personal information will be regarded as a personal information processor. The term "processing" refers to the activities of collecting, storing, using, refining, processing, transmitting, providing, and disclosing personal information. The concept of a personal information processor in China is therefore different to the concept of a "controller" or "processor" under the GDPR and not determined by whether the organization or person determines the purposes and means of processing.

The Civil Code is an amalgamation of existing civil and tort-related laws and regulations and certain judicial interpretations that covers many aspects of civil society, including privacy, contracts, and torts. The right to privacy, previously recognized in the Tort Law of 2009, is expressly codified as one of the "rights of personality."

The Civil Code governs both the right to "privacy" and the processing of "personal information" more broadly.

These are separate concepts under the Civil Code.

The Right to Privacy

The right to privacy refers to the "undisturbed private life of a natural person and his private space, private activities, and private information that he does not want to be known to others."

Under Article 1033 of the Civil Code, no organization or individual shall:

- Intrude upon another person's private life through making phone calls, sending text messages, using instant messaging tools, sending emails and flyers, or similar means.
- Process a person's private personal information (i.e., information people do not wish to disclose).

without the person's **express consent** or where otherwise provided by law.

Processing of Personal Information

Under Article 1035 of the Civil Code, personal information processors must obtain **consent** to process a person's personal information unless otherwise provided by law. In addition, under Article 1036, an actor does not bear civil liability for processing personal information where they have reasonably performed an act that the natural person consented to.

The provisions relating to privacy and personal information may overlap in certain cases. The Civil Code states that the rights relating to privacy take precedence and, where applicable, apply preferentially to "private personal information". Otherwise, the provisions relating to personal information apply.

Currently, and in the absence of further guidance and cases, it is unclear whether consent or express consent is required in the context of digital advertising. Arguably, under the Civil Code, consent will suffice for the purposes of digital advertising (i.e., display advertising) and expressed consent is required in order to send marketing emails or text messages, make marketing phone calls, or send marketing through other equivalent means. However, it is unclear whether in certain contexts digital advertising could involve "private information", especially as private information may overlap with personal information in certain cases. For example, when a person reads a book online, they may not want anyone to know what they are reading, especially if the book can reflect characteristics about the person (such as their mental health or a mental illness).

Please see Section 3.7 for more information on the standard of consent under the Civil Code.

2.1.2. Cybersecurity Law

CSL applies to "network operators" and "critical information infrastructure operators."

- According to Article 76, "network operators" include owners and managers of networks as well as network

service providers. In practice, a "network" is defined broadly to include the internet, intranets, and industrial control systems–ultimately, therefore, any website or app that collects and processes personal information falls within the scope of CSL. This will include publishers (websites, mobile apps, etc.), advertisers (brands, agencies, etc.), and intermediaries (DSPs, SSPs, etc.). The concept of a "network operator" is distinct from the concept of a "controller" or "processor" under the GDPR in that the definition is not based on determining the means or purposes of processing.

- According to Article 31, "critical information infrastructure operators" ("CIIOs") operate in important industries and fields, such as public communication and information service, energy, communications, water conservation, finance, public services, and e-government affairs, as well as key information infrastructures that may endanger national security, people's livelihood, and public interest in the event of damage, function loss, or data breach.

CSL governs all kinds of cyber security matters, including the security of personal information online. It consists of seven chapters-General Provisions; Support and Promotion of Cyber Security; Security of Network Operation; Security of Network Information; Monitoring, Early-warning, and Emergency Response; Legal Liability; and Supplementary Provisions.

If an organization falls into the definition of network operator, the cyber security sections of CSL apply (such as the obligations to grade the classification of cyber security and to formulate and exercise a cyber security emergency response plan). In addition, to the extent the organization collects and uses personal information, then the personal information sections of CSL will also apply.

If an organization is a CIIO, the security of critical information infrastructure operation section will apply (such as the obligations of data localization and data cross-border transmission).

CSL describes two major legal bases for processing personal information: (1) the user's consent; and (2) legal obligations. There are other possible legal bases under CSL, such as public interests and the individual's vital interests, but these are not well fleshed out in the law.

In addition, under Article 42 the user's agreement is required to disclose their personal information to another party, except where the information has been de-identified so that it is impossible to identify the user and the user cannot be re-identified.

Please see Section 3.7 for more information on the standard of consent under CSL.

2.1.3. Advertising Law

The Advertising Law applies to commercial advertising activities in which commodity operators or service providers

directly or indirectly introduce the commodities or services they promote. It covers advertising through any means, including email marketing, telephone marketing, apps, and other forms of digital advertising. The Advertising Law applies to (1) "advertisers"; (2) "advertisement publishers"; (3) "advertising agents"; and (4) "endorsers."

Although the law applies to advertising over the Internet, it does not contain any provisions that specifically regulate or are clearly relevant to digital advertising. The most notable requirements are:

- Under Article 43, organizations and individuals may only send advertisements to individuals at their address or vehicle, through electronic means or otherwise, either at the request of or with the consent of the individual concerned. Where advertisements are sent by electronic information, the sender's true identity, and contact information must be clearly indicated and the recipient must be provided with a way to opt out from receiving further marketing.
- Under Article 44, pop-up advertisements must conspicuously indicate a close mark that permits the advertisement to be closed with one click. The law does not clearly define "pop-up," but it is generally understood to include advertisements that are displayed via a pop-up GUI.

These rules therefore relate to direct marketing and formatting requirements for certain types of online advertising, but do not clearly pertain to privacy or personal information in the context of digital advertising and display advertising.

There are additional requirements under the *Internet Advertising Measures*. For example, if the same device logs in to the same website (including the top-level domain name and its subdomains) within 24 hours, the website should provide the user with the option to temporarily block all pop-up advertisements on the website. For emails containing advertising, opt-out functions should also be provided (e.g., unsubscribe links, an option to enter the words such as "TD" to refuse messages) and marketing whitelists should also be maintained.

2.1.4. E-Commerce Law

The E-Commerce Law applies to "e-commerce operators", which are defined as "natural persons, legal persons or unincorporated organizations that engage in the operational activities of selling goods or providing service through the Internet and other information networks" (Article 9).

This includes "e-commerce platform operators" (i.e., e-commerce operators that provide online platforms, transaction matching, and other services to parties in an e-commerce transaction, such as Taobao and Jing dong), "in-platform operators" (i.e., e-commerce operators that sell goods or services through an e-commerce platform, such as sellers on Taobao), and other e-commerce operators that sell goods or services via self-built websites or other network services (such as via a public WeChat account). There are some notable exceptions to the law, including: "financial products and services, or services providing news and information, audio and video programs, publication and cultural products through information networks" (Article 2).

The E-Commerce Law requires e-commerce operators to comply with the personal information protection requirements of other laws, and specifically requires e-commerce operators to comply with the Advertisement Law when sending advertisements to their users. In addition:

- Under Article 24, users have the right to access, correct, and delete their information and cancel their account.
- Under Article 18, when an e-commerce operator provides a user with search results relating to commodities or services based on the consumer's hobbies, consumption habits, or any other traits, the e-commerce operator must also provide the consumer with other options not targeting their identifiable traits at the same time.
- An e-commerce platform operator must implement technology, organizational and other necessary measures to ensure the security of personal information and must implement a cyber security emergency response plan (similar to the requirement under CSL).

Information about goods, services, and transactions must be retained for at least three years from the date of the transaction, unless otherwise provided by any law or regulation.

2.2. Jurisdictional Reach

Any organization that operates in China will be governed by China's laws and regulations. The position for non-Chinese companies is more complicated, as different laws have different requirements, but in general most of China's current laws apply to personal information processing activities within the territory of China (whether the organization is based inside or outside China).

In practice, if a website uses a Chinese domain name or has an Internet Content Provider (ICP) filing or license in China, or an app can be downloaded from app stores within China, then Chinese authorities will likely consider the processing activity to take place in China and therefore the laws of China will apply. By contrast, if a global website does not use servers based in China or a Chinese domain, or offer services in Chinese languages or currency, then Chinese authorities will not likely consider the processing activity to take place in China.

Laws	Regulates	Jurisdictional reach
Civil Code	Civil activities and personal and proprietary relationships between people (including natural and legal persons). Also governs privacy and personal information processing in China*.	Processing within the territory of the People's Republic of China
CSL	The construction, operation, maintenance, and use of networks, as well as the supervision and management of network security, including network information security.	Processing within the territory of the People's Republic of China
Advertising Law	Commercial advertising activities in which commodity dealers or service providers directly or indirectly introduce goods or services via certain media and in certain forms.	Processing within the territory of the People's Republic of China
E-Commerce Law	E-commerce activities, i.e., business activities relating to the sale of goods or providing services through the Internet or other information networks.	Processing within the territory of the People's Republic of China

* Privacy is different from personal information under the Civil Code. Privacy refers to the undisturbed private life of a natural person and his or her private space, private activities, and private information that he does not want to be known to others.

2.2.1 Application to Digital Advertising

Scenario 1 (The baseline): A user residing in China (determined by IP address or geo identifier) goes onto a Chinese domain and is served an ad by a Chinese advertiser. The advertiser uses the user data to build a user profile.

Please see response in Scenario 2.

Scenario 2 (User outside China): A Logged-on/signed-in user, known by the publisher to be a Chinese resident, goes onto a Chinese domain but the user's IP address or geo identifier indicates the user is outside China. A Chinese advertiser serves an ad and uses the user data to build a user profile.

China's privacy laws and regulations will likely apply in Scenarios 1 and 2, regardless of the location of the user. The processing takes place in China. This is true of the publisher's legal obligations and the advertiser's legal obligations.

The Draft PIPL will apply to all processing of personal information that takes place within the territory of China, regardless of the location of the data subject's nationality or the PI Processor. The Draft PIPL will also confer extraterritorial applicability to processing that is conducted outside China if the purpose is to provide products or services to data subjects located in China, or for analyzing and evaluating the behavior of such data subjects. Please see Section 16.1(b) "Extraterritorial Jurisdiction" for more information on the extraterritorial applicability proposed under the Draft PIPL.

Laws	Applies?
CSL	Yes, to the advertiser
Civil Code	Yes, to the advertiser
Advertising Law	Yes, to the advertiser
E-Commerce Law	Yes, to the advertiser
Draft PIPL	Yes, to the advertiser and also to the publisher if the domain is designed for the purposes of providing products or services to data subjects located in China, or analyzing and evaluating the behavior of such data subjects.

- **Q1: Does the answer change if the site hosts content aimed at Chinese residents (e.g., a news aggregator with a section on Chinese current affairs)?**

  No. Under China's current laws, even if the site targets Chinese residents the processing will be deemed to take place outside of China because the site's domain is outside of China. China's current laws only apply to processing that takes place in China. Therefore, China's current privacy laws and regulations will not likely apply to the publisher but will likely apply to the advertiser.

  The position is different under the Draft PIPL. Here, the Draft PIPL will likely apply to the publisher. The Draft PIPL will confer extraterritorial applicability where the purpose of the processing is to provide products or services to data subjects located in China. Please see Section 16.1(b) "Extraterritorial Jurisdiction" for more information on the extraterritorial applicability proposed under the Draft PIPL.

- **Q2: Does the answer change if the advertiser is based outside of China?**

  Yes. China's current laws will not likely apply to the advertiser if the advertiser is based outside China (and its servers are also located outside China).

  The Draft PIPL will likely apply to the advertiser if the purpose of the advertising is to provide products or services to data subjects located in China. Please see Section 16.1(b) "Extraterritorial Jurisdiction" for more information on the extraterritorial applicability proposed under the Draft PIPL.

Scenario 4 (Advertiser outside China): A user residing in China (determined by IP address or geo identifier) goes onto a Chinese domain and is served an ad by an advertiser based outside China. The advertiser uses the user data to build a user profile.

China's privacy laws and regulations will likely apply in Scenario 4, regardless of the fact the advertiser is located outside China. This is true of the publisher's legal obligations and the advertiser's legal obligations. This is because the processing will likely be deemed to take place in China. If the advertiser builds the user profile using servers located outside China, then China's privacy laws and regulations may technically not apply to that profiling activity. Moreover, despite the legal position Chinese regulators are more likely to regulate the activities of companies in China.

The Draft PIPL will also apply to the publisher but it is unclear whether it will apply to the advertiser. Please refer to Section 16.1(b) "Extraterritorial Jurisdiction" for further info regarding the extraterritorial applicability proposed under the Draft PIPL.

Laws	Applies?
CSL	Yes
Civil Code	Yes
Advertising Law	Yes
E-Commerce Law	Yes
Draft PIPL	Yes, to the operator of the Chinese domain (i.e., the publisher). But it remains unclear as to whether the Draft PIPL applies to the advertiser based outside China.

- **Q1: Does the answer change if the advertiser has an affiliate/group company based in China?**

  No. However, under the Draft PIPL if such affiliate/group company is the designated representative of the foreign advertiser, we could not exclude the possibility where such affiliate/group company might potentially face penalties for violations of personal information protection obligation by the personal information processor it represents. Please see Section 16.1(b) "Extraterritorial Jurisdiction" for more information.

3. DEFINITIONS

3.1. Collect

There is no definition of "collect" under China's current mandatory laws and regulations. However, under the Information Security Standards "collect" refers to obtaining control of personal information.

China's laws do not make a direct distinction between the entity that collects personal information and an entity that does not directly collect personal information but processes it, since both activities will be caught by the relevant requirements. However, under Article 42 of CSL, consent is required to disclose personal information to another party. This indicates that if an entity obtains personal information indirectly through another entity, this data sharing must be agreed to by the individual.

- **"When a publisher allows an ad tech company's pixel on its page, who is deemed to "collect" personal**

information and incur legal obligations (e.g., controller/co-controller obligations under GDPR or "business" obligations under CCPA)–the publisher, the ad tech company or both?"

China's current mandatory laws and regulations do not distinguish (in terms of legal obligations) between the entity that directly collects personal information and an entity that indirectly collects (or receives) personal information. Equally, there is no concept of "controller" or "co-controllers." This means that any organization that collects personal information, whether directly or indirectly, will be subject to the obligations under Chinese laws and regulations. So, the ad tech company will be subject to the legal obligation regarding personal information first and, if it shares the personal information with the publisher, the publisher will also be subject to the legal obligations when it receives the personal information.

The Information Security Standards do contain the concept of a "personal information controller" and "joint controllers" that have a similar meaning to "data controller" and "joint controllers" under GDPR. We understand if an ad tech company and the publisher jointly decide the purposes and manners of personal information processing, then the ad tech company and publisher shall be deemed "joint controllers" under the Information Security Standards. However, the Information Security Standards are national standards and are not mandatorily enforced in China.

Please see Section 3.6 for more information about how Chinese laws apply, and the practical consequences for, companies that directly collect personal information and companies that indirectly collect personal information.

3.2. Data Processing (i.e., collecting, capturing, retaining, recording, organizing, structuring, storing, altering, retrieving, consulting, using, disclosing, transmitting, disseminating, making available, aligning, combining, restricting, erasing, destroying, or otherwise processing)

Under the Civil Code, "processing" refers to the "collection, storage, use, refinement, transmission, provision, disclosure, and the like, of personal information." The definition is therefore broad and covers most uses of personal information. There is no definition of processing under CSL.

3.3. Personal Information

Under the Civil Code, personal information refers to "information recorded electronically or in other ways that can be used, by itself or in combination with other information, to identify a natural person, including the name, date of birth, identification number, biometric information, residential address, telephone number, email address, health information, whereabouts, and the like, of the person."

The definition of personal information under CSL is essentially the same and the definition under the Draft PIPL does not appear to be materially different from the definition under the current laws.

For the purposes of this guidance (and Section 3.3), we apply the definition of personal information under the Civil Code but, if applicable, indicate where there may be a notable difference under CSL and/or other laws.

Type of Information Collected	Does this Category Independently Constitute Personal Information? (Yes/No)	Qualifying Notes (if any)
IP Address	Yes	Listed in Annex A.1 of the Information Security Standards
Mobile Advertising IDs (IDFA, AAID)	Yes	Listed in Annex A.1 of the Information Security Standards
Consumer identifiers such as: • User device ID • Publisher persistent ID/Cross-publisher cookie ID • Household ID	Yes, if the consumer identifier is unique (see below)	User device ID is listed in Annex A.1 of the Information Security Standards
Hashed identifiers such as: • Hashed email • Hashed IP address	No	
User Agent such as: • Character string identifying the application • Operating system • Browser information, vendor, and/or version of the requesting user agent	No	

Device Information such as: • Type, version, system settings, etc.	Yes, if the information reveals a unique fingerprint of the device	Listed in Annex A.1 of the Information Security Standards
Website Information such as: • Name • URL, etc.	No	
Advertisement Information such as: • Placement • Title • Creative ID, etc.	No	
Timestamps	No	
Metrics such as: • Counts • Amounts of time	No	
Event Data such as: (e.g., full URL including query string, referral URL)	No	
Precise geolocation (latitude, longitude)	Yes	Listed in Annex A.1 of the Information Security Standards
General geolocation (city, state, country)	No	

- **Are digital identifiers by *themselves* personal information (e.g., IDFA, cookie IDs, proprietary IDs, IP addresses, etc.)? Please provide context to the above chart.**

  Yes, digital identifiers are considered personal information by themselves under China's current laws to the

extent that the identifiers are unique to a particular individual (and therefore directly identify an individual). This may include, for example, IP address, mobile advertising ID, and user device ID. Whether a particular digital identifier is considered personal information by itself may change over time with technological developments.

Please note that there is no definition or concept of "pseudonymous" information under current Chinese laws. We understand that pseudonymization is a technical process that roughly corresponds to "de-identification" under the Information Security Standards, which involves making personal information unidentifiable when on its own and not combined with other information. By contrast, anonymization is a technical process to ensure that the individual cannot be re-identified from the information.

Under the Draft PIPL, "anonymization" refers to the processing of personal information in a manner such that it is impossible to identify specific individuals and also the identification is unable to be recovered. By contrast, "de-identification" is defined as processing of personal information such that it is impossible to identify specific individuals without the use of additional information. This means that unlike the anonymized data, the de-identified data can still be used to re-identify specific individuals with additional information.

- **If the answer to the above question is, "no," if a Company possesses a persistent digital identifier in Database 1 and has that same identifier in Database 2 with directly identifying information, does that render the pseudonymous information in Database 1 as personal information?**

  Yes. Under current Chinese laws and the Draft PIPL, a pseudonymous digital identifier (i.e., one that is re-identifiable in combination with other information) will be considered personal information. In this scenario, the digital identifier in Database 1 may be combined with the directly identifying information in Database 2 and therefore it will be considered personal information.

- **Is a Company's possession of a pseudonymous identifier plus other non-directly identifying data (e.g., age, gender, precise or imprecise geolocation, user agent string, timestamps) considered "personal information"?**

  No. Here, the company is not capable of re-identifying the individual because it merely possesses a pseudonymous identifier and other non-directly identifying data.

- **Is a Company's possession of a pseudonymous identifier "personal information" if it can hire a service provider or otherwise engage in a transaction with a third party where the identifier could be matched to the person, but the Company chooses not to hire such service provider or undertake such transaction. Is the mere fact that this service is potentially available to match to the person sufficient to render that pseudonymous identifier as "personal information"?**

Yes. Under a strict interpretation of current Chinese laws and according to the Draft PIPL, the pseudonymous identifier will be considered personal information because it may be combined with the directly identifying information held by the service provider or third party. However, in practice the company should not undertake privacy compliance unless and until it decides to hire the service provider or undertake the transaction that will enable re-identification.

- **What level of geolocation is personal information (precise vs. approximate)? Does it need to be associated with an identifier to be considered PI?**

  There is no clear answer under current mandatory Chinese laws or the Draft PIPL. If the geolocation information can be combined with other information to identify a natural person, then it will be considered personal information. According to Annex A of the Information Security Standards, precise geolocation data (which is considered personal information) includes latitude/longitude, tracking and accommodation information. There are no cases where this question has been considered or tested. Under the Draft PIPL, the information about personal whereabouts is defined as a form of sensitive personal information. However, there is no further explanation on what type of information constitutes personal whereabouts.

- **Is a household identifier personal information? (Consider: If a company has a residential IP address (household level ID) and multiple unique device IDs (e.g., MAIDs for every mobile device in the house) associated with that IP address, would that affect whether the household identifier is considered personal information?)**

  A household identifier may be considered personal information. Unlike CCPA, the definition of personal information under Chinese law only covers information relating to an identified or identifiable natural person. In some cases, information relating to a household could constitute personal information (for example, if an individual lives alone).

  In this scenario, if the company has multiple device IDs and a household identifier is associated with each of those device IDs, then to the extent the device IDs are considered personal information the household identifier will also be considered personal information (relating to each of the device IDs).

- **Is a hashed identifier personal information? (Consider: there are commercially available services that will take batches of emails encrypted using standard hashes and return (often a high percentage) of clear emails from them. Does that affect whether they are considered personal information, if all a company has to do is pay for the commercial service?)**

  Yes. Under a strict interpretation of current Chinese laws and according to the Draft PIPL, a pseudonymous identifier (including a hashed identifier) will be considered personal information because it may be combined with the directly identifying information held by the service provider or third party. However, in practice the company should not undertake privacy compliance unless and until it decides to

hire the service provider or undertake the transaction that will enable re-identification.

- **Is probabilistic information considered personal information?**

  Unclear.

  Neither does the Draft PIPL set out clear guidance on whether probabilistic information is considered personal information. If probabilistic information is a type of aggregated analytical data and does not link or direct to any specific individual, we are of the view that under the Draft PIPL, probabilistic information is unlikely to be considered as a form of personal information.

3.4. Sensitive Data

There is no concept of sensitive data under China's current mandatory laws and regulations.

Under the Information Security Standards, sensitive personal information refers to information vital to personal interests that once leaked, illegally provided, or misused, may endanger the individual's personal or property safety, or easily damage the individual's personal reputation, mental or physical health, or lead to discriminatory treatment. The Draft PIPL will introduce the concept of sensitive personal information (see Section 16).

3.5. Anonymized/De-identified/Pseudonymous Information

There is no definition of anonymized or pseudonymous information under China's current mandatory laws and regulations. However:

- According to Article 3.15 of the Information Security Standards, de-identification is the technical process of making personal information unidentifiable when it is on its own and not combined with other information. We understand that this is essentially equivalent to the technical process of pseudonymization.
- According to Article 1038 of the Civil Code, combined with Article 3.14 of the Information Security Standards, anonymous information is information that, after being processed, cannot be used to identify any specific individual, and cannot be restored to its original status.

Under the Draft PIPL, "anonymization" refers to the processing of personal information in a manner such that it is impossible to identify specific individuals, and also, the identification is unable to be recovered. By contrast, "de-identification" is defined as processing of personal information such that it is impossible to identify specific individuals without using additional information. The Draft PIPL sets higher standards for "anonymization" than "de-identification."

- **Is pseudonymous information considered personal information?**

  Yes. There is no definition or concept of pseudonymous information under current Chinese laws. However, information that is de-identified (i.e., you cannot identify the individual from the information on its own without further identifying information) is considered personal information.

Under the Draft PIPL, information that has been de-identified will also be considered personal information. Please refer to Section 16.1(c) "Definition" for more information regarding "Anonymization" and "De-identification" under the Draft PIPL.

- **Are persistent digital identifiers pseudonymous information (e.g., IDFA, cookie IDs, proprietary IDs, IP addresses, etc.)?**

  As stated above, there is no definition or concept of pseudonymous information under current Chinese laws. Whether a digital identifier is considered personal information by itself or only in combination with other information depends on the type of digital identifier. Please see responses in Section 3.3 for more information about digital identifiers.

- **Does the law subject pseudonymous information to fewer obligations than "regular" personal information?**

  No. Pseudonymous information (or de-identified information under current Chinese laws and the Draft PIPL) may still be used to identify a natural person and thus is still subject to the requirements that apply to personal information.

3.6. Data Controller and Processor

There is no equivalent definition of data controller or data processor under current Chinese mandatory laws and regulations. The Civil Code applies to "personal information processors," which include any organization or person that processes personal information. Equally, CSL applies to "network operators." Therefore, current Chinese mandatory laws do not distinguish between the entity determining the means and purposes of processing and an entity that merely acts on behalf of that entity.

The table below sets out the roles under China's mandatory laws and the Draft PIPL.

Law/mandatory rules	Applies to?	Obligations?
Civil Code	Personal information processors. This includes any organization or person that processes personal information, such as publishers, advertisers, and intermediaries.	Any organization that collects and processes personal information must comply with the obligations under the Civil Code (e.g., provide notice, obtain consent, etc.). This includes organizations that have a direct relationship with the user (i.e., the publisher) and organizations that do not have a direct relationship with the user but collect personal information indirectly (i.e., the advertiser or ad tech intermediary).

CSL	Network operators and CIIOs. This includes any website, app or online service that collects and processes personal information, such as publishers, advertisers, and intermediaries.	Any party that collects and processes personal information, whether directly or indirectly, must comply with the obligations under CSL (e.g., provide notice, obtain consent, etc.).
E-Commerce Law	E-commerce operators (including e-commerce platform operators, in-platform operators and other operators that provide products and/or services via a self-built website or other network service). This includes any publisher or advertiser that provides an e-commerce platform or offers products or services through a self-built platform.	User device ID is listed in Annex A.1 of the Information Security Standards
Measures for App Operators	App operators This includes any publisher that provides an app.	Any app operator, to the extent the app can be downloaded in app stores in China, must comply with the obligations under the Measures for App Operators (e.g., provide notice and obtain explicit consent).

Draft PIPL	PI Processor This includes any organization or person that processes personal information and determines the purposes and means of processing. Entrusted party is the party that processes personal information on the basis of the entrusted arrangement with the PI Processor.	Any organization or person that processes personal information and determines the purposes and means of processing must comply with the obligations under the Draft PIPL. The concept of PI Processor is similar to the concept of the data controller under GDPR. Under the current draft of the law, the PI Processor is required to enter into an agreement with an **entrusted party** (similar to the concept of a data processor under GDPR). An entrusted party must ensure the security of the processed personal information and shall bear certain obligations set out under the Draft PIPL. Please refer to Section 16.1(h) for more details on entrusted arrangements under the Draft PIPL.

The Information Security Standards do contain the concept of a "personal information controller" and "joint controllers" that have a similar meaning to "data controller" and "joint controllers" under GDPR. The Information Security Standards require, in the case of indirect collection, that:

1. The personal information controller should require the personal information provider to explain the source of the personal information and verify the lawfulness of such source.
2. The personal information controller should understand the scope of consent the personal information provider has obtained to process the personal information (including the purposes of use and whether the individual has authorized the transfer, sharing, public disclosure and deletion of such information).
3. If the processing activity goes beyond the scope of the consent obtained, the personal information controller should obtain consent from the individual (either by itself or through the personal information provider) within a reasonable time after obtaining the personal information or before processing the information for that purpose.

We understand if an ad tech company and the publisher jointly decide the purposes and manners of personal information processing, then the ad tech company and publisher shall be deemed "joint controllers" under the Information Security Standards. However, the Information Security Standards are national standards and are not mandatorily enforced in China.

In practice, where an organization does not have a direct relationship with the user and only collects personal information indirectly (e.g., an ad tech intermediary or advertiser) then we understand they should provide a privacy notice on their website and ask the third party that has a direct relationship with the user to take responsibility to obtain consent from the individual and provide notice. These obligations should be contained in the parties' contractual terms.

However, this obligation may not be relevant if the organization does not actually collect or process the personal information. For example, an advertiser may not collect or obtain the personal information from the publisher, they may just want to know the effectiveness of advertisements and measure ad performance, and may therefore only receive statistical, anonymous data.

The Draft PIPL will introduce the concept of a PI Processor (see Section 16). However, this is different to the concept of a "data processor" under GDPR and, in fact, is more like a "data controller" under GDPR (i.e., the party that decides the purpose and manners of processing). The Draft PIPL also includes an entrusted arrangement for processing of personal information: the entrusted party must process personal information on the basis of the entrusted arrangement with the PI Processor. Please refer to Section 16.1(h) for more details on entrusted arrangements under the Draft PIPL.

3.7. Other Definitions

Profiling: There is no equivalent concept of profiling under current Chinese mandatory laws or under the Draft PIPL. The Information Security Standards include the concept of "profiling" as analyzing, predicting, and modelling the personal characteristics of a particular natural person (such as occupation, financial status, health status, education, personal preferences, credit records and behavior) by collecting, gathering and analyzing the person's personal information.

Automated Decision Making: There is currently no equivalent concept of automated decision making under current Chinese mandatory laws. The Draft PIPL will introduce the concept of automated decision making, which will refer to the use of personal information to automatically analyze, evaluate, and make decisions through computer programs based on personal behavior and hobbies, or economic, health, and credit status.

Consent: There is no definition of consent under Chinese law. Generally speaking, consent in China does not need to be express and a lower standard of consent is tolerated-this means that consent can be opt-in, opt-out or implied (all are acceptable forms of consent). For example, on a website consent does not require any affirmative user action and implied consent (i.e., "by using this website, you agree to our privacy policy and cookie policy") is currently acceptable. However, please note that the Measures for App Operators require mobile apps to obtain

explicit consent to the app's privacy policy and the mobile phone's permissions. For the standard of consent under different laws, please see the table below.

Law/Guidance	Standard of consent
Civil Code	Consent is required to process personal information. There is no clear standard for consent under the Civil Code and we understand **both express or implied consent are allowed.** * Express consent is required to process "private personal information" (different from general personal information under the Civil Code). However, in the absence of further guidance or cases, it is not clear whether express consent is relevant in the context of digital advertising.
CSL	Consent is a lawful basis to process personal information and is required to share personal information with third parties. Article 41 of CSL requires that consent be "informed" but otherwise there is no clear standard for consent, and we understand **both express or implied consent are allowed**.
Measures for App Operators	**Explicit consent** to the privacy policy is required for mobile apps. In practice, app users are presented with a pop-up that asks them to explicitly agree to the privacy policy.
Draft PIPL	Consent is required to process personal information. Consent must be fully informed and **freely and unambiguously given**. The Draft PIPL provides more clarity on the "informed consent" principle. However, it remains unclear as to whether this requirement is equivalent to explicit consent. This is expected to be further clarified by the PRC regulators. The Draft PIPL will also require **specific/written consent** in certain circumstances, including to process sensitive personal information, to share personal information with third parties, and to transfer personal information outside China.

Apart from China's mandatory laws, the Information Security Standards provides some guidance on the definition of consent and explicit consent.

- According to Article 3.7 of the Information Security Standards, **consent** refers to a behavior whereby a data subject expressly authorizes the specific processing of their personal information, including through a positive act (i.e., opt-in) or through a passive act (i.e., implied).
- According to Article 3.6 of the Information Security Standards, **explicit consent** refers to a behavior whereby a data subject explicitly authorizes the specific processing of their personal information through a written statement, electronic means, an oral statement, or through an affirmative action of their own willing. Affirmative action includes situations where a data subject checks or clicks "agree," "register," "send," "dial," "fills in a form," or provides their personal information on their own volition. Opt-in or opt-out are both considered as explicit consent.

  There is no concept of implied consent under the Information Security Standards.

  Please see Section 4 for further information on consent.

4. DATA CONTROLLER RIGHTS AND RESPONSIBILITIES

4.1. Overview

The obligations regarding notice and consent under the Civil Code and CSL are discussed elsewhere in this guidance. Otherwise, Article 41 of CSL also requires network operators to:

- Follow the principles of legality, fairness, and necessity.
- Provide a privacy notice that explicitly indicates the purposes, means, and scope of the collection and use of the personal information.
- Obtain the consent of the individual whose personal information is collected.

4.2. Accountability

4.2.1. Overview

Although there is no equivalent to GDPR "accountability" concept under Chinese law, Article 1035 of the Civil Code lays out some basic accountability principles, including that personal information must be processed in compliance with the principles of lawfulness, justification, and within a necessary limit. Article 41 of CSL also requires network operators to follow the principles of lawfulness, justification, and minimization, and provide notice of the rules of collection and use of personal information (we understand that practically this should be in a privacy policy) and obtain consent from the individuals when collecting or using personal information.

In addition, under Article 21 of CSL network operators must demonstrate compliance with cyber security requirements. Accordingly, network operators must:

- Formulate internal security management system and operating procedures, determining the persons in charge of network security, and implementing responsibility for cyber security protection.
- Adopt technical measures to prevent computer viruses and the endangerment of cyber security such as network attack and network intrusion.
- Adopt technical measures for monitoring and recording network operation status and the network security incidents, and keeping relevant network logs for at least six months in accordance with relevant provisions.
- Adopt measures such as data classification as well as backup and encryption of important data.
- Comply with other obligations prescribed by laws and administrative regulations.

Otherwise, under Articles 40 and 41 of CSL, network operators must implement personal information protection systems and clarify in their privacy notices how they process personal information. However, there is no regulation or binding rules on these requirements.

The Draft PIPL sets out the following key principles of personal information protection which are generally consistent with those under the current Chinese laws:

- Lawfulness and legitimacy
- Legitimate purpose and data minimization
- Transparency
- Accuracy
- Security

4.2.2. Application to Digital Advertising

There are no requirements under current mandatory Chinese laws that specifically relate to accountability in the context of digital advertising, but the general requirements discussed above will apply. Please refer to Section 16.4 (i) and (j) for more information regarding draft rules on targeted advertisements and content automatically generated via technologies such as big data and artificial intelligence.

4.3. Notice

4.3.1. Overview

Under Articles 1035(2) and (3) of the Civil Code, a personal information processor must publicize "the rules for processing information" and clearly indicate "the purpose, method, and scope of the information processing." In practice, we understand this requires the personal information processor to display a privacy policy or notice.

Under Article 41 of CSL, where network operators process their users' personal information, they must notify their users. Based on the Measures, the privacy policy must disclose the purposes, means, and scope of personal information collected through third-party cookies, plug-ins, and links.

In practice, when a user typically visits a website or uses an app in China:

- The website displays a privacy policy that explains the purposes, means and scope of personal information collected through the website.
- The app displays a pop-up that contains the app's privacy policy and further pop-ups for mobile phone permissions.

Chinese companies seldom display separate cookie policies or banners, but rather include the content of a cookie policy in their general privacy policy. Therefore, it seems likely that notice around the use of cookies and similar technologies should be included in the privacy policy.

- **Who must receive notice? When must notice be provided? What must be in the notice in the digital advertising context? (Consider also, what notice needs to be provided when pixels fire on a webpage?)**

  Users must receive notice when they visit or use the website or application. In practice, when a user typically visits a website in China, the website provides a privacy policy and includes a link to the privacy policy on each page of the website. When a user installs an app, the app displays a pop-up that contains the app's privacy policy and further pop-ups for mobile phone permissions.

  Under China's current mandatory laws, the privacy policy should explain the purposes, means, and scope of personal information collected through the website or app.

  Under Article 5.5(a) of the Information Security Standards, the privacy policy should explain:

  - Basic information about the personal information controller, including identity and contact information.
  - The business functions that collect and use personal information, and the types of personal information each of the business functions collects. Where sensitive PI is involved, relevant content shall be explicitly marked or highlighted.
  - The collection method and storage period of personal information, whether cross-border data transfer is involved, and other processing rules.
  - The purposes of the sharing, transfer, and public disclosure of personal information, the types of personal information involved, the types of third parties receiving personal information, and the respective security and legal responsibilities.

- The rights of data subjects and implementation mechanisms, such as methods to access, rectify, or delete their personal information, to de-register, withdraw consent, obtain a copy of their personal information, and to lodge a complaint about automated decisions.
- The security risks after consenting to personal information collection, and possible impacts of not consenting to personal information collection.
- The basic principles of personal information security followed, the data security capabilities in place, and the security protection measures adopted; compliance certificates related to data security and protection may be disclosed when necessary.
- The channels and mechanisms for handling the inquiries and complaints of data subjects, and external dispute settlement agencies and their contact information.

The Information Security Standards also include a template privacy policy (at Annex D).

Under the Draft PIPL, the privacy policy or the equivalent document should explain:

- The identity and contact information of the PI Processor.
- The purpose and method of personal information processing.
- The categories and storage period of personal information to be processed.
- The methods and procedures for individuals to exercise their personal information protection rights.
- Other matters that shall be informed in accordance with laws and administrative regulations.

- **Is there specific notice required for sensitive information?**

  There are currently no specific notice requirements around "sensitive information" under Chinese mandatory laws and regulations. However:

  - The Information Security Standards require that data subjects are provided separate notice about the processing of biometric information (which is deemed a kind of sensitive personal information).
  - The Measures for App Operators require apps to display a separate notice when collecting sensitive personal information, such as the user's ID number, bank account number, whereabouts, etc.

The Draft PIPL will introduce the concept of "sensitive personal information," which refers to personal information that may lead to discrimination or serious harm to the safety of persons or property if disclosed or unlawfully used (e.g., information relating to race, ethnicity, religious beliefs, personal biometrics, medical health, financial information, and personal whereabouts). PI Processors must provide notice of sensitive personal information processed, in particular, the necessity for processing sensitive personal information and the implication(s) for individuals, and "separate consent" should be obtained from data subjects. However, as the Draft PIPL has not been finalized yet, it remains unclear regarding how to enforce this "separate consent" requirement in practice (e.g., whether a separate checkbox with relevant specific consent language would be deemed to be sufficient).

- **Are there any specific requirements for providing notice related to processing children's personal information?**

  Yes. Under Article 9 of the Children's Measures, network operators that collect, use, transfer, and disclose children's personal information must notify the child's parent or guardian in a conspicuous and clear manner and must obtain the consent of the child's parent or guardian. A child is any person under 14 years of age. In practice, most Chinese companies provide this specialized notice in their general privacy policy while some choose to provide a separate policy regarding children's personal information.

- **Are there any requirements compelling vendors directly collecting personal information or those receiving it from others to provide additional notices? Who is responsible for those notices? Publishers? The vendors?**

  Current Chinese mandatory laws and regulations do not differentiate between entities that collect personal information directly and those that receive it indirectly. Therefore, both publishers and vendors are responsible for providing notice in accordance with the requirements under Chinese law.

  In practice, currently the party that has a direct relationship with the user (i.e., the publisher) provides notice and obtains the individual's consent. For parties that do not have a direct relationship with the user or collect personal information indirectly (i.e., the advertiser and intermediaries), they should provide a privacy notice on their website and ask the third party that has a direct relationship with the user to take responsibility to obtain consent from the individuals and provide notice via contract terms.

  Under the Draft PIPL, PI processors should notify data subjects of the third party's identity, contact information, processing purpose, processing method and categories of personal information and obtain a separate consent for the purpose of sharing personal information with the third party. Please refer to Section 16.1(h) for obligations regarding sharing personal information with third parties proposed under the Draft PIPL.

4.3.2. Application to Digital Advertising

- **Do third parties need to be named? For example, if a publisher's privacy policy says that it may share personal information with third parties for advertising purposes, does it have to specify which third parties? Do specific digital advertising activities or purposes need to be disclosed as well (e.g., TCF purposes)?**

  No, there are currently no requirements under mandatory Chinese laws and regulations that require specifically naming third parties that will receive personal information for advertising purposes. Article 42 of CSL requires consent to share personal information with third parties and Article 41 requires that consent must be "informed." Best practice favors naming third parties individually. However, usually a privacy policy in China only explains the categories of third parties and does not list the third parties individually. To date, there has been no enforcement for failing to specify third parties.

  Under the Draft PIPL, PI processors should notify data subjects of the third party's identity, contact information, processing purpose, processing method and categories of personal information. Hence, the approach that the publisher displays to the data subjects a list of third-party recipients specifying relevant information mentioned above respectively relating to each of the third-party recipients may be seen as a legally compliant manner.

- **From an industry perspective it's common to distinguish data use for ad targeting vs. profile building vs. measuring ad campaigns. Does the notice requirement require separate disclosure of those things? Or is it enough to say something general like "advertising and related purposes."**

  No, there are currently no requirements under mandatory Chinese laws and regulations that would specifically require the privacy policy to include separate disclosures regarding the use of personal information for ad targeting vs. profile building vs. measuring ad campaigns to notice in the context of digital advertising.

  Under Article 5.4(a) of the *Information Security Standards*, it is recommended that a specific notice is provided if there are more than one data processing activity. Under Articles 5.4(b) and (c), the specific notice should be part of the consent when processing personal sensitive information. Therefore, best practice would favor distinguishing between different processing purposes in the privacy policy but, in practice, a privacy policy may simply say that personal information will be processed for "advertising and related purposes."

  The Draft PIPL does not specifically require the publisher / advertiser to distinguish data use for the purposes of ad targeting, profile building, or measuring ad campaigns respectively in the privacy policy. However, considering that these processing activities are conducted for different purposes, to comply with "informed consent" and transparency principles, it is advisable to provide a more detailed description

on each of the purposes and types of personal information collected and processed instead of using a general statement in the privacy policy.

4.4. Consent and Exceptions to Consent

4.4.1. Overview

Under current Chinese mandatory laws, consent is generally required to process personal information.

Civil Code

Under Article 1035 of the Civil Code, personal information processors must obtain consent from the individual to process the individual's personal information, and under Article 1038 consent is a lawful basis to share personal information. In addition, under Article 1033 of the Civil Code personal information processors must obtain express consent to process the individual's private personal information (i.e., information the individual does not want to disclose). Currently, and in the absence of further guidance and cases, it is unclear whether consent or express consent is required in the context of digital advertising. Arguably, under the Civil Code consent will suffice for the purposes of digital advertising (i.e., display advertising) but there may be certain contexts where digital advertising involves private information.

There are certain exemptions to the consent requirement and consent is not the only lawful basis to process personal information under the Civil Code (for example, if the processing is required by law or regulation). In particular, under Article 1036 of the Civil Code personal information processors will not be held accountable where:

- The processing is within the scope of a consent.
- The personal data has already been disclosed by the individuals themselves or is already in the public domain (except where the individual explicitly objects to the processing or the processing is contrary to their vital interests).
- The processing is reasonable to protect the public interest or the lawful interests of the individual.

However, the non-consent exemptions are unlikely to be applicable in the context of digital advertising.

CSL

Under Article 42 of CSL, entities must not disclose personal information to any other organizations or individuals without the consent of the persons whose information has been collected, except where the information has been anonymized (i.e., processed in a manner that it is impossible to identify a specific person and so that it cannot be restored to its original status).

We understand that consent does not need to be specific under CSL. This means that third parties do not need to be named specifically, and consent to processing generally and consent to sharing with third parties can be general and

bundled. We expect the requirements around consent and how consent should be obtained from individuals, may be subject to further judicial scrutiny in the future.

Measures for App Operators

Under the *Measures for App Operators*, app operators must ensure individuals agree to their privacy policies and the consent must be explicit and positive. The Measures also further require app operators to allow app users to use and refuse SDKs and other technologies.

In particular, under Article 3 of the Measures for App Operators the following behaviors are identified as "collecting and using personal information without obtaining the user's consent":

1. Collecting personal information or enabling the mobile phone permission to collect personal information before obtaining user consent.
2. Continuing to collect personal information, enabling the mobile phone permission to collect personal information, frequently asking for user consent, or interfering with the user's normal use of the app after the user has expressly opted-out or withdrawn consent.
3. Obtaining the user's consent in a non-explicit way, such as choosing to agree to the privacy policy by default.
4. Changing the mobile phone permission status to collect personal information without the user's consent (such as automatically changing the permissions set to the default status when the app is updated).
5. Failing to provide users with a way to withdraw their consent to the collection of personal information.

Standard of Consent

Generally speaking, the standard of consent is low in China and implied consent is tolerated. However, best practice favors express consent and explicit consent is required for apps. Please see Section 3.7 for more information about the standard of consent.

- **For what types of personal information or purposes of processing is consent required?**

  Under China's current laws, consent is generally required to process all types of personal information. Consent is also required for nearly all processing purposes in the context of digital advertising.

  The Draft PIPL will introduce more non-consent bases for processing, which include where:

  - The processing is necessary in order to conclude or perform a contract with the data subject who is a party of such contract;
  - The processing is necessary in order to respond to public health incidents or to protect the life, health, and property of data subjects in emergency cases.

- The information to be processed is publicly available and the processing is within the reasonable scope and in compliance with the requirements under Draft PIPL;
- The PI Processor is acting in the public interest for news reports or media supervision purposes within a reasonable scope.
- Other circumstances apply which are provided by laws and regulations (a "catch-all" clause).

Unlike GDPR, the Draft PIPL (in its current draft form) does not allow for the collection and processing of personal information on the basis of "legitimate interests." And we are of the view that the catch-all clause is not intended to be interpreted as the same as the legal basis for the collection and processing of personal information on the basis of "legitimate interests."

The Draft PIPL will require separate consent under certain circumstances, including to process sensitive personal information, to share personal information with third parties, to disclose personal information to the public, and to transfer personal information outside of China.

- **How is valid consent manifested–express consent, opt-in, implied consent, or opt-out?**

  As explained above, the standard of consent is low in China and implied consent is generally tolerated. The notable exception is for mobile apps, where express consent is required. Please see Section 3.7 for more information about the standard of consent in China.

- **Is specific notice required as part of the consent?**

  No, there are currently no requirements under mandatory Chinese laws and regulations that require specific notice as part of consent. Article 41 of CSL requires that consent must be “informed” but this does not require any specific notice, and generally consent is bundled in China. Please see Section 4.3.2 for more information about the notice requirements under Chinese law.

- **Does the consent obligation require granularity (i.e., consent for distinct processing activities) similar to GDPR? Or is the consent obligation more generalized (e.g., consent to "online behavioral advertising" more broadly, without having to obtain consent to each constituent processing activity/party)? Is consent different for different uses or types of data (e.g., sensitive data, profiling, automated decision making, etc.) Please provide details.**

  See above–generally speaking, under China’s mandatory laws consent does not require granularity for different purposes and is usually bundled (e.g., processing for advertising purposes and sharing with third parties”). The *Information Security Standards* currently require a separate consent to process sensitive personal data and under the Draft PIPL separate consent will be required in certain circumstances (e.g., including to process sensitive personal information).

- **Can personal information be processed for secondary purposes (i.e., differing purposes from which it was collected)?**

  No. Under Article 1036(1) of the Civil Code, where personal information is processed for a secondary purpose that is different from the original purpose, the personal information can be processed for that secondary purpose if it is within the scope of the consent to the original one. If the secondary purpose is beyond the scope of the original consent (e.g., not reasonably relevant), the organization must obtain consent for the secondary purpose. The words "within the scope of consent" are yet to be clarified.

- **Are there any rules compelling downstream recipients/processors of personal information to provide additional notices?**

  There are no specific rules regarding the notice obligations of downstream recipients. Strictly speaking, if downstream recipients collect and use personal information (e.g., ad tech intermediaries and advertisers), then they are required to provide notice under current China's mandatory laws (in particular, CSL and the Civil Code). Technically, this applies both where the downstream recipient is merely acting as a service provider on behalf of the organization collecting the information or upstream recipient, and where the downstream recipient is using the data for its own purposes.

  In practice, downstream recipients that do not have a direct relationship with the users may choose to require the publisher or upstream recipients to provide notice on their behalf under their contractual agreements. This is not followed in all cases in China but is common practice amongst larger companies.

  Under the Draft PIPL, the entrusted party must process personal information on the basis of the agreement with the PI Processers and within the agreed purpose and method. In that case, the entrusted party is not required to provide additional notices to or collect consent from the data subjects.

- **Are there any issues concerning the timing of consent?**

  The data subject must consent prior to the processing and the data subject must be fully informed before providing consent. However, under China's current mandatory laws this does not require a banner/pop-up/ just in time notice. Instead, implied consent is obtained through the user's use of the website. However, for mobile apps the consent must be explicit and therefore the user is presented with a pop-up when they download the app that obtains their consent to the privacy policy.

- **Are there distinct consent requirements for sensitive personal information?**

  There are currently no mandatory consent requirements around sensitive information.

  The concept of "sensitive personal information" was introduced under the Information Security Standards. This is defined as personal information that if breached, illegally provided or abused, could endanger the personal or property safety of an individual, or easily lead to damages to personal reputation, mental and

physical health, or discriminatory treatment, etc. Sensitive personal information includes ID numbers, personal biometric information, bank account information, communication records and content, property information, credit information, records of whereabouts, accommodation information, health information, transaction information, and the personal information of minors up to 14 years of age. Article 5.4(b) of the Information Security Standards requires that before the collection of sensitive personal information, the personal information controllers must obtain explicit consent from the data subjects. The explicit consent must be specific, clear and freely given, and fully informed.

Under the Draft PIPL, "Sensitive Personal Information" refers to personal information that may lead to discrimination or serious harm to the safety of persons or property if disclosed or unlawfully used. Examples include information relating to race, ethnicity, religious beliefs, personal biometrics, medical health, financial information, and personal whereabouts. A separate consent requirement is proposed for processing sensitive personal information, however, there remains uncertainties regarding how the "separate consent" can be obtained in practice.

- **Are there distinct consent requirements for profiling consumers? If a business gets consent to use personal data for "advertising and marketing" purposes, is a separate (or more specific?) consent required to build an advertising profile for advertising?**

  No.

- **Are there distinct consent requirements for automated decision making?**

  No.

- **Are there any age restrictions related to consent? Are there distinct consent requirements around processing children's personal information?**

  Yes, under the Children's Measures consent must be obtained from the child's parent or legal guardian where the child is under the age of 14. However, the standard of consent is not clearly defined.

- **Can consent, however manifested, be revoked?**

  Yes. Under Article 8.4 of the *Information Security Standards*, consent can be withdrawn and the method to withdraw consent must be specified in the privacy notice. The withdrawal of consent does not affect the lawfulness of processing based on consent before withdrawal.

  In practice, it is uncommon to provide an opt-out mechanism (such as a cookie preference center) and usually consent is managed by clearing or deleting cookies from the user's browser. This is still a developing area in China, but there are no mandatory requirements or commonly followed processes.

  Under the Draft PIPL, consent can be withdrawn at any time. A PI Processor cannot refuse to provide

products or services on the grounds that the data subject does not consent or withdraws his/her consent, except where the processing is necessary for the provision of such products or services. That being said, any withdrawal of consent will not affect the processing activities based on such consent prior to the withdrawal.

4.5. Appropriate Purposes

4.5.1. Overview

Under the Civil Code, the appropriate purposes are as follows:

- Personal information processors must obtain consent from the individual or their guardian and the processing is within the scope of a consent.
- The personal information has already been disclosed by the individuals themselves or it is already in the public domain (except when an individual explicitly objects to the processing or the processing is contrary to their vital interests).
- Where the processing is reasonable to protect the public interest or protect the lawful interests of the individual.

4.5.2. Application to Digital Advertising

- **Does the law or legal guidance require a specific legal basis for specific digital advertising activities? Clarify for each activity (suggest using TCF/IAB CCPA "purposes") ("profiling" must be addressed here).**

  No. Under China's current mandatory laws, consent is the main legal basis for nearly all digital advertising activities while for certain activities performing legal obligations will also be a legal basis. Unlike GDPR, current Chinese laws and the Draft PIPL do not provide for legitimate interests as a possible legal basis.

  Using the TCF purposes to clarify for each activity:

TCF purpose	Legal basis
Store and access information on the device such as cookies and device identifiers for the purposes presented to a user	Consent
Select basic ads	Consent
Create a personalized ads profile	Consent

Select personalized ads	Consent
Create a personalized content profile	Consent
Select personalized content	Consent
Measure ad performance	Consent
Measure content performance	Consent
Apply market research to generate audience insights	Consent
Develop and improve products	Consent
Ensure security, prevent fraud, and debug	Legal obligation according to CSL
Technically deliver ads or content	Consent

- **If yes, what are the legal bases (e.g., consent, legitimate interest)? Are there any requirements related to lawful basis (need a valid legal basis to process)/fairness (scope of processing is fair)/transparency (transparent about the processing activity to the consumer and the lawful basis)?**

  See above. Consent is generally required to process personal information under Chinese mandatory laws (except where the processing is required by law or regulation).

  The Draft PIPL will specify more (non-consent) bases for processing which include (i) conclusion or performance of contract(s); (ii) responding to public health incidents or for the protection of the life, health, and property of data subjects in emergency cases; (iii) acting in the public interest for news reports or media supervision purposes within a reasonable scope; (iv) processing publicly-available personal information within the reasonable scope, and (v) other circumstances provided by laws and regulations (a "catch-all" clause). Unlike GDPR, the Draft PIPL (in its current draft form) might not allow for the collection and processing of personal information on the basis of "legitimate interests" of corporate entities.

  The Draft PIPL will require separate consent in certain circumstances, including to process sensitive

personal information, for the sharing personal information with third parties, and to transfer personal information outside China.

- **Does the law address processing for secondary purposes/differing purposes from which it was collected?**

  See above. Consent is required to process personal information for a secondary purpose that does not fall within the scope of the original consent.

4.6. Safeguards

4.6.1. Overview

Safeguards generally include physical and technical safety measures.

Article 21 of CSL requires that the state shall implement graded cybersecurity rules. Network operators must, according to the graded cybersecurity rules, fulfill the following security protection obligations to ensure that the network is free from interference, damage or unauthorized access, and prevent network data from being divulged, stolen, or falsified. Network operators must therefore:

- Develop internal security management rules and operating procedures, determining the persons in charge of cybersecurity, and carrying out the responsibility for cybersecurity protection.
- Implement technical measures to prevent computer viruses, network attack, network intrusion, and other acts endangering cybersecurity.
- Implement technical measures to monitor and record the status of network operation and cybersecurity incidents and preserve relevant weblogs for not less than six months as required.
- Implement measures such as data categorization, and back-up and encryption of important data.
- Comply with other obligations as prescribed by laws and administrative regulations.

4.6.2. Application to Digital Advertising

There are currently no requirements under mandatory Chinese laws and regulations specifically relating to safeguards in the context of digital advertising.

5. DATA SUBJECT RIGHTS/EXEMPTIONS

5.1. Overview

The rights discussed below are contained in CSL, Civil Code, and E-Commerce Law. Please see Section 16 for individuals' rights under the Draft PIPL.

5.2. Access

The data subject is entitled to make a request to the personal information processor for access to their personal information. If the data subject wishes to access their personal information, they can do so at any time by contacting the personal information processor.

5.3. Rectify

In cases of any inaccurate personal information, the data subject is entitled to make a request to the personal information processor for rectification of their personal information. If the data subject wishes to correct or update their personal information, it can do so at any time by contacting the personal information processor.

5.4. Deletion/Erasure

If the personal information processor processes the data subject's personal information unlawfully or in violation of the parties' agreement, the data subject is entitled to request deletion of their personal information in a timely manner. If the data subject wishes to request deletion of their personal information, it can do so at any time by contacting the personal information processor.

The Measures also provide users with the right to cancel their application accounts. This cancellation right is different from the deletion right as it includes cancelling all the information relating to the account.

5.5. Restriction on Processing

There is currently no equivalent right under mandatory Chinese laws and regulations.

5.6. Data Portability

There is no equivalent right under mandatory Chinese laws and regulations under Article 8.6 of the *Information Security Standards*, there is a similar right whereby individuals can obtain a copy of their personal information, and have the right to transfer their information to another organization where technically feasible.

5.7. Right to Object

There is currently no equivalent right under mandatory Chinese laws and regulations. Please see Section 16.10 for right to object processing under the Draft PIPL.

5.8. Right Against Automated Decision-Making

There is currently no equivalent right under mandatory Chinese laws and regulations. Please refer to Section 16.1(i) for data subject rights regarding automated decision-making proposed under the Draft PIPL.

5.9. Responding to Data Subject Rights Requests

There is no clear mandatory requirement on the time limit for responding to rights requests. Under the Measures for

App Operators, mobile apps must provide a means for users to submit requests and the time limit for responding to rights requests 15 working days.

Under Article 8.7 of the *Information Security Standards*, after verifying the identity of the data subject the response and reasonable explanation should be given within 30 days or other time period stipulated by laws or regulations.

Currently, e-commerce operators must clearly state the methods and procedures for user information access, correction, deletion, and cancellation requests, and must not set unreasonable conditions on the user's ability to exercise their rights. When an e-commerce operator receives an access, correction, or deletion request, it must comply with the request promptly after verifying the user's identity. If the user logs off, the e-commerce operator must immediately delete the user's information.

5.10. Record Keeping Concerning Rights Requests

There is no record keeping requirement for rights requests under Chinese law.
Please refer to Section 16.1(i) for statutory data subject rights proposed under the Draft PIPL.

5.11. Is Providing Consumers with these Rights Required by Law or Mere Suggestions?

The rights discussed above are required under mandatory laws such as CSL, the Civil Code and the E-Commerce Law. The *Information Security Standards* contain related rights, but this is only a recommended national standard and is not enforced mandatorily.

5.12. Application to Digital Advertising

The Civil Code and CSL do not provide any detail about how individuals should be able to exercise the right to access, correct, delete or withdraw their consent.

Under Article 24 of the E-commerce Law, the e-commerce operator must provide a method to exercise the right to access, correct and delete. Before responding to requests, the e-commerce operator must verify the identity of the users and must not set up any unreasonable barriers for the user to exercise such rights.

The Information Security Standards provide further guidance about managing data subject rights:

Access: The personal information controller must provide the data subject with the following information:

- The categories of personal information, or the personal information itself held by the personal information controller.
- The source of the above-mentioned PI, as well as the purpose for which it is used.
- The identity or categories of any third party who has obtained the above-mentioned PI.

Correct: The personal information controller must provide a channel for the data subject to request to rectify the error or provide supplemental information.

Delete: Upon request, and in the following circumstances, the personal information controller must delete the personal information without delay:

- The personal information controller has collected and used the personal information in violation of laws or regulations.
- The personal information controller has collected and used the personal information in violation of its agreement with the data subject.

If the personal information controller has shared personal information with, or transferred personal information to a third party in violation of laws or regulations, or in violation of its agreement with the data subject, and the data subject requests deletion, the personal information controller must immediately stop the sharing and transfer, and notify the third party to delete the information in a timely manner.

Withdrawal of Consent: The personal information controller must provide a method for data subjects to withdraw their consent to the collection and use of their personal information, and after the withdrawal of consent the personal information controller must not continue to process the personal information.

The personal information controller must also ensure that data subjects have the right to refuse to receive commercial advertisements targeted to them based on their personal information. The personal information controller must also provide data subjects with a method to withdraw consent in the case of sharing, transferring or publicly disclosing personal information.

Obtaining a Copy of Personal Information

Upon request, the personal information controller should provide the data subject with a method to obtain a copy of the following personal information or, where technically feasible, transmit a copy of the following personal information to a third party designated by the data subject:

- Basic personal information and identity information.
- Personal health and physiological information, educational and occupational information.

The requirements on responding to data subject's rights requests under the Draft PIPL do not differ much from those under the current Chinese law. That said, the right to object processing may provide the data subjects the power not to be bound by certain processing activities such as automatic decision making or customer profiling.

6. DATA CONTROLLER AND PROCESSOR AGREEMENTS

6.1. Overview

There are currently no equivalent requirements under mandatory Chinese law that govern agreements between data controllers and processors.

6.2. Data Controller Outsourcing of Processing

There are currently no equivalent requirements under mandatory Chinese laws that govern the outsourcing of processing by a personal information processor or a network operator.

However, under Article 9.1(d) of the Information Security Standard, the personal information controller can choose to specify the responsibilities and obligations of its third-party service providers (similar to the role of processor under GDPR) and audit service providers. In practice, we suggest that clients prepare a GDPR-style data processing agreement to govern the arrangement with service providers, but the terms can be more flexible.

Please refer to Section 16.1(h) regarding outsourcing requirements proposed under the Draft PIPL.

6.3. Data Processor Rights and Responsibilities

As there is no equivalent to GDPR's concept of a "data processor" under Chinese law, there are no specific requirements that apply to these organizations.

Please refer to Section 16.1(h) regarding responsibilities for entrusted parties and joint processor proposed under the Draft PIPL.

6.4. Application to Digital Advertising

There are currently no requirements under mandatory Chinese laws and regulations that specifically regulate agreements in the context of digital advertising.

Please refer to Section 16.1(h) regarding outsourcing requirements and responsibilities for entrusted parties and joint processors proposed under the Draft PIPL.

Considering that China data protection law is fast evolving, in practice, it is advisable for the advertisers and publishers to enter into a definitive agreement with robust data protection clauses in order to clearly allocate parties' obligations and responsibilities concerning collection and processing of data subjects' personal information.

7. DATA TRANSFER & OUTSOURCING

7.1. Overview

Under the Civil Code and CSL, the legal basis to transfer personal information outside of China must be consent. This means that personal information processors and network operators must obtain consent before transferring personal information outside China. However, the standard of consent is relatively low (as discussed above).

There are more prescriptive requirements for critical information infrastructure operators. Under Article 37 of CSL, where personal data and important data and important data generated from critical information infrastructure has to be transferred data overseas due to business needs then the critical information infrastructure operator ("CIIO") must conduct a security assessment in accordance with measures developed by the Cyberspace Administration of China ("CAC"), unless the transfer is otherwise prescribed by law.

Please note that the data localization and transfer obligations only apply to CIIOs, not network operators. Although the CAC has drafted some rules and measures to expand these obligations to network operators (such as the draft *Measures for Security Assessment of Export of Personal Information*), these measures are not currently in effect.At the time of writing, it is not clear how the security assessment should be conducted. CSL creates this requirement but provides no guidelines.

Please note the draft Measures for Security Assessment of Export of Personal Information ("Draft Security Assessment Measures") provides detailed guidance for the personal information cross border transfer security assessment. It includes a Chinese standard contractual clause for data transfers and also guidance for how data exporters should conduct the transfer security assessment.

Under the Article 13 of Draft Measures for Data Export, the contract should contain certain terms, including:

1) The purpose, categories and duration of the personal information going abroad.
2) The fact that the data subject is a beneficiary of the terms of the contract involving the rights and interests of the data subject.
3) When the rights and legal interests of the data subject are harmed, they can claim compensation from the network operator or receiver (or both), either by themselves or by an agent, and the network operator or receiver must compensate the data subject (unless it is proved that it is not liable).
4) When the legal environment of the country where the recipient is located makes it difficult to perform the contract, the contract must be terminated, or the safety assessment must be performed again.
5) The termination of the contract does not exempt the network operator and receiver from the responsibilities and obligations of the relevant provisions of the contract involving the legal rights and interests of the data subject, unless the receiver has destroyed or deleted the received personal

information or anonymized it.

6) Any other content agreed by both parties, such as the rights and responsibilities of the parties, the method for data subjects' rights requests, data retention, consent for sensitive personal information, etc.

However, as this law is not currently in effect it is not yet followed by most of Chinese companies.

Please refer to Section 16.1(j) and Section 16.3 for detailed information regarding the stringent regulatory regime on cross-border transfer of personal information proposed by PRC regulators.

7.2. Application to Digital Advertising

Apart from the Draft Security Assessment Measures, there are no specific requirements regarding data transfers and contractual terms (e.g., between a publisher and advertiser) under current Chinese mandatory laws and regulations. Article 9.8 of the Information Security Standards just refers to the requirements of current laws.

If a publisher needs to transfer personal information to a third party (e.g., an advertiser) whose server is located outside China, then in practice the publisher should take certain steps.

Under the Civil Code and CSL, the legal basis to transfer personal information outside of China must be consent. While consent is required for the transfer, this is not a high standard of consent and a general, implied consent is permitted. It is unclear how many times the publisher should obtain consent since the data transfer may happen frequently and there is no detailed requirement or guidance on this question. To some extent, the Draft PIPL appears to provide that the consent should be obtained explicitly and from time to time, but this is just one interpretation of the law.

Secondly, the transferor is obligated to complete a data transfer security assessment, but in practice, most companies do not currently understand how to comply with this since there is no detailed requirement or practical guidance. We have heard that CAC is trying to push big tech companies to address this obligation but current market practice, and whether the bigger tech companies will comply, is still unclear. The Draft Measures for Data Exports (discussed above) were intended to impose an obligation for CIIOs to complete a data transfer security assessment (under CSL) but it also provides for a standard contractual clause model. Again, this is not something that is generally followed at present.

The Draft PIPL requires PI Processors to enter into a standard contract clause formulated by cyberspace administrative authorities with foreign data recipients for any transfer of collected personal information out of China, to ensure that data recipients process personal information in accordance with the standards under the Draft PIPL. The Draft Security Assessment Measures may provide certain indications on the must-have clauses with respect to the standard contract clause. That said, since the Draft PIPL and Draft Security Assessment

Measures are still in draft form and it is not clear when it will be finalized nor has the PRC regulator released the (draft) form of said standard contract clause, companies in the digital advertising industry may still rely on their existing data transfer agreements, Binding Corporate Rules (BCRs) or other equivalent documents with their overseas affiliates or counterparties. However, we envision that such data transfer agreements will be required to be updated in accordance with the standard contract clause released by cyberspace administrative authorities in order to conform with the requirements stipulated under the draft Chinese data protection laws.

8. AUDIT/ACCOUNTABILITY

8.1. Overview

There is currently no audit requirement under mandatory Chinese laws and regulations, and also no clear requirement of accountability. There are relevant rules for audit and accountability under the national and sector standards, such as the *Information Security Standards*, which can provide guidance to organizations on audit and accountability.

Please refer to Section 16.1(d) for audit and accountability obligations proposed under the Draft PIPL.

- **Audit-What audit rights are dictated by law (e.g., must companies have audit rights over their vendors? Does it matter what the classification of those vendors are?)**

  There is currently no audit requirement under mandatory Chinese laws. Under Article 11.7 of the *Information Security Standards*, audit requirements include:

  - The effectiveness of personal information protection policies, relevant procedures and security measures shall be audited.
  - An automated audit system shall be established to monitor and record personal information processing activities.
  - Records of the audit process shall be able to provide support for security incident handling, emergency response and post-event investigations.
  - Unauthorized access to, tampering with or deletion of audit records shall be prevented.
  - Illegal use and abuse of personal information discovered during audits shall be handled in time.
  - Audit records and retention time shall follow the requirements of laws and regulations.

  In the financial sector, the People's Bank of China has released the *Personal Financial Information Protection Technical Specification* (JR/T 0171—2020) which include audit obligations around the processing of personal information for financial institutions and their service providers.

  Under Article 54 of the Draft PIPL, PI Processors will have a mandatory obligation to regularly audit

their data processing activities to ensure compliance with applicable laws and regulations.

- **Accountability-Must companies/vendors keep certain records to prove they've met certain requirements? What are those requirements?**

  There is currently no clear accountability requirement under mandatory Chinese laws. There is no requirement for companies to prove or publish what they have done to comply with the requirements. Under Article 40 of CSL, network operators must develop internal personal information protection policies, but they are not required to publish how they comply.

  However, accountability is recommended as best practice. In the 2017 case *Mr.Pang VS China Eastern Airlines Company Limited*, the court held that Mr. Pang (an individual) was not able to prove whether China Eastern Airlines had suffered a data breach or not, whereas China Eastern Airlines was able to prove what measures it had taken to protect the personal information from data breaches. It should be noted that case law is not a formal source of law in China, and it is not a formal supplement to the law either.

  Under Article 9 of the Draft PIPL, the PI Processor will be responsible for its personal information processing activities and, as per Article 65, in the event of any claim regarding the PI Processor's infringement upon personal information, it will be assumed that the PI Processor is liable for the infringement upon the data subject's personal information rights unless the PI Processor can prove that they are not at fault.

8.2. Application to Digital Advertising

There are currently no requirements under mandatory Chinese laws specifically relating to audit and accountability in the context of digital advertising.

Once the Draft PIPL is finalized in its current form, the publishers and advertisers in China should audit their data processing activities on a regular basis.

9. DATA RETENTION

9.1. Overview

There are no explicit restrictions around data retention under Chinese law. Based on the data principles enshrined in Article 41 of CSL, Chinese entities must follow the principles of legality, rightfulness, and necessity. Essentially, personal information should only be retained so long as the information is necessary for the purpose of collection. Please refer to Section 16.1(g) regarding data retention requirements under the Draft PIPL.

9.2. Application to Digital Advertising

There are currently no requirements under mandatory Chinese laws specifically relating to data retention in the context of digital advertising.

10. DATA PROTECTION AUTHORITY REGULATORY AUTHORITY

10.1. Overview

Since there is no uniform data protection law in China, no single authority or agency has responsibility for the supervision of compliance with data protection laws. Generally, the government authorities that supervise specific sectors have responsibility for supervision within the same sectors.

10.2. Main Regulator for Data Protection

At the time of writing, there are seven regulated industry sectors in China. They include the telecommunications and network services, financial, credit reference, healthcare, consumer, and e-commerce sectors. Examples of such sector-specific supervisory authorities include:

- The Cybersecurity Administration of China ("CAC").
- The Ministry of Industry and Information Technology ("MIIT").
- The Ministry of Public Security ("MPS").
- The State Administration for Market Regulation("SAMR")
- The China Banking and Insurance Regulatory Commission ("CBIRC").
- The National Health and Family Planning Commission ("NHFPC").
- The National Medical Products Administration ("NMPA").

10.3. Main Powers, Duties, and Responsibilities

CAC is responsible for implementing an internet information dissemination policy and promoting a legal system of internet information dissemination, as well as guiding, coordinating, and reinforcing the administration of internet content and investigating and punishing websites in violation of relevant laws and the regulations.

MIIT is for compliance within the telecommunications industry.

MPS is responsible for supervising and administering the security and examination of public information systems, controlling classified cybersecurity protection, and punishing cybercrime.
SAMR is for compliance with the consumer sector.

CBIRC is responsible for compliance with data protection related obligations within the banking and financial industry.

NHFPC is for compliance by medical institutions.

NMPA is for compliance of medical and healthcare products.

10.4. Application to Digital Advertising

CAC is the main authority to regulate personal information processing in cyberspace and therefore likely to regulate the privacy of digital advertising, except SAMR also regulates the advertisement sector so it also has the power to supervise digital advertising.

11. SANCTIONS

11.1. Overview

The sanctions may differ under different laws, but there are essentially two types of sanctions:

1) Administrative Penalties. Under CSL, fines can be imposed of either up to CNY 1 million (approx. €132,470) OR no less than one time but no more than ten times the amount of any illegal income obtained through the violation.
2) Criminal Penalties. Under Article 235.1 of CSL, criminal penalties can include (a) a sentence of no more than three years' imprisonment or criminal detention in combination with fines; (b) fines alone; or (c) if the circumstances are particularly serious, a sentence of three to seven years imprisonment or criminal detention in combination with fines. The fines for criminal penalties are different from administrative fines (as this is a criminal sanction).

The Civil Code does not include any direct penalties for non-compliance but provides a private, rights of action for individuals to sue non-compliant companies/organizations.

11.2. Liability

The relevant national provisions for non-compliance with China's mandatory data protection laws and regulations are as follows:

Administrative Penalties

Under Article 64 of CSL, where any network operator or provider of network products or services infringes upon the right that personal information must be protected in accordance with the law, the competent department can order it to take corrective action and either separately or concurrently:

- Give it a warning.
- Confiscate its illegal income.
- Impose a fine of no less than one time but no more than ten times the amount of the illegal income.
- Impose a fine of no more than CNY 1 million (approx. €132,470) on the network operator and impose a fine of no less than CNY 10,000 (approx. €1,320) but no more than CNY 100,000 (approx. €13,250) on directly responsible persons in charge and other directly liable persons.
- In serious cases, order it to suspend its relevant business operation, cease its business operation for rectification, close down the website, or revoke the business permit or license.

In addition, where anyone acquires personal information through theft or any other illegal means, or illegally sells or provides personal information to any other person, in violation of Article 44 of CSL but where such act does not constitute a crime, the public security authority may confiscate the illegal income and impose a fine of no less than one time but no more than ten times the amount of the illegal income, or no more than CNY 1 million (approx. €132,470).

More broadly, under Article 65 of the Law of the People's Republic of China on Protection of Consumer Rights, if there are other sanctions required by other laws and regulations (such as CSL) then those sanctions shall be applied. If there are no applicable sanctions under other laws and regulations, and the organization infringes a consumer's personal freedom or right to protection of personal information, then the competent department or other relevant administrative department may issue correction orders and, depending on the circumstances, impose warnings, confiscate illegal gains, and impose a fine of one to ten times the illegal gains obtained from the violation. If there are no illegal gains, a fine of no less than CNY 500,000 (64386.52 EUR) may be imposed and if the circumstances are serious, the business can be ordered to suspend business pending rectification or the organization's business license can be revoked.

The Draft PIPL has greatly increased penalties on top of CSL. Please refer to Section 16.1(m) for detailed information regarding administrative penalties for any infringement upon personal information proposed under the Draft PIPL.

Criminal penalties

Article 253A of the Criminal Law provides that either (a) a sentence of no more than three years' imprisonment or criminal detention in combination with fines; (b) fines alone; or (c) if the circumstances are particularly serious, a sentence of three to seven years; imprisonment or criminal detention in combination with fines for; may be imposed for the following offenses:

- When a person sells or provides personal information to others in violation of relevant national provisions, the circumstances are serious.

- When persons sell or provide personal information of citizens to others in violation of relevant national provisions, which are obtained during the performance of duties or provisions of services, the sentence shall be heavier within the stipulated range of paragraph 1.
- In case of stealing or otherwise illegally acquiring personal information of citizens, the sentence shall be in accordance with the provisions of the paragraph 1.

When entities commit the crimes above, the entities shall be sentenced to fines; the persons who are directly in charge and any other persons who are directly liable for the offences shall be sentenced according to each respective paragraph.

In addition, Article 286 of the Criminal Law provides that network service providers who do not perform their duties of safety management of information networks as provided by laws and administrative regulations, and refuse to correct their conducts after the regulatory authorities order them to correct the non-performance, as well as under any of the following circumstances:

- Resulting in the dissemination of a large number of illegal information.
- Causing the disclosure of user information, resulting in serious consequences.
- Causing the loss of criminal evidence, if the circumstances are serious.
- Having other serious circumstances.

shall be subject to fixed-term imprisonment of no more than three years, criminal detention, or public surveillance, in combination of fines or the sentence can be fines alone. When entities commit the crime, the entities shall be fined, and the persons who are directly in charge and any other persons who are directly liable for the offences shall be sentenced according to the provision.

As for persons who have committed this crime, and commit other crimes in the meantime, provisions with a heavier penalty shall be followed for conviction and punishment.

- **Scope of liability for ad tech companies for collection activities of publishers and advertisers.**

Ad tech companies are responsible for any infringement of the above mandatory provisions.

Under the Interpretations of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Application of Law in the Handling of Criminal Cases Involving Infringement of Citizens' Personal Information, which interprets China's Criminal Law, the following ***collection activities*** will be deemed criminal and will be subject to fixed-term imprisonment of no more than three years, criminal detention, or public surveillance where:

1) The party concerned illegally obtains, sells or provides 50 pieces of information about citizens' whereabouts and tracks, communication details, credit, and property.

2) The party concerned illegally obtains, sells or provides 500 pieces of citizens' personal information that are likely to affect citizens' personal safety or property safety, such as information about accommodation, communication record, physical health, and transactions.

3) The party concerned illegally obtains, sells or provides 5,000 pieces of citizens' personal information, other than the information list above.

4) The respective amount of certain information does not reach the criteria specified in Items above, but the amount in aggregate according to the relevant proportions surpasses the stipulated threshold.

5) The party concerned obtains illegal gains of over CNY5,000.

The following collection activities will be deemed "particularly serious" and can lead to a sentence of three to seven years, imprisonment, or criminal detention:

6) Where such act results in the death, serious injury, psychiatric disorder of the victim, or that the victim is kidnapped, or causes any other serious consequence.

7) Where such act leads to major economic losses or evil social influences.

8) Where the quantity of information or the amount of illegal gains is over ten times as much as the criteria specified in the preceding paragraph.

9) Any other circumstance where the case is particularly serious.

In addition, please note the act of illegally purchasing or receiving personal information for lawful business activities shall be deemed criminal:

10) Where the party concerned makes a profit of over CNY5, 000 by taking advantage of the information that is illegally purchased and received.

11) Where the party concerned has been subject to criminal punishment as result of an infringement of citizens' personal information or to any administrative penalty in the past two years, but illegally purchases and receives citizens' personal information again.

12) Any other circumstance where the case is serious.

Ad tech companies will generally be considered network operators under CSL. Currently, there are no examples of ad tech companies that collect personal information being sanctioned under the provisions of CSL listed above. There have been cases where advertising companies have been for breaches of the cybersecurity provisions of the CSL for example, placing gambling ads on their website-but these cases have not involved breaches of the obligations relating to the processing of personal information.

However, there is a case involving a fine under Article 56 of the Law of the People's Republic of China on Protection of Consumer Rights. The company was fined RMB 20,000 (approximately EUR 2,600) by the local administrator for

market regulation in Shanxi Province for the illegal collection of personal information without consent of the data subjects. The company had illegally collected more than 300 pieces of personal information and sent advertisements to the data subjects and disturbed their life and work.

- **Scope of liability for ad tech companies for other ad tech companies they enable to process data (either because they make the decision on behalf of publishers or advertisers or agency dictates it).**

The current laws and regulations in China do not distinguish between controllers and processors, and thus both controllers and processers (as defined under GDPR) are regulated by the above provisions. The Draft PIPL will introduce similar definitions and requirements for controllers and processors (see Section 16).

In terms of scope of liability for ad tech companies that enable other ad tech companies to process data:

- For **criminal sanctions**, under the *Interpretations of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Application of Law in the Handling of Criminal Cases Involving Infringement of Citizens' Personal Information:*
    - Any act in violation of the provisions on the protection of personal information as stipulated in laws, administrative regulations or department rules shall be deemed as "one violating relevant provisions of the State" as mentioned in Article 253A of the Criminal Law.
    - The act of providing a particular individual with any personal information or making public any citizen's personal information by means of the information network or otherwise shall be deemed as "one providing citizens' personal information" as mentioned in Article 253A of the Criminal Law.
    - The act of providing any other individual with any citizen's personal information legally collected without the consent of the citizen whose personal information is collected shall be deemed as “one providing citizens' personal information.”
    - The act of purchasing, receiving or exchanging any citizen's personal information or obtaining such personal information by other means, or collecting any citizen's personal information while performing duties or providing services, which contravene the relevant provisions of the State, shall be deemed as "one illegally obtaining citizens' personal information by other means" as mentioned in Paragraph 3 of Article 253A of the Criminal Law.
- For the administrative sanctions, ad tech companies that qualify as network operators may be subject to administrative sanctions under CSL.
- For civil compensation, based on the entrusted relationship between the ad tech company and the publisher (or the advertiser, agency) the liability for the ad tech companies will depend on the contractual terms with the publisher or advertiser (although the contract is not mandatorily required by laws).

In addition, under Article 24 of *Internet Advertising Measures*, any subject that attaches advertisements or advertisement links to emails sent to a user without the user's permission can be ordered to make corrections and/or be fined between RMB 10,000 and RMB 30,000.

11.3. Enforcement and Market Practice

- **How are claims raised under the law?**

  In practice, regulatory enforcement is triggered by two different ways:

  1) Regulators proactively conduct investigations on personal information protection (please see Section 10):
  2) Individual complaints or whistleblowing.

- **Who enforces them?**

  In China, various administrative departments have the power to issue enforcement notices or penalties under their own jurisdictions. For example:

  - MPS and its local branches may issue enforcement notices for the purposes of preventing and cracking down on crime.
  - The MIIT and its local branches may issue enforcement notices for those offences that do not amount to a crime.
  - SAMR and its local branches may issue enforcement notices for the purpose of consumer information protection.
  - Sector regulators, such as the People's Bank of China ("PBC"), may issue enforcement notices to entities which fall within their jurisdiction.

- **What's their practice (quietly working with companies to fix, publicly coming out with large investigations? Fact specific?)**

  In practice, enforcement currently focuses on the personal information protection requirements of the Measures for App Operators. However, regulators don't generally issue fines for non-compliance and instead take the following measures:

  1) Issuing warnings via official document.
  2) Notifying the app operator by different app stores.
  3) Communicating with app operators and working with the companies to resolve the issue.
  4) Publicly disclosing non-compliance via official media.
  5) Ordering app stores to suspend downloading of non-compliance apps.

- **What's guidance been to date on how to handle requirements in the ad ecosystem? Have the regulators been educated on how the ecosystem operates? Have compliance regimes been discussed with them? Has their feedback been solicited?**

  We are not aware of any current requirements or guidance in the ad ecosystem, and generally speaking, regulators are not well informed or educated on this topic.

11.4. Remedies

For civil cases, under the Circular of the Supreme People's Court on Issuing the Revised Provisions on Causes of Action in Civil Cases there are causes of actions named, "Disputes over personal information protection," which permit individuals to raise personal information protection infringement claims under laws other than the Criminal Law, including the Civil Code.

For criminal cases, under the Criminal Procedure Law of the People's Republic of China public security bodies are responsible for investigation, detention, execution of arrests and preliminary inquiry in criminal cases. The People's Procuratorates are responsible for prosecutorial work, authorizing approval of arrests, conducting investigation and initiating public prosecution of cases directly accepted by the security bodies. The People's Courts is responsible for adjudication. Except as otherwise provided by law, no other bodies, organizations, or individuals have the authority to exercise such powers.

11.5. Private Right of Action

In accordance with the Civil Code, the Chinese Supreme Law has added personal information protection as a private right of action. For civil cases, the Circular of the Supreme People's Court on Issuing the Revised Provisions on Causes of Action in Civil Cases provides a private right of action named, "Disputes over personal information protection," which permits individuals to raise personal information protection infringement claims under laws other than the Criminal Law, including the Civil Code.

The Draft PIPL will introduce a shift regarding the burden of proof in terms of personal information infringement in a private right of action. This means that it will be assumed that the PI Processor is liable for the infringement upon the data subject's personal information rights unless the PI Processor can prove that they are not at fault.

The *Measures for the Determination of the Collection and Use of Personal Information by Apps in Violation of Laws and Regulation* establishes channels for personal information security complaints and reports. In addition, under Article 59 of the *E-Commerce Law*, e-commerce operators must establish a convenient and effective mechanism for data subjects to submit complaints and reports and must accept and handle complaints and reports in a timely manner.

11.6. Digital Advertising Liability Issues

Currently, we have not found any civil litigation cases involving digital advertising or enforcement under CSL or

E-Commerce Law. However, there are some cases to note.

- Case No. (2019) Zhejiang 0191 Civil Ehu No.189, Mr. Jia vs Shangyou (Hangzhou) Information Technology Co., Ltd "Shangyou". The facts of this case took place in June 2018 and the decision was handed down in 2019. The case involved different civil issues, but in terms of the personal information aspects of the case:
    - Shangyou provides advertising design, consulting, and publishing by using profiling and targeted advertising.
    - Shangyou collected personal information from users (time, gender, age, preference, purchase history, etc.) by using device MAC address and automatically generated user profiles. The users of Shangyou logged in to the "Shangyou Box" software to access the customer's Mac address, analyze customer characteristics, and carry out online advertising through the computer, and match the Mac address with the customer's mobile phone number, generate a virtual number, and deliver advertisements to customers via text messages and phone calls.
    - Shangyou admitted that the act of obtaining the personal information through the "Shangyou Box" and sending advertisements to users without the user's consent violated the mandatory provisions. The court believed that this constituted a violation of Article 43 of the Advertising Law. However, the court did not consider the legality of the actual collection of personal information or the online advertising activities since this did not form part of the plaintiff's claim.
- Prior to 2020, consumers would generally use breach of contract as the cause of action. For example, Mrs. Wang sued Beijing MISS FRESH E-Commerce Co Ltd (a large online fruit and vegetable seller) for violating its terms and conditions and privacy policy, after she had objected to direct marketing messages (via the method stipulated in the privacy policy) but continued to receive such commercial messages. The court judged this case according to the Contract Law of People's Republic of China (which was by the Civil Code in January 2020). MISS FRESH lost the case and was ordered to compensate the plaintiff for the loss of CNY 0.1 in SMS charges.
- In an advertising case, Shanxi DuTe Decoration Engineering Co. Ltd was fined RMB 20,000 (approximately EU R2,600) by the local administration of market regulation of Shanxi Province for the illegal collection of personal information without consent of the data subjects. The company had illegally collected more than 300 pieces of personal information and sent advertisements not digital advertising to individuals and disturbed their life and work. This fine was issued under Article 56 of the Law of the People's Republic of China on Protection of Consumer Rights.

Under the Draft PIPL, in the event of any claim regarding the PI Processor's infringement upon personal information, it will be assumed that the PI Processor is liable for the infringement upon the data subject's personal information

rights unless the PI Processor can prove that they are not at fault. Therefore, market players in digital advertising are advised to take note of the importance of data protection compliance in their daily operations.

12. NOTIFICATION | CERTIFICATION | REGISTRATION

12.1. Overview

There are currently no requirements under mandatory Chinese laws and regulations regarding notification, certification, or registration. Please refer to Section 16.1(d)(1) regarding the requirement of appointing a data protection officer introduced under the Draft PIPL.

12.2. Requirements and Brief Description

Notification

There are currently no requirements under mandatory Chinese laws and regulations regarding notification.

Certification

There are currently no requirements under mandatory Chinese laws and regulations regarding certification. There is, however, is a recommended certification rule published by Chinese regulatory authorities (SAMR and CAC)–*the Implementation Rules on Mobile Internet Application (App) Security Certification (CNCA-App-001)* (the "App Certification," only available in Chinese here). The App Certification is based on the standards under the *Information Security Standards*, which is very similar to GDPR. The procedure for obtaining the App Certification includes:

- Making an application
- Accepted by the certification bodies
- Technical verification
- On-site review
- Deciding to certificate
- Making compliant
- Post-certification audit

It generally takes 90 working days to obtain the App Certification after the application date.

Registration

There are currently no requirements under mandatory Chinese laws and regulations for network operators to register their personal information processing activities or to register their DPO.

12.3. Application to Digital Advertising

There are currently no requirements under mandatory Chinese laws specifically relating to notification, certification, or registration in the context of digital advertising.

13. DATA PROTECTION OFFICER

13.1. Overview

There are currently no requirements under mandatory Chinese laws to appoint a DPO. CSL requires network operators to determine the persons in charge of cybersecurity and carry out the responsibility for cybersecurity protection, but we understand this is different from the concept of DPO under GDPR as it is focused on cyber security rather than data protection, has to follow the instructions of companies, and also assumes responsibility for the company's non-compliance with CSL.

There are DPO requirements under the Information Security Standards, which are quite similar to those under GDPR. This is not mandatory but encouraged as best practice. Under Article 11.1(b) of Information Security Standards, personal information controllers must appoint a person and department responsible for personal information protection. The person responsible must be someone with relevant management experience and data protection expertise and must participate in important decisions on personal information processing activities and report directly to the organization's principal. The responsibilities include:

- Coordinating the internal personal information security efforts of the organization and bearing direct responsibility for personal information security.
- Organizing the development of a personal information protection work plan and supervising its implementation.
- Drafting, issuing, implementing, and regularly updating personal information protection policies and related procedures.
- Establishing, maintaining, and updating a list of the personal information the organization possesses (including the type, amount, source and the recipient of the PI) and the policy for access authorization.
- Carrying out personal information security impact assessments, putting forward measures, and suggestions for personal information protection and supervising the rectification of security risks.
- Organizing personal information security trainings.
- Conducting testing before the release of products or services to avoid unknown collection, use, sharing, and other processing activities.

- Publishing information such as the channel for complaints and tip-off, and accepting and dealing with the complaints and tip-offs.
- Conducting security audits.
- Liaising with the supervision and management departments to inform them of or report to them the status of personal information protection and incident handling.

Please refer to Section 16.1(d)(1) regarding the registration requirement of appointing a data protection officer introduced under the Draft PIPL.

13.2. DPO – Compulsory Appointment (Yes/No)

Not currently – please see above.

If the Draft PIPL is finalized and implemented as is, companies in China are obligated to appoint a DPO if the volume of personal information processed by them reaches the quantity specified by the competent authority (such quantity has not been clarified yet).

13.3. Requirements

No mandatory requirements but see above for best practice.

13.4. Application to Digital Advertising

There are currently no requirements under mandatory Chinese laws for network operators to appoint a DPO. However, to comply with their cyber security obligations most network operators will appoint a person in charge of cyber security (as discussed above). For larger companies, they may follow the requirement to appoint a DPO under the Information Security Standards and provide the DPO with resources to manage personal information protection within the company.

If the Draft PIPL is finalized and implemented as is, the advertisers and publishers in China may be obligated to appoint a DPO if the volume of personal information processed by them reaches the quantity specified by the competent authority (such quantity has not been clarified yet).

14. SELF-REGULATION

14.1. Overview

- **Are there any industry-self regulatory schemes in place in the jurisdiction?**

Yes. The *Industry Standard Framework of China Internet Targeted Advertisement Customer Information Protection (2014)* ("Industry Targeted Advertisement Framework"), published by the Interactive Network Branch of China Advertising Association, is a self-regulated industry scheme which applies to targeted digital advertising

(i.e., advertising sent to specific devices based on the collection and profiling of the user's personal information). The obligations for organizations under the Industry Targeted Advertisement Framework include:

- Implementing an internal training program and provide training to employees and suppliers (if necessary).
- Complying with the obligations of data minimization and necessity.
- Providing privacy notice to users and notifying users when the notice is first published or substantially amended.
- Allowing users to control the personal information processing for the purpose of internet targeted advertising, such as the opt-in and opt-out mechanism, consent for data sharing, and withdrawing consent.
- Taking measures to keep data secure.
- Obtaining consent when processing sensitive personal information.
- Implementing a data violation and breach response plan.
- Implementing a search result moving mechanism when providing search services.
- Establishing and publishing effective channels for personal information security complaints and reports.
- Disclosing the means, purpose and retention period of precise location information and the directory information of mobile devices before providing mobile services in a wireless environment.

Organizations participating in the Industry Targeted Advertisement Framework are audited by the third parties appointed by the Interactive Network Branch of China Advertising Association.

Is the framework widely adopted?

Please note the framework is not a mandatory law, but rather a self-regulation framework made by the Interactive Network Branch of China Advertising Association and its members. If a company is not the member of the Interactive Network Branch of China Advertising Association, they can choose whether they want to follow the standard. Since the laws are changing so fast in China, the use of these types of standards are also questionable.

How do companies actually meet the opt-in/opt-out requirements?

For the collection of the common personal information on websites, the standard of consent is the same as the statutory requirements (i.e., implied consent is permissible). However, users can choose to opt-out, for example by clearing cookies via their browser settings or sending an email request to the publisher.

When collecting sensitive personal information, express consent is needed, and the collection and processing of sensitive information must also be highlighted within the privacy policy. In practice, some companies use a pop-up on their website or a special notice to notify users when collecting sensitive personal information.

For mobile apps, companies generally choose to comply with the Measures for Apps Operators as this is a mandatory law and actively enforced.

Are there any technical specifications that need to be met?

Yes, the framework includes technical measures that should be taken. Generally, companies must ensure personal information is confidential and secure from data breaches. Except for that general requirement, there are also some more detailed requirements:

1) Organizations must take reasonable and necessary measures to de-identify personal information.
2) Without user's consent, organizations may only share de-identified information with third parties, and the data recipient must promise that it will not re-identify the information and only use it for the purpose of target advertising or other purpose which have been informed to the users.
3) if the data recipient discloses the information to other third parties, the third parties must also comply with the same requirements.

Are there any signal-based programs used in the territory to assist with digital advertising compliance?

We are not aware of any signal-based program to assist with digital advertising compliance in China.

14.2. Application to Digital Advertising

Please see above – the Industry Targeted Advertisement Framework applies to digital advertising where the advertisement is sent to specific devices based on the collection and profiling of users' personal information. The Industry Targeted Advertisement Framework does not apply in three scenarios:

- Common, undifferentiated advertising.
- Advertising monitoring not for the purpose of targeted digital advertising.
- Behaviors of placing advertisements in real time on the webpage or application corresponding to the user's operation on the Internet.

15. PENDING PRIVACY BILLS

15.1. Personal Information Protection Law ("PIPL")

Overview

The *Personal Information Protection Law* was released in draft form ("Draft PIPL") for public comments on October 21, 2020 and April 29, 2021. Once passed, PIPL will be the first comprehensive and dedicated law governing personal data protection in China and will function jointly with the Civil Code and other laws and regulations.

The ***Draft PIPL*** incorporates and integrates the basic principles in the Civil Code and CSL systematically, covering the entire lifecycle of personal information processing. It also absorbs the legislative experience of other jurisdictions in the data protection area (for example, GDPR) and crafts a unique and suitable path for personal information protection in China.

As a general note, the ***Draft PIPL*** set out the following key principles of personal information protection:

- Lawfulness and legitimacy
- Legitimate purpose and data minimization
- Transparency
- Accuracy
- Accountability and Security

Key Points

(a) Scope of Application

The ***Draft PIPL*** applies to all processing activities of a data subject's personal information that take place within the territory of China, regardless of the data subject's nationality or the personal information processor ("PI processor").

(b) Extraterritorial Jurisdiction

The ***Draft PIPL*** confers the necessary extraterritorial applicability to personal information processing activities conducted outside China if the purpose is to provide products or services to data subjects located in China, or for analyzing and evaluating the behavior of such data subjects.

Further, the ***Draft PIPL*** requires that overseas PI processors falling within the jurisdictional scope should set up a dedicated agency or designate a representative within China to be responsible for personal information protection matters, whose name and contact information should be submitted to the China data protection authority. Such agencies or representatives could potentially face penalties for violations of PIPL by the PI processor they represent.

(c) Definitions

"**Processing**" of personal information refers to the collection, storage, use, processing, transferring, sharing, and disclosing of (and other activities relating to) personal information.

"**Personal Information**" refers to a variety of information that is recorded by electronic or other means relating to an identified or identifiable natural person, excluding any personal information that has been anonymized.

"**Sensitive Personal Information**" refers to personal information that may lead to discrimination or serious harm to the safety of persons or property if disclosed or unlawfully used. Examples include information relating to race, ethnicity, religious beliefs, personal biometrics, medical health, financial information, and personal whereabouts.

"Personal Information Processor" or "PI processor" (as defined below) refers to organizations and individuals that independently determine the processing purpose and processing methods and other matters relating to processing of personal information. This is akin to the concept of "data controller" under GDPR.

"Anonymization" refers to the processing of personal information in a manner such that it is impossible to identify specific individuals, and also the identification is unable to be recovered. By contrast, "de-identification" is defined as processing of personal information such that it is impossible to identify specific individuals without the use of additional information. The ***Draft PIPL*** sets higher standards for "anonymization" than "de-identification."

"Automated Decision Making" means activities of making analysis, assessment, or decision automatically via computer applications on the personal aspects (such as behavior, habits, personal preference, interests, economic situation, health, and credit) using the data subjects' personal information.

(d) PI Processors' Rights and Responsibilities

Under the ***Draft PIPL***, PI processors are required to implement holistic internal data governance measures commensurate with potential risks and impacts in order to ensure the security and compliance of processing activities. For instance, PI processors should establish internal systems and policies, conduct regular training, and implement technical security measures.

The ***Draft PIPL*** imposes the following specific requirements for PI Processors:

1. Data Protection Officer (DPO)

PI processors that process personal information that exceeds certain volume thresholds should designate a data protection officer to be responsible for monitoring its processing activities and security measures. The name and contact information of the DPO should be publicly available and submitted to data protection authorities. The volume threshold amount is pending further guidance, and it remains unclear whether the DPO needs to be an employee or internal staff of the PI processor.

Relatedly, as noted above, for any offshore PI processor subject to extraterritorial jurisdiction of PIPL, a local representative or agency within China is required.

2. Audits

A PI processor is required to regularly audit its data processing activities and security measures.

3. Risk Assessment

PI processors should conduct risk assessments prior to the following data processing activities:

- Processing sensitive personal information.
- Using personal information to conduct automated decision making.
- Entrusting third parties to process personal information.

- Providing personal information to third parties or the public.
- Exporting personal information.
- Other personal information processing activities that will impose a major impact on data subjects.

The report of the risk assessment and records of processing activities should be retained at least for three years. To be distinguished from the requirement of audits on a regular basis, the risk assessment should be conducted prior to these specified processing activities.

4. Additional Obligations for PI Processors Operating Mega Internet Platforms

The following additional obligations must be followed by the PI processor providing fundamental Internet platform services with a significant number of users and complex business models:

- setting up an external independent supervisory committee to supervise personal information processing activities.
- suspending services if the service providers or the relevant products severely violate laws and regulations in their processing of personal information.
- publishing periodic social responsibility reports in order to be supervised by the society.

(e) Legal Bases for Data Processing (Consent and Exceptions for Consent)

Legal Bases. CSL provides that a data subject's consent and legal obligations are the lawful bases for processing personal information. The ***Draft PIPL*** takes a further step to specify additional non-consent bases which include (i) conclusion or performance of contract(s); (ii) responding to public health incidents or for the protection of the life, health, and property of data subjects in emergency cases; (iii) acting in the public interest for news reports or media supervision purposes within a reasonable scope; (iv) processing publicly-available personal information within the reasonable scope; and (v) other circumstances provided by laws and regulations. It is worth noting that the last basis ("*other circumstances provided by laws and regulations*") is a "catch-all" clause.

The ***Draft PIPL*** does not allow for the collection and processing of personal information on the basis of the "legitimate interests" of corporate entities.

Consent Requirements. The ***Draft PIPL*** reiterates and clarifies the informed consent principle. This means that a data subject must be fully informed before providing his/her consent, and such consent must be freely and unambiguously given. In the event of any change of data processing purpose, method or categories of personal information involved, a new consent should be obtained.

Data subjects have the right to withdraw their consent in a convenient way, but a PI processor cannot refuse to provide products or services on the grounds that the data subject does not provide consent, or withdraws his/her consent, except where processing is necessary for the provision of such products or services. That being said, any withdrawal of consent will not affect the processing activities based on such consent prior to the withdrawal.

The Draft PIPL, for the first time, stipulates a "separate consent" requirement in certain circumstances, including for processing sensitive personal information, sharing data with third parties, disclosing personal information to the public and transferring personal information outside of China; however, there remains uncertainty regarding how this "separate consent" can be obtained in practice.

In consistency with the Children's Measures, consent must be obtained from the parents or legal guardian of minors/children under the age of 14.

(f) Notices

To obtain the data subject's "informed" consent, a PI processor is required to inform a data subject of the following information and any subsequent changes thereof in a conspicuous way using clear and understandable language: (i) identity of the PI processor and contact details; (ii) purposes and methods for processing; (iii) categories of personal information to be processed; (iv) retention period; and (v) methods and procedures for such data subject to exercise his/her rights. However, it remains to be further clarified by PRC regulators as to how to satisfy this requirement on display of the notice.

(g) Data Retention

The retention period of personal information should be limited to the minimum period necessary for achieving the data processing purpose, unless otherwise provided by laws and regulations.

Without affecting any deletion requests from data subjects, the PI Processor is required to delete personal information under the following circumstances:

- the processing purpose has been achieved, or such personal information is no longer required for the processing purpose;
- the PI Processor has ceased to provide products or services, or the agreed retention period has expired;
- the data subjects have withdrawn their consent;
- the PI Processor's processing of personal information violates any laws, administrative regulations or agreements; and
- other circumstances provided by laws and administrative regulations.

(h) Data Sharing and Outsourcing

Entrusted Party. A PI processor is required to enter into an agreement with the entrusted party on the purpose, period and method of the entrusted processing, categories of personal information to be processed, protection measures, and rights and obligations of both parties. A PI processor should also supervise the entrusted processing activities. Accordingly, the entrusted party must process personal information on the basis of the parties' agreement and within the agreed purpose and method. The PI processor is required to return or delete the personal information upon termination of the agreement or in any case where the agreement is void, revoked or not effective, and must

not retain any personal information. Without consent from the PI processor, the entrusted party cannot outsource or entrust any other party to process the personal information. An entrusted party should also bear the applicable obligations of the PI processor under the ***Draft PIPL*** and take the necessary measures to ensure the security of all processed personal information.

Other than the aforesaid requirements on engaging an entrusted party, the ***Draft PIPL*** does not clearly differentiate the concepts of "Data Controller" and "Data Processor" as the terms defined under GDPR.

Joint Processor. In circumstances where two or more PI processors jointly decide the purpose and method of personal information processing, the joint PI processors should agree on their respective rights and obligations. Nevertheless, the PI processors will assume joint liability and data subjects can exercise their rights against any of the joint PI processors.

Data Sharing with Third Parties. As referred to in the above consent requirements, separate consent must be obtained for sharing personal information with third parties, for which purpose PI processors should notify data subjects of the third party's identity, contact information, processing purpose, processing method and categories of personal information. In the event that the third-party recipient intends to process the received personal information out of the scope of the original purpose or method, consent from data subjects should be re-obtained.

Also, the risk assessment requirements will apply for entrusted processing as well as data sharing with third parties.

(i) Data Subject Rights

Following the legalization of a data subject's rights in CSL and the Civil Code, the ***Draft PIPL*** expands the scope of data subject rights, in addition to right to be informed, right to access and request for a copy of personal information, right to rectify, right to withdraw consent, right to erasure under circumstances; two additional data subject rights (i.e.,) (a) right to object processing, and (b) right to explanation and reason have been included.

With respect to automated decision-making that has a major adverse impact on personal rights and benefits, data subjects are entitled to request an explanation from the PI processor. They may also object to the PI processor using automated decision-making as the sole approach to making decisions. In this regard, if the PI processor uses automated decision-making for promotion activities or push notifications, said PI processor is required to make an option available for data subjects so that such activities can be conducted without individual profiling, or allow data subjects to reject such promotion activities or push notifications. Prior to the release of the ***Draft PIPL***, this requirement was reflected as a non-mandatory national standard for personal information protection, which is seen as the best data protection practice. This indicates that the ***Draft PIPL*** intends to impose a stricter personal information protection regulatory regime.

Additionally, the rights to the personal information of a deceased person may be exercised by his/her close relatives.

(j) Data Localization and Cross-Border Data Transfer

The ***Draft PIPL*** addressed the heavily debated issue of data localization and cross-border data transfer, providing

several option mechanisms for PI processors. Regardless of which mechanism is adopted, a separate consent from a data subject should be obtained, and the PI processor should conduct a risk assessment prior to the transfer.

The ***Draft PIPL*** supplemented the data localization requirements for CIIO under CSL, extending the obligation to a wider group of processors. For CIIO and other PI processors that process personal information reaching a certain threshold amount, personal information collected and generated within the territory of China must be stored within China, and cross-border data transfer is subject to security assessment by cyberspace administrative authorities.

At the same time, the ***Draft PIPL*** provides other PI processors more options to transfer personal information collected out of China, which include:

- Security assessment by cyberspace administrative authorities.
- The ***Draft PIPL*** does not spell out the details of security assessment. The Draft Security Assessment Measures can shed some light on the intended regulatory approach at this conjuncture (please refer to our detailed advice below).
- Certification issued by a professional organization as authorized by cyberspace administrative authorities.
- (It remains unclear what the certification requirements are, and which are considered as qualified certifying institutions, which would be pending further clarifications from the relevant authorities.)
- Enters into agreement based on the standard contract clause formulated by cyberspace administrative authorities with foreign data recipients to ensure that data recipients process personal information in accordance with the standards under the PIPL
- Other circumstances as may be provided by applicable laws and regulations and conditions as may be prescribed by the cyberspace administrative authorities.

Consistent with the draft Data Security Law, approval should be obtained from data protection authorities prior to transferring any personal information stored within China to foreign authorities.

(k) Data Breach Notification

A PI processor should take remedial measures immediately once it is aware of unauthorized disclosure of personal information and notify the data protection authority and the responsible personnel. Such notification should include: (i) reasons for data breach; (ii) categories of personal information and potential impacts; (iii) remedial measures already taken; (iv) how data subjects can mitigate the impacts; and (v) contact information of the PI processor.

Although the PI processor may determine not to notify the affected data subjects provided that it can "effectively" prevent harm caused by such data breach, the data protection authority has the power to override the decision and request the PI processor to notify affected data subjects if the authority is of the view that the data breach is likely to cause harm to data subjects.

(l) Data Protection Authority

Authorities responsible for protection of personal information include CAC, relevant departments of State Council and local governments at the county level or above. Data protection authorities have the power to, among others, conduct on-site investigations and in-person interviews, audit relevant documents and materials, and confiscate illegal gains.

(m) Penalties

Administrative Penalty. The ***Draft PIPL*** has greatly increased penalties on top of CSL-the capped amount of fines for serious violations is RMB 50 million (approx. US$ 7.4 million) or 5% of the preceding year's turnover of the violator. However, the ***Draft PIPL*** remains silent on whether the specific entity or the whole company group will be involved or whether the preceding year's turnover is global or just limited within China. Other adverse penalties and consequences include rectification orders, confiscation of illegal gains, business suspension, revocation of business licenses, etc. Also note that simultaneously, directly responsible personnel may face fines of up to RMB 1 million (approx. US$ 152,100).

Shift of the burden of proof for personal information infringement. In any civil claim concerning personal information infringement brought by the data subject, it will be assumed that the PI Processor is liable for the infringement upon the data subject's personal information rights unless the PI Processor can prove that they are not at fault.

15.2. Data Security Law ("DSL")

Overview

The Data Security Law ("DSL") was passed on June 10, 2021 and will come into effect on September 1, 2021. The ***DSL*** will have a profound impact on data security governance and personal information processor practices.

The ***DSL*** intends to establish a data security system by classifying data into different categories based on the importance of data and potential impact/influence on national security or public interest, etc., and then applying the respective security measures. Under this framework, processors of "important data" are subject to more stringent data protection obligations (as further clarified below); however, the ***DSL*** does not define "important data" or provide any guidance. That said, the Draft Measures for the Administration of Data Security ("Draft Data Security Measures") released by CAC in May 2019 defined "important data" as *"the data, if leaked, that may directly have impact on national security, economic security, social stability or public health and safety. Examples of important data given in the Draft Data Security Measures include unpublished government information, large scale/coverage of population data, genetic and health data, geoinformation and mineral resource data, excluding personal information and network operators' production and operation related information and internal management information."*

Although the ***DSL*** seems to place emphasis on the national governance of data security, there are several systems that have brought widespread concern, especially in connection with the classification of important data, national data security review, and data export. The current DSL only lays out the skeleton of such systems and remains silent

on operational rules or implementation practices. As such, below we have summarized points based on our reading of the ***DSL*** for reference purposes.

- **National, Local and Industry Level of Data Classified and Levelled Protection System**

  The ***DSL*** proposed that a data-classified and levelled protection system be established at the national and local level, as well as by industries, whereby data will be classified into different categories and various levels of protection requirements will be applied in terms of the importance of data and the extent of harm.

  Data related to national security, the lifeline of the national economy, important aspects of people's livelihoods, and major public interests are state-level core data, and thus are subject to more stringent scrutiny.

  Each region and government department must determine the catalogue of important data within that region, department, and the corresponding industries and sectors on the basis of the classified data protection system, and impose stricter protection requirements on the data within the scope of such catalogues.

- **National Data Security Review System**

  The ***DSL*** proposed a security review system under which data activities affecting (or likely to affect) national security will be subject to national review. Despite the uncertainties of the responsible authority and assessment standards, it shows some connection with the security review requirement for CIIO under CSL.

- **Export Control**

  Data falling under the scope of "controlled item" relating to international obligations and national security will be subject to export control regulations.

- **Restrictions on Cross-border Transfer of Important Data**

  CIIOs must comply with the relevant requirements under the CSL in terms of transferring important data out of China. Cross-border transfer of important data collected and generated in China by other data processors will be subject to separate rules.

Despite the fact that the *DSL* is seen as one of the most important laws in China's data protection regulatory regime, it only sets out certain general principles and lacks clear detailed guidelines on how to enforce such principles. Hence, we expect that further regulations and rules will be introduced after the *DSL* comes into effect.

Key Points

(a) Scope of Application

The ***DSL*** applies to all data activities carried out within the territory of China.

(b) Extraterritorial Jurisdiction

Art. 2 of the ***DSL*** provides that the DSL also applies to entities and persons located outside of China if their data activities may "harm the national security or public interests of China, or the legitimate rights of Chinese individuals or entities"–it is subject to further clarification on what kind of activities will fall within this scope.

(c) Definitions

"**Data**" refers to any electronic or non-electronic records of information.

"**Data Processing**" refers to the collection, storage, use, processing, transmission, provision, or publication, etc., of data.

(d) Data Security Protection Obligations

Chapter 4 of the ***DSL*** provides various data security protection obligations on entities and individuals carrying out data activities, including:

- Establish a data security management system, organize data security trainings, and adopt technical measures and other necessary measures to ensure data security. Use of the internet or other information networks to carry out data-processing activities must be done under the multi-level cyberspace protection scheme, and the relevant data security protection obligations described herein must be complied with.
- Strengthen risk monitoring and take remedial actions immediately when data security defects or loopholes are detected.
- Notify users and authorities in the event of data security incidents.

Processors of important data are required to appoint responsible data security personnel and set up management teams. Furthermore, such processors should conduct periodic risk assessments of their data activities and submit the reports to authorities.

Additionally, requests for data by foreign judiciary or law enforcement must be handled in accordance with the relevant international or bilateral treaties and conventions to which China has acceded. Without the prior approval of the competent PRC authorities, no organization or individual in China is permitted to provide any data to foreign judiciary or law enforcement. As this requirement may have a significant impact on multinational companies when they are involved in legal proceedings, investigations and regulatory enforcements brought by foreign governmental agencies where their activities in China are concerned, we expect that this provision will be further clarified by PRC regulators in order to implement this requirement in a practical manner.

(e) Authority

Local governments are responsible for data security in their respective regions. Public security authorities and national security authorities will take supervision responsibilities. Cyberspace administrative authorities are responsible for network-related data security matters.

(f) Sanctions

The ***DSL*** provides steep administrative penalties for violations of the ***DSL***, including:

- Entities that are in violation of data security management, risk monitoring or risk assessments obligations under the DSL and refuse to rectify, or that lead to significant consequences such as large amounts of data leakage, may face administrative sanctions including the revocation of their business license, business suspension, and a fine of up to RMB 2 million (*approx. US$ 313,120*), and the personnel directly responsible could be fined up to RMB 200,000 (*approx. US$ 31,312*).
- Violation of the requirements for the protection of state-level core data will entail a fine of up to RMB 10 million (*approx. US$ 1,565,600*). Additionally, an entity may also be ordered to suspend or temporarily close their business or have their licenses or permits revoked for such violations. Serious violations could even lead to criminal liabilities.
- Entities violating the obligations on the cross-border transfer of important data will entail a fine of up to RMB 1 million (*approx. US$ 156,560*). For serious violations, the fine amount could be increased to RMB 10 million (*approx. US$ 1,565,600*). Such entities may also be ordered to suspend or temporarily close their business or have their licenses and permits taken for their violations. The personnel directly responsible could also be fined up to RMB 1 million (*approx. US$ 156,560*).
- Entities failing to obtain prior approval for the provision of data to foreign judicial or enforcement agencies will receive a fine of up to RMB 1 million (*approx. US$ 156,560*). If a violation causes "serious consequences," the entity will entail a fine of up to RMB 5 million (*approx. US$ 782,800*). Similarly, such entities may be ordered to suspend or temporarily close their business or have their business licenses or permits revoked. The personnel directly responsible could also be fined up to RMB 500,000 (*approx. US$ 78,280*).

15.3 Measures for Security Assessment of Export of Personal Information (for public consultations) ("Draft Security Assessment Measures")

Overview

CAC published the draft Measures for Security Assessment of Export of Personal Information in June 2019, as part of the system for personal information protection.

Unlike the draft Measures for Security Assessment of Export of Personal Information and Important Data released by CAC in April 2017 ("2017 Draft Measures") whereby outbound provision of personal information and important data was intended to be subject to the same set of security assessment rules, it appears that CAC has opted to apply two separate sets of security assessment requirements for the cross-border transfer of personal information and important data. This is also in line with the current legislative approach to regulate personal information under

the Personal Information Protection Law, and important data under the Data Security Law, separately.

Also, it is worth noting that the ***Draft Security Assessment Measures*** were released prior to the release of the Draft PIPL, hence, we expect that the ***Draft Security Assessment Measures*** will be subject to further revision according to the cross-border transfer mechanisms stipulated under the Draft PIPL. As an implementation of regulations of CSL and PIPL, the ***Draft Security Assessment Measures*** is expected to serve as a clear and definitive guidance to clarify the detailed requirements and procedure for security assessment of outbound provision of personal information once passed.

Key Points

(a) Scope of Application

The 2017 Draft Measures proposed that a government-administered security assessment will be triggered only if specific thresholds (such as the quantity of the personal information and the nature of and the risk impact on the information and data being transferred) are crossed. However, the ***Draft Security Assessment Measures*** introduced a more aggressive and sweeping requirement which, if implemented as currently drafted, will capture all outbound flow of personal information from network operators in China without any trigger that is quantity or risk impact based. As described in the PIPL section, if the Draft PIPL is passed "as is", this requirement will be less aggressive and restrictive.

(b) Security Assessment for Cross-Border Transfer of Personal Information

The general rule proposed under the ***Draft Security Assessment Measures*** is that in order to transfer any personal information overseas, a network operator must conduct a security self-assessment and then file the self-assessment report with the provincial counterpart of CAC for its security assessment review.

Before a Network Operator can file for CAC's security assessment review of a proposed export of personal information, it must:

- Enter into a contract or other forms of legally binding document with the foreign recipient concerning the export of personal information (collectively, "Contract").
- Conduct a self-assessment of security risks associated with the intended export and the security safeguards and measures to be adopted to address such risks and prepare a security assessment report.

(c) Personal Information Transfer Contract Requirement

The requirement on concluding a Contract between the network operator exporting personal information and the foreign data recipient is akin to the concept of the data transfer agreement or the binding corporate rules or BCR (as the internal rules for data transfers within multinational companies) stipulated under GDPR. Instead of providing model data transfer clauses to be incorporated into or referenced in the Contract, the ***Draft Security Assessment Measures*** provide that the Contract must contain the following contents and information:

- The purpose of personal information export, the types of exported personal information and the period of retention of exported personal information by the foreign data recipient.
- The relevant data subjects shall be the beneficiaries of the provisions concerning rights and interests of data subjects contained in the Contract.
- When the legitimate rights and interests of the relevant data subjects are infringed, they shall be able to, by themselves or through an attorney, seek indemnity from the network operator exporting their personal information, the foreign data recipient, or both of them who shall then indemnify the data subjects in the absence of evidence that they are not responsible for the infringement.
- The Contract shall be terminated or a new security assessment should be conducted where the legal environment of the jurisdiction where the foreign data recipient is located has changed and resulted in the Contract not being capable of being performed.
- Unless the foreign data recipient has destroyed the exported Personal Information or otherwise anonymized such personal information, the responsibilities and obligations of the network operator and the foreign data recipient shall not be exempted as a result of termination of the Contract.

For network operators that have already signed data transfer agreements or BCRs for the purpose of compliance with GDPR, there is a strong argument that they may rely on such existing documents with their overseas affiliates or counterparties, provided that these documents include provisions that conform with the Contract requirements stipulated under the Draft Security Assessment Measures.

(d) Ongoing Compliance Requirements for Cross-border Transfer of Personal Information

In addition, a network operator transferring personal information overseas will be required under the ***Draft Security Assessment Measures*** to establish and maintain records of exporting personal information for five years covering the certain aspects of transferred personal information[2]. A network operator shall submit an annual report on its export of personal information and the status of performance of the Contract(s) within the relevant calendar year to the provincial counterpart of CAC by December 31 of each calendar year.

[2] The information includes:
(1) when (time and date) outbound provision of personal information is conducted.
(2) identity (name, address and contact methods) of the foreign data recipient(s).
(3) type and volume of the exported personal information and level of sensitivity.
(4) other information that may be required by CAC.

(e) Authority

Cyberspace administrative authority at provincial level will be responsible for the security assessment.

(f) Review Timeframe

Although the ***Draft Security Assessment Measures*** stipulate that CAC's security assessment review must be completed within 15 days which may be extended if the circumstance is complicated, it is also questionable whether provincial counterparts of CAC would have sufficient manpower and bandwidth (even with assistance from external experts and institutions designated by CAC) to handle the vast volume of security assessment applications that companies within their respective provincial jurisdictions will submit in accordance with this 15-day timeframe.

(g) CAC's Ongoing Monitoring of Personal Information Export

Aside from receiving the annual reporting and the ad-hoc reporting submitted by network operators with respect to their respective personal information exports, the provincial counterparts of CAC are authorized under the ***Draft Security Assessment Measures*** to regularly inspect network operators' actual practices of personal information export and the performance of the Contracts included in their security assessment review applications. The provincial counterparts of CAC may request network operators (and to cause the foreign data recipients) to take remedial measures when they become aware of circumstances where data subjects' legitimate rights and interests are infringed upon as a result of exporting their personal information or where data breach incidents occur. CAC may also request a network operator to suspend or cease personal information export where:

- An incident of a relatively major data breach or data misuse occurs to the network operator or the foreign data recipient(s).
- The relevant data subjects are unable to safeguard or have difficulty in safeguarding their legitimate rights and interests (i.e., they are not able to exercise their rights as contemplated under the applicable Contract or as informed by the network operator exporting their personal information).
- The network operator of the foreign data recipient is not capable of safeguarding the security of the exported personal information.

(h) Extraterritorial Jurisdiction

Where an overseas entity directly collects the personal information within the territory of China through the Internet, the overseas entity should perform the obligations of the network operators under this ***Draft Security Assessment Measures*** via its legal representative or agency within China.

This requirement is drafted in a rather vague manner and may be quite confusing to a certain extent (e.g., whose legal representative or which domestic institution should be designated), it literally means that CAC's intention is for foreign companies collecting personal information from data subjects residing in China to also designate a representative in China to undergo the two-step security assessment process. However, it is unclear how CAC and its provincial counterparts would be able to enforce the relevant requirements on foreign companies, especially

those that do not have any registered presence in China. This requirement having been further developed and reflected in the Draft PIPL.

15.4 Draft Measures for the Administration of Data Security ("Draft Data Security Measures")

Overview

The ***Draft Data Security Measures*** released on May 28, 2019 regulates the security of both personal information and important data and lays down various obligations of network operators.

The ***Draft Data Security Measures*** are generally seen as an implementation regulation of the CSL and the DSL, however it was released prior to the release of the DSL and the Draft PIPL. Hence, we expect that the ***Draft Data Security Measures*** will be further revised in order to further address the principles concerning data processing in general set out in the DSL without creating any conflicts with the requirements set out in the Draft PIPL concerning personal Information.

Key Points

(a) Scope of Application

The ***Draft Data Security Measures*** cover the activities of data collection, storage, transmission, processing, and use, etc. as well as the protection and administration of data security. Activities for purely family/personal reasons will not be covered by this draft.

(b) Definitions

Prior to the release of the ***Draft Data Security Measures***, Important Data is strictly regulated under PRC law, but the term "Important Data" has not been specifically defined in any effective laws or regulations. The ***Draft Data Security Measures***, for the first time, propose to define Important Data as:

"the data, if leaked, that may directly have impact on national security, economic security, social stability or public health and safety."

Examples of important data given in the ***Draft Data Security Measures*** include unpublished government information, large scale/coverage of population data, genetic and health data, geoinformation and mineral resource data, excluding Personal Information and Network Operators' production and operation related information and internal management information.

According to this definition, network operators' internal business and management data and information would not be considered important data for the purpose of the PRC data protection laws and regulations. However, there is no further interpretation or guideline to clarify what kind of data constitute internal business and management data and information.

(c) Exterritorial Jurisdiction

The state could take measures to deal with data security risks and threats arising outside the territory of China. Given that there is no definition for "risks and threats," this could confer overreach into other jurisdictions.

(d) Notification Requirements for Collection and Processing Personal Information

Following the requirement under PRC Cybersecurity Law, network operators should develop and disclose their rules for collection and use of personal information through websites, applications, or other products. Such rules should be explicit, specific, in plain language and easily accessible.

Such rules can be included in a privacy policy or made available to users by other means; if included in a privacy policy and should be relatively centralized and clearly indicated.

The ***Draft Data Security Measures*** set out comprehensive disclosure requirements for such rules, which include, among others,

- Basic information of network operator.
- Name and contact information of the person responsible for data security.
- The purpose, category, quantity, frequency, method and scope of personal information collection and use.
- The retention location and period, and disposal methods
- Rules for sharing personal information with third parties.
- Personal information security protection strategies.
- Approaches and methods by which the personal information subjects can withdraw consent, and access, rectify or delete their personal information.
- Channels for complaints and reports.

(e) Consent

Under the ***Draft Data Security Measures***, network operators can only collect personal information on the basis of a user's informed consent of Rules. Any use of personal information outside the original scope of rules is subject to consent from data subjects.

Network operators are not allowed to force or mislead users to provide consent by means of function bundling or default authorization, on the grounds of improving user experience, targeted push notification or new products development, etc. Network operators cannot refuse to provide the core functions of network products based on the reason that users do not consent or withdraw the consent for collection of personal information beyond the necessary scope for the operation of core functions. Further, no network operator may discriminate against personal information subjects (e.g., price difference) on account of different consent scope for information collection.

Minor's Consent. Legal guardian's consent must be obtained for collection of the personal information of minors

under the age of 14.

(f) Filing Requirements

Network operators that collect sensitive personal information or important data for business purposes are required to make a filing with the local cyberspace administrative authority. However, no clear implementation rules have been published with regard to the detailed procedure and documentation for such filing.

(g) Data Retention

Network operators must retain personal information within the period as specified in the Rules. Personal information should be deleted promptly after the termination of a user's account.

(h) Data Subjects Rights

Personal information subjects have the right to access, rectify or delete personal information or request to terminate their accounts.

(i) Targeted Push

If network operators use users' data and algorithms to push news or advertisements, the wording "Targeted Push (定向推送)" should be labelled in a prominent way. The function for users to stop receiving the targeted push should also be provided. Network operators are required to stop targeted push and delete related user's data and personal information if users choose not to receive the targeted push.

(j) Automated-Decision Making

Automatic data collection and access on websites should not interfere with the normal operation of websites, and network operators should stop doing so when they seriously affect the operation of websites. More specifically, the ***Draft Data Security Measures*** propose that if the automatic data collection traffic exceeds one third of a website's average daily traffic, such automatic data collection is deemed to severely interfere with the normal operation of the website and should be stopped.

For content (news, blogs, posts, comments, etc.) automatically generated via technologies such as big data and artificial intelligence, the content must be clearly marked as "Synthesis," and under no circumstances shall such content be generated for benefits or causing harm to others.

(k) Data Sharing with Third Parties

Network operators are obliged to assess the potential security risk and obtain consent from data subjects for sharing personal information with third parties. This issue has been further clarified in the Draft PIPL.

Network operators should conduct a self-assessment of the potential risk and submit for pre-approval by the competent supervisory authority or CAC in case the competent supervisory authority is unclear for the publication, sharing, trade, or cross-border transfer of important data. However, as mentioned in the above section, the scope of

Important Data has not been clearly defined and there is no clear guidance as to the procedure for such approval.

(l) Cross-border Data Transfer

For *important data* – export of important data should be pre-approved by authorities.

For *personal information* – the ***Draft Data Security Measures*** only provided that the export of personal information is subject to relevant regulations, which, based on current released drafts of laws and regulations, could include the PIPL and Measures for Security Assessment of Export of Personal Information.

(m) Security Obligations of Network Operator

Network operators are required to establish internal accountability and assessment systems, develop data security plans and conduct trainings, as required by applicable laws and regulations.

In connection with data processing and use, network operators should implement technical measures such as data classification, backup, and encryption to ensure the security of personal information and important data.

Obligation for third-party app. For third-party apps integrated into its platform, network operators are required to specify the data security requirements and supervise the data security management of such third-party apps. Network operators will be held fully or partially liable for losses caused to users due to data security incidents of third-party apps, unless the network operator can prove it was not at fault.

(n) Data Breach

In the event of any actual or suspected data breach incidents, network operators should promptly notify the data subject and report to the authorities as required by law. Similar to the Draft PIPL, there are no specific timing requirements for the notice.

(o) Data Security Responsible Person

Network operators that collect important data or sensitive personal information for business purposes should appoint the responsible person for data security.

(p) Authority

Cyberspace administrative authorities will supervise the security protection of personal information and important data.

(q) Sanctions

A Network operator that violates the Draft Data Security Measures may be subject to administrative sanctions including public exposure, confiscation of illegal gains, closure of website, business suspension and revocation of business license, etc.

iab.

India

Cross-Jurisdiction Privacy Project

1. THE LAW

1.1. Overview & Key Acts, Regulations, and Directives

Data protection in India is mainly governed by the Information Technology Act, 2000 ("**IT Act**") (English translation available here) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**Privacy Rules**") (English translation available here). The purpose and objective of enactment of the IT Act is to provide legal recognition for transactions that are carried out through electronic means and electronic communication. In pursuance of the enabling provisions of the IT Act, the Central Government framed the Privacy Rules.

The IT Act and the Privacy rules, inter alia, focus on identification of an individual through the various types of data collected by an entity. While the law is not clear as to what identification of an individual means, it has been understood as identifying different aspects of an individual, including but not limited to, name, geographic location, financial status, medical history, and government issued identification numbers. Furthermore, as standard practice across different sectors, data controllers are advised not to use personal data to discriminate or hurt the sentiments of the person in the course of processing such data.

The IT Act and the Privacy Rules mainly govern two categories of data: (i) personal information; and (ii) sensitive personal data or information.

As per the Privacy Rules, "personal information" means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a corporate entity, is capable of identifying such a person ("**Personal Information**"). Furthermore, the Privacy Rules also govern the collection and processing of sensitive personal data or information ("**SPDI**"), which includes, among other things, an individual's financial information, health and medical information, and biometric information.

The IT Act and Privacy Rules

The IT Act and the Privacy Rules act as enablers for digital commerce in India and do not expressly provide for data protection through privacy by design or the data protection regime as provided under the General Data Protection Regulation, 2016 ("**GDPR**"). Unlike the GDPR, these laws do not regulate or impose compliance requirements with respect to the collection or processing of ordinary Personal Information. Similarly, these laws do not require data controllers to enter into standard contracts or obtain any regulatory approvals to transfer Personal Information to affiliates and third parties.

The IT Act mandates that body corporate (e.g., companies, firms, sole proprietorships, and other associations of individuals engaged in commercial or professional activities) that handle SPDI maintain reasonable security practices and procedures and are liable to pay damages for any loss caused by their negligence in implementing

and maintaining reasonable security practices and procedures. While the IT Act is silent as to what constitutes " reasonable security practices and procedures", the Privacy Rules offer examples of these standards without providing a clear-cut definition.

The IT Act also prescribes criminal penalties, that include both imprisonment of up to three years and fines for persons, including intermediaries, who disclose Personal Information without the consent of the Data Subject (defined below), in breach of a relevant contract, or to cause wrongful loss or gain.

The Privacy Rules require companies to have a privacy policy, obtain consent when collecting or transferring SPDI, and inform the data subject ("**Data Subject**") of recipients of such collected data.

The Personal Data Protection Bill

The Indian Parliament is currently in the process of overhauling India's data privacy regime. In December 2019, the Government of India released the Personal Data Protection Bill, 2019 ("**PDP Bill**"). The PDP Bill, if enacted into law, would repeal the IT Act and Privacy Rules. At present, there is no clear timeline for the passage and enactment of the PDP Bill.

It should be noted that the PDP Bill is broadly consistent with the principles of the GDPR and also principles from the Supreme Court's ("**SC**") ruling in the Privacy Judgment (*defined below*), where the right to privacy was upheld as a fundamental right of an individual under the Indian constitution.

Our detailed assessment of the PDP Bill is provided in Paragraph 15 onwards.

1.2. Guidelines

There are no guidelines applicable to digital advertising in this jurisdiction.

1.3. Case Law

In *Kharak Singh v. The State of Uttar Pradesh and Others*, decided in 1962, the SC held that domiciliary visits by the police at night constitutes unauthorized intrusion into a person's home and a violation of liberty. In a majority judgment, the SC ruled that privacy was not a guaranteed constitutional right. However, it held that Article 21 of the Constitution was the repository of residuary personal rights and recognized the common law right to privacy.

Furthermore, in *Maneka Gandhi vs. Union of India*, the passport of Maneka Gandhi, a minister then, was impounded in "public interest." In this case, the meaning of the word " personal liberty" was again considered by the SC as Maneka Gandhi's passport had been impounded by the Central Government under Section 10(3)(c) of the Passport Act, 1967. Hence, no person can be deprived of such rights, except through procedures established by law. Since the State had not made any law regarding the regulation or prohibiting the rights of a person in such a case, the confiscation of the petitioner's passport was held to be in violation of Article 21 of the Constitution of India

and its grounds being unchallenged and arbitrary. The SC held that the personal life and liberty of a person must be understood in the broader and liberal sense. Considering this, a person's right to privacy and the liberty associated therewith can be understood in a broader sense.

In a Writ Petition filed before the SC in 2005, the petitioner stated that mobile telephone service providers and telemarketers violate the law by using the personal data of subscribers for their business purposes. The SC issued instructions to the Reserve Bank of India to institute measures to reduce such unsolicited calls.

In October 2018, a nine-judge SC bench, in *Justice Puttaswamy (Retd.) and Anr. v Union of India and Ors* [Writ Petition (Civil) No. 494 of 2012] ("Privacy Judgement") specifically held that right to privacy is a fundamental right under Article 21 of the Constitution and that it included, at its core, a negative obligation to not violate the right to privacy and a positive right to take all actions necessary to protect the right to privacy.

The SC recognized certain data protection principles such as data minimization, data retention, and data security. This paved way for the legislature to consider passing the law which specifically addresses data privacy and data protection. The judgement made several observations on the complex relationship between personal privacy and "big data" particularly in the context of how the judicious use of these technologies can result in the State achieving its legitimate interests with greater efficiency. One of the judges in this case identified concerns of surveillance and profiling, whereas with regard to private entities, he emphasized on the impact of big data and technology on the data intensive generation and its collection and use in a growing digital economy.

The Privacy Judgment changed the contours of Indian privacy law, the interpretation of the existing privacy rules, and raised the specter of a robust common law tort of violation of privacy, independent of statutory rules. The SC went on to clarify that any law that encroaches upon the right to privacy is subject to constitutional scrutiny and must meet the three-fold requirement for legality, necessity and proportionality.

Furthermore, the SC crafted a positive obligation on the government to enact legislation that adequately protects the right to privacy. Various High Courts frequently address data protection issues (e.g., export of data, transfer of data between group companies, and adequacy of consent) from a post-Privacy Judgment perspective. While there is no clear judicial trend yet, it is nevertheless evident that those entities engaging in data collection and processing efforts in India must evaluate and anticipate the impact of the Privacy Judgment on Indian data law.

1.4. Application to Digital Advertising

Application of data privacy law to digital advertising is in its nascent stage in India. While there are no specific provisions under the IT Act and the Privacy Rules that address data pertaining to digital advertising, provisions pertaining to Personal Information and SPDI would apply in certain instances. For example, if an advertising agency collects any information from a Data Subject, obligations of the advertising agency would depend on whether the data collected is Personal Information or SPDI. It should also be noted that there are no specific

provisions pertaining to a publisher in digital advertising. However, provisions regarding breach and contravention under the IT Act and Privacy Rules will accordingly apply to the activities of a publisher.

Further, if an advertising agency collects data from Data Subjects located in India, the advertising agency would be required to have a privacy policy in place. As per the Privacy Rules, it is mandatory for Data Collectors (defined below) to have a privacy policy in place that discusses handling of Personal Information or SPDI collected from the Data Subject. It should also be noted that the IT Act and Privacy Rules currently do not govern activities such as collection of pixels on publisher's pages.

The IT Act and the Privacy Rules do not contain any standards for anonymization or de-identification of data by the digital advertising agencies or the publishers.

For the purposes of this document, data collector means "body corporate" under the IT Act and Privacy Rules. The term body corporate means, "*any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities* ('***Data Collector***')."

2. SCOPE OF APPLICATION

2.1. To Whom Does the Laws/Regulations Apply, and What Types of Processing Activities are Covered/Exempted?

The Privacy Rules impose obligations on corporate entities and any persons who on behalf of a corporate entity process Personal Information, including companies, firms, and other associations of persons engaged in commercial or professional activities. The collection or processing of data by individuals is not covered under the scope of Privacy Rules.

2.2. Jurisdictional Reach

Overview

The IT Act has extra-territorial applicability in certain cases. As per Section 75, the provisions of the IT Act extend to any offence or contravention committed outside India by any person irrespective of his/her nationality, if the act or conduct constituting the offence or contravention involves a computer[1] , computer network[2] , or computer system[3] located in India. Therefore, in the context of data protection, the provisions of the IT Act and Privacy Rules

[1] The IT Act defines "computer system" as "a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programs, electronic instructions, and input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control, and other functions.

(Annotations continued on next page)

would apply if the collection or processing of personal information or SPDI involves a computer or computer system located in India.

Furthermore, there are no specific restrictions or requirements imposed on Data Controllers when Personal Information is transferred outside India. The IT Act and Privacy Rules do not impose any restrictions or requirements on the transfer of ordinary Personal Information to third parties. However, there are certain restrictions imposed when SPDI is transferred to a third party. As per the Privacy Rules, transfer of SPDI is only allowed if:

- The recipient ensures the same level of data protection that is adhered to by the Data Collector; and
- The transfer of SPDI:
  - » Is necessary for the performance of a lawful contract between the Data Collector and the Data Subject; or
  - » Has been expressly consented to by the Data Subject.

Therefore, while explicit consent is not required for transfer of ordinary Personal Information, the same is required for transfer of SPDI to a third party. Similarly, where SPDI is transferred to a third party, the recipient would need to ensure the same level of data protection as is provided by the Data Collector in India. Typically, this is ensured by parties by entering into a Data Transfer Agreement or Data Processing Agreement that sets out the minimum data security and protection measures to be implemented by the recipient.

In sum, the provisions of the IT Act will apply to persons outside India if the collection or processing of Personal Information or SPDI by such persons involves a Computer, Computer System, or Computer Network located in India.

---

[2] The IT Act defines "computer network" as "the inter-connection of one or more computers or computer systems or communication device through:
(i) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and
(ii) terminals or a complex consisting of two or more inter-connected computers or communication device whether or not the inter-connection is continuously maintained."

[3] The IT Act defines a computer as "any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network."

Application to Digital Advertising

For each scenario, we should ask how (if at all) does the Privacy Law apply to:[4]

1. serving the ad to the user
2. building a profile of the user
3. the publisher's legal obligations
4. the advertiser's legal obligations

Scenario 1 is the baseline scenario, where the user, publisher, and advertiser are all based in India, where it seems reasonable to assume the Privacy Law applies.

Scenario 1 (The baseline): A user residing in India (determined by IP address or geo identifier) goes onto an Indian domain and is served an ad by an Indian advertiser. The advertiser uses the user data to build a user profile.

As per details provided in Scenario 1, the obligations under the IT Act and Privacy Rules would fall upon the entity who collects the data of the user in the first instance. Accordingly, if the Indian domain collects data of the user, then the Indian domain becomes the Data Controller, and the user residing in India becomes the Data Subject. Depending on the type of data that is collected by the Indian domain, the Privacy Rules will apply accordingly. Furthermore, in case the Indian domain collects only Personal Information, there would be no obligations on the Indian domain. However, if the Indian domain collects SPDI from the user, obligations on the Indian domain will change accordingly.

Scenarios 2, 3, and 4 vary depending on the location of the user, publisher, and advertiser to test in each case the jurisdictional reach of the Privacy Laws.

Scenario 2 (User outside India): A Logged-on/signed-in user, known by the publisher to be an Indian resident, goes onto an Indian domain but the user's IP address or geo identifier indicates the user is outside India. An Indian advertiser serves an ad and uses the user data to build a user profile.

Q1: Does the answer change if this is a signed-out user, with no way of knowing where they are domiciled?

If the Computer, Computer System, or Computer Network is located in India, the provisions of IT Act will apply to all processing activities arising from that computer resource. However, if the user's IP address indicates that the

[4] NB. The application of the Privacy Laws to intermediaries has been deliberately omitted (this can be considered later if needed).
(Annotations continued on next page)

computer resource of the user is located outside India, the provisions of IT Act will not apply. It should be noted that the determining factor here is the location of the Computer, Computer Resource, or Computer Network but not the residential status of the user.

Scenario 3 (Publisher domain outside India): A user residing in India (determined by IP address or geo identifier) goes onto a domain outside of India. An Indian advertiser serves an ad and uses the user data to build a user profile.

A user residing in India would be considered a Data Subject. As long as the Data Subject is located in India and the advertiser uses the Data Subject's information to build a user profile, the IT Act and Privacy Rules will apply to the Indian advertiser and the Data Subject.

Q1: Does the answer change if the site host's content is aimed at Indian residents (e.g. a news aggregator with a section on Indian current affairs)?

No, the answer does not change if the site hosts content aimed at Indian residents. To reiterate, as long as the advertiser collects information from a Data Subject located in India, the IT Act and Privacy Rules still apply.

Q2: Does the answer change if the advertiser is based outside of India?

No, the answer does not change. The IT Act and Privacy Rules still apply even if the advertiser is based outside India.

Scenario 4 (Advertiser outside India): A user residing in India (determined by IP address or geo identifier) goes onto an Indian domain and is served an ad by an advertiser based outside India. The advertiser uses the user data to build a user profile.

In this scenario, the provisions of IT Act and Privacy Rules will apply to the user residing in India and the entity that collects data at the first instance to build a user profile. Therefore, the provisions of IT Act and Privacy Rules will apply to the advertiser based outside India if the advertiser collects data at the first instance and such data is collected from a Data Subject located in India.

Q: Does the answer change if the advertiser has an affiliate/group company based in India?

No, the answer will not change if the advertiser has an affiliate/group company based in India. The user residing in India will be the Data Subject. The advertiser based out of India will be the data controller/data processor. The IT Act and the Privacy Rules will apply to the entity that collects data at first instance from the Data Subject.

* * * End of Hypotheticals * * *

3. DEFINITIONS

3.1. Collect

The IT Act and Privacy Rules neither define the term "collect" nor the term "data collector." Correspondingly, the IT Act and Privacy Rules refer to the term "body corporate" instead of "data collector." The term "body corporate" has been defined as follows:

"any company and includes a firm, sole proprietorship, or other association of individuals engaged in commercial or professional activities."

Furthermore, the IT Act and Privacy Rules lay out certain obligations to be adhered by a body corporate. A body corporate is required to implement reasonable security practices and procedures for the protection of personal information and SPDI. Any person aggrieved by the activities of a body corporate may bring a private right of action against such body corporate which has contravened provisions of the IT Act or the Privacy Rules which render it liable to pay a penalty or compensation.

- "When a publisher allows an ad tech company's pixel on its page, who is deemed to "collect" personal information and incur legal obligations (e.g., controller/co-controller obligations under GDPR or "business" obligations under CCPA)—the publisher, the ad tech company or both?"

In case a publisher allows an ad tech company's pixel on its page, the ad tech company would be the Data Collector and accordingly, the ad tech company would have to adhere to the obligations of a Data Collector stipulated under the IT Act and Privacy Rules. However, if the ad tech company is placing pixels on behalf of the publisher, then the publisher will be treated as the Data Collector.

3.2. Data Processing (i.e., collecting, capturing, retaining, recording, organizing, structuring, storing, altering, retrieving, consulting, using, disclosing, transmitting, disseminating, making available, aligning, combining, restricting, erasing, destroying, or otherwise processing)

The IT Act and the Privacy Rules do not define "data processing."

3.3. Personal Information

As per the Privacy Rules, Personal Information means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available to an entity, can identify such a person. Indian law has recognized natural persons to mean human beings, therefore, differentiating natural persons from legal persons under the eyes of law.

In view of the above, information collected via cookies may be categorized as Personal Information, if it can be used independently or in combination with other information, to identify a person's identity.

Type of Information Collected	Does this Category Independently Constitute Personal Information? (Yes/No)	Qualifying Notes (if any)
IP Address	IT Act/Privacy Rules: No. PDP Bill: No	
Mobile Advertising IDs (IDFA, AAID)	IT Act/Privacy Rules: No. PDP Bill: No.	
Consumer identifiers such as: • User device ID • Publisher persistent ID/Cross-publisher cookie ID • Household ID	IT Act/Privacy Rules: No. PDP Bill: No.	
Hashed identifiers such as: • Hashed email • Hashed IP address	IT Act/Privacy Rules: No. PDP Bill: No	
User Agent such as: • Character string identifying the application • Operating system • Browser information, vendor, and/or version of the requesting user agent	IT Act/Privacy Rules: No. PDP Bill: No.	

Device Information such as: • Type, version, system settings, etc.	IT Act/Privacy Rules: No. PDP Bill: No	
Website Information such as: • Name • URL, etc.	IT Act/Privacy Rules: No. PDP Bill: No.	
Advertisement Information such as: • Placement • Title • Creative ID, etc.	IT Act/Privacy Rules: No. PDP Bill: No.	
Timestamps	IT Act/Privacy Rules: No. PDP Bill: No.	
Metrics such as: • Counts • Amounts of time	IT Act/Privacy Rules: No. PDP Bill: No.	
Event Data such as: (e.g., full URL including query string, referral URL)	IT Act/Privacy Rules: No. PDP Bill: No.	
Precise geolocation (latitude, longitude)	IT Act/Privacy Rules: Yes. PDP Bill: No.	
General geolocation (city, state, country)	IT Act/Privacy Rules: No. PDP Bill: No.	

- **Are pseudonymous digital identifiers *by themselves* personal information (e.g., IDFA, cookie IDs, proprietary IDs, IP addresses, etc.)? Please provide context to the above chart.**

While there is no specific regulatory guidance, IP addresses, IDFA or proprietary IDs and cookie IDs, may be regarded as Personal Information depending on the other information available to the body corporate and whether such body corporate has the tools necessary to combine such information to identify individual Data Subjects. Furthermore, pseudonymous digital identifiers by themselves do not constitute Personal Information.

- **If the answer to the above question is, "no," if a Company possesses a persistent digital identifier in Database 1 and has that same identifier in Database 2 with directly identifying information, does that render the pseudonymous information in Database 1 as personal information?**

Persistent identifiers by themselves are not considered Personal Information. However, they may be categorized as Personal Information, if they can be used independently or in combination with other information, to establish a person's identity by way of any identification number issued by the government. In the event where an entity possesses a persistent digital identifier in one database and has the same identifier in another database with directly identifying information, the pseudonymous information in the former database would constitute Personal Information because the company has the capability of establishing the identity of an individual in Database 1.

Where an advertising technology company uses a Mobile Ad ID ("MAID") with other identifying information of an individual such as his/her email address, the MAID will still not be generally considered Personal Information since the identity of the individual has not been established with such information. However, for example, if the information is used to establish the government identification number/code issued to an individual, then, such MAID will be considered Personal Information. While the law does not prescribe that persistent digital IDs would have to identify an individual with his/her identification numbers issued by the government, it should be noted that, in practice, such persistent digital IDs will be considered Personal Information.

- **Is a Company's possession of a pseudonymous identifier plus other non-directly identifying data (e.g., age, gender, precise or imprecise geolocation, user agent string, timestamps) considered "Personal Information"?**

No, a company's possession of pseudonymous identifiers along with other non-directly identifying data does not constitute Personal Information. Mere possession of such data does not qualify as Personal Information. As mentioned above, the identifier must be capable of establishing the identity of an individual. For example, data relating to age, gender, precise or imprecise geolocation will not constitute Personal Information. Such data will qualify as Personal information when the data in possession of the entity is used to identify or establish the identity of an individual.

- **Is a Company's possession of a pseudonymous identifier "Personal Information" if it can hire a service provider or otherwise engage in a transaction with a third party where the identifier *could* be matched to**

the person, *but* the Company chooses not to hire such service provider or undertake such transaction. Is the mere fact that this service is *potentially* available to match to the person sufficient to render that pseudonymous identifier as "Personal Information"?

No, mere ability of a set of data without establishing the identity of an individual does not constitute Personal Information.

- **What level of geolocation is Personal Information (precise vs. approximate)?**

  Does it need to be associated with an identifier to be considered Personal Information?

Any level of geolocation which extends to establishing the identity of a person constitutes Personal Information. For example, specific geolocation consisting of a person's residential address, thereby, directly or indirectly capable of identifying a person would constitute Personal Information. If multiple people live at a particular address, the geolocation which establishes the identity of the particular person amongst the others who live at the same address will be considered Personal Information.

- **Is a household identifier Personal Information? (Consider: If a company has a residential IP address (household level ID) and multiple unique device IDs (e.g., MAIDs for every mobile device in the house) associated with that IP address, would that affect whether the household identifier is considered personal information?)**

The IT Act and the Privacy Rules do not define "household identifier". Furthermore, there is no difference between "household level information" and "consumer information" under the IT Act and Privacy Rules.

In case an entity has an IP address that is of a residential address and multiple unique device IDs associated with the IP address, the household identifier in the form of residential IP address would not be considered Personal Information.

- **Is a hashed identifier Personal Information? (Consider: there are commercially available services that will take batches of emails encrypted using standard hashes and return (often a high percentage) of clear emails from them. Does that affect whether they are considered personal information, if all a company has to do is pay for the commercial service?)**

At present, the IT Act and Privacy Rules do not contain provisions pertaining to hashed identifiers. Additionally, the IT Act and Privacy Rules do not provide for any exemptions for the processing of Personal Information or SPDI that has undergone pseudonymization or anonymization. However, if the hashed identifier can be used to establish the identity of a person directly or indirectly, it would be considered Personal Information. If the hashed identifier contains information that is irreversibly de-identified or anonymized, such hashed identifier would fall outside the purview of Privacy Rules, since such information would no longer fall within the definition of Personal Information.

In the event, an entity offering commercial services to return encrypted emails in a clear form, information set out in those emails will be considered Personal Information as long as it enables the Data Collector to establish the identity of a person.

- **Is probabilistic information considered Personal Information?**

Please refer to our response above.

3.4. Sensitive Data

Under the Privacy Rules, SPDI is defined to include passwords, financial information (such as bank account, credit card, debit card or other payment instrument details), physical, physiological, or mental health conditions, sexual orientation, medical records and history, and biometric information. However, it does not include any personal data that is freely available or accessible in the public domain, or furnished under the Right to Information Act, 2005 or any other law. For instance, if a user visits a mental health information page (that has freely made such information available to the public) and uses information gathered there to target an advertisement for a mental health treatment facility, the data used will not be considered SPDI.

3.5. Pseudonymous Information

- **Is pseudonymous information considered Personal Information?**

The IT Act and the Privacy Rules do not define pseudonymous information. If digital identifiers can establish the identity of a Data Subject, they will be considered Personal Information.

While the IT Act and the Privacy Rules are not clear as to what identification of an individual means, in practice, it is understood as identifying different aspects of an individual including without limitation the person's name, residential address, bank account details, medical history, government issued identification numbers, etc.

- **Are persistent digital identifiers pseudonymous information (e.g., IDFA, cookie IDs, proprietary IDs, IP addresses, etc.)?**

There are presently no specific requirements for the use of cookies and other online tracking technologies in India. Persistent identifiers by themselves would not be categorized as Personal Information but may be categorized as Personal Information if they can be used independently or in combination with other information to identify a person's identity.

At present, the IT Act and Privacy Rules do not provide for any specific exemptions for the processing of Personal Information or SPDI that has undergone pseudonymization or anonymization. However, if the persistent digital identifier representing Personal Information can be re-identified into Personal Information, it may be considered Personal Information.

- **Does the law subject pseudonymous information to fewer obligations than "regular" personal information?**

The IT Act and Privacy Rules do not provide for any specific exemptions for the processing of Personal Information or SPDI that has undergone pseudonymization or anonymization.

3.6 Anonymized/De-identified Information

The IT Act and the Privacy Rules do not contain provisions that define anonymized/de-identified information.

- **Is there a difference between anonymized or de-identified data?**

The IT Act and Privacy Rules do not differentiate between anonymized data and de-identified data. Furthermore, " anonymized data" and " de-identified data" are not defined under the IT Act and Privacy Rules.

- **What common data categories are passed between publishers, advertisers, and ad tech companies that fall into this category when no persistent identifier is present (e.g., browser type, device type, operating system, app name, publisher site)?**

  N/A

3.7. Data Controller and Processor

3.7.1. Data Controller

The IT Act and the Privacy Rules do not define "data controller." However, the government distinguishes between: (a) an entity that merely processes Personal Information and SPDI on behalf of another corporate entity; and (b) an entity that by itself collects Personal Information and SPDI from a Data Subject, on the other. The distinction is drawn based on the activity of the entity i.e., processing of Personal Information and SPDI on behalf of another entity is differentiated from mere collection of Personal Information and SPDI from a Data Subject.

3.7.2. Joint Controller/Co-Controller

The IT Act and the Privacy Rules do not define "joint controller" or "co-controller."

3.7.3. Data Processor/Service Provider (i.e., an entity that is qualified as a processor or service provider under the law because it meets certain requirements and processes data pursuant to a permissible purpose on behalf of a controller/business)

Please refer to Paragraph 3.6 above.

Furthermore, while the Privacy Rules do not define a data controller and a data processor, the government has clarified that certain obligations prescribed under the Privacy Rules do not apply to a data processor that does not collect Personal Information or SPDI from a Data Subject, but merely receives such information from a Data

Collector on a principal-to-principal basis. For instance, a data processor is not required to obtain Data Subject's consent to receive his or her SPDI. Also, there is no requirement on the data processor to give the Data Subject the ability to access and rectify his or her information. The government has clarified that these obligations fall on the Data Collector only, and not the data processor.

3.7.4. Third Party (i.e., a third party that receives data from a business for non-business purposes and does not necessarily have specific requirements under the law as to such data, such as a third-party under the CCPA)

The IT Act and the Privacy Rules do not define "Third Party."

4. DATA CONTROLLER RIGHTS AND RESPONSIBILITIES

4.1. Overview

It may be noted that currently, Indian law does not explicitly define or distinguish between a data controller and a data processor. However, the Privacy Rules contain certain provisions relating to steps that are to be taken by an entity collecting SPDI which is set out in detail in 4.4.1 below.

4.2. Accountability

4.2.1. Overview

N/A

4.2.2. Application to Digital Advertising

N/A

4.3. Notice

4.3.1. Overview

Who must receive notice?

The IT Act states that a Data Subject should receive notice prior to collection of Personal Information and SPDI. However, there are no specific requirements related to providing notice of data collection for digital advertising purposes. Furthermore, there are no additional rules that require processors to provide additional notices.

When collecting Personal Information or SPDI from a Data Subject, the Data Collector must take reasonable steps to ensure that the Data Subject has knowledge of:

- The fact that the particular Personal Information or SPDI is being collected.

- The purpose for which the Personal Information or SPDI is being collected.
- The intended persons who will receive the Personal Information or SPDI; and
- The name and address of the entity that collects and the entity that stores the Personal Information or SPDI

The Data Collector would thereafter be required to obtain the explicit consent of the Data Subject in written or electronic form for the proposed collection and use of such SPDI. It is to be noted that there is no consent requirement for the collection of Personal Information (which does not contain or consist of SPDI).

In the event a user visits a website that collects Personal Information from the user (via cookies, sign-ups etc.), it will be sufficient if the website contains a privacy policy providing details of: (i) the fact that the data is being collected; (ii) the types of information that the website collects; (iii) the purpose for collection; and (iv) the recipients of the data. However, if SPDI is also collected, then a consent mechanism would be required to be built in to obtain consent from the user.

- **Are there any requirements compelling vendors directly collecting Personal Information or those receiving it from others Personal Information to provide additional notices? Who is responsible for those notices? Publishers? The vendors?**

As per the Privacy Rules, an entity that collects data is responsible for providing notice to the Data Subjects from whom the data is collected. In case of digital advertising, vendors collecting data from the Data Subject would be responsible for providing such notice to the Data Subject. Since vendors do not have direct relationship with the publisher who provides the capability and inventory for advertisers to run ads, the vendors will be considered as Data Controllers if such vendors collect data from the Data Subject at the first instance.

There are no specific requirements related to providing notice of data collection for digital advertising purposes. Further, there are no rules that require processors to provide additional notices.

When collecting Personal Information or SPDI from a Data Subject, the Data Collector must take reasonable steps to ensure that the Data Subject is aware of the purpose of collection of such data (please refer to our response to "*Overview*" under 4.3.1 above).

- **Who must receive notice? When must notice be provided? What must be in the notice in the digital advertising context? (Consider also, what notice needs to be provided when pixels fire on a webpage?)**

  Please refer to our response above.

- **Is there specific notice required for sensitive information?**

  Please refer to our response above.

- **Are there any specific requirements for providing notice related to processing children's Personal Information?**

  The IT Act and Privacy Rules do not specifically regulate the collection or processing of data relating to children. The terms " child" or " children" have not been defined under the current data protection regime, and therefore, no additional compliances or requirements have been prescribed in respect of data pertaining to children.

- **Are there any requirements compelling vendors directly collecting Personal Information or those receiving it from others personal information to provide additional notices? Who is responsible for those notices? Publishers? The vendors?**

  Please refer to our response in Paragraph 3.1 above. Additionally, in case vendors collecting Personal Information or SPDI from the Data Subject share such data with third parties for advertising purposes, the vendor is required to provide generic details of the third parties who will receive such data from the vendor. For instance, if a publisher provides notice through privacy policy that it may share Personal Information with third parties for the purposes of advertising, it will be sufficient if generic details of the third parties are provided. Language in the notice to mention that "the data may be shared with group entities, third party processors, payroll providers, consultants and other service providers."

4.3.1. Application to Digital Advertising

- **Do third parties need to be named? For example, if a publisher gives privacy policy notice that it may share personal information with third parties for advertising purposes, does it have to specify which third parties? Do specific digital advertising activities or purposes need to be disclosed as well (e.g., TCF purposes)?**

  There are no specific requirements in this regard. The notice requirements under the IT Act and Privacy Rules would have to be adhered to in relation to digital advertising.

  In case Personal Information of a Data Subject is shared with a third party, it is not necessary that such third party needs to be named. It will be sufficient if generic details of the third parties are provided. It is advisable that specific digital advertising activities be disclosed.

- **From an industry perspective, it is common to distinguish data use for ad targeting vs. profile building vs. measuring ad campaigns. Does the notice requirement require separate disclosure of those things, or is it enough to say something general like, "advertising and related purposes"?**

  It is sufficient if the Data Collector provides a generic purpose for collection of data from the Data Subject. The Privacy Rules stipulate that the Data Collector is required to mention the purpose of collection. While specificity of the purpose is not a requirement, if the industry practice is to distinguish usage of data for multiple purposes, the Data Collector may mention the same.

4.4. Consent and Exceptions to Consent

4.4.1. Overview

The IT Act and Privacy Rules do not define consent. However, as per the provisions of Privacy Rules, consent is required when an entity collects SPDI from a Data Subject.

- **For what types of Personal Information or purposes of processing is consent required?**

  At present, there is no requirement to obtain consent to collect Personal Information. To collect SPDI, a Data Collector is required to obtain consent of the Data Subject. The IT Act and Privacy Rules, however, do not contain provisions relating to consent requirements in case of processing Personal Information or SPDI.

- **How is valid consent manifested–express consent, opt-in, implied consent, or opt-out?**

  In general, consent forms the most essential element of the Privacy Rules. If such consent is obtained by virtue of a standard form contract, then the terms of the contract must be reasonable. As per the Privacy Rules, express consent in writing/electronic form, from the Data Subject providing SPDI, is required. It means that for the Data Subject's consent to be considered valid under law, such consent should be expressly provided, either in written or electronic form. This can be in the form of unchecked tick boxes prior to collection of data. Section 10A of the IT Act contains a provision regarding validity of contracts formed through electronic means:

  > *Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.*

  Furthermore, under the Privacy Rules, the Data Subject should have the option to opt out of providing the data or information that is being sought by corporate entities. Data Subjects should always have this option while availing themselves of services from corporate entities, as well as have an option to withdraw consent that might have been given earlier. However, the Privacy Rules are silent on whether the option to opt-out would only apply to SPDI. Accordingly, the position to be taken is that a Data Subject should be provided the option to opt out of sharing any of his/her Personal Information/SPDI. Further details on the opt-out functionality have been set out in detail in Paragraph 4.4.1 in Page 23 above.

  Unlike many other jurisdictions, should a Data Subject not consent to the collection of information or otherwise withdraw their consent, the Privacy Rules allow corporate entities not to provide goods or services for which the information was sought. In addition to the right to opt-out of sharing information, Data Subjects have the right to review the information they have provided and to seek the correction or amendment of such information if incorrect. As general practice, a Data Subject may opt-out of sharing information by contacting the designated Grievance Officer of the Data Collector.

The entity collecting the data must ensure it provides the Data Subject with the option to not provide any SPDI sought for collection.

The obligation for every set of specific SPDI collected requires consent from the Data Subject. If the Data Collector intends to collect data that is separate from the notice for the data earlier provided, the Data Collector must obtain consent from the Data Subject for new submissions of Personal Information or SPDI by the Data Subject.

- **Is specific notice required as part of the consent?**

  Yes, specific notice is required in addition to consent, and is required to be provided to the Data Subject.

- **Does the consent obligation require granularity (i.e., consent for distinct processing activities) similar to GDPR? Or is the consent obligation more generalized (e.g., requiring consumers to opt-in to "online behavioral advertising" more broadly, without having to consent to each constituent processing activity/ party)? Is consent different for different uses or types of data (e.g., sensitive data, profiling, automated decision making, etc.) Please provide details.**

  Please refer to our response to "Overview" under 4.3.1 above for information regarding collection of SPDI and consent from a Data Subject.

- **Can Personal Information be processed for secondary purposes (i.e., differing purposes from which it was collected)?**

  The Privacy Rules provides that any information collected must be used exclusively for the purposes for which it was collected. This rule does not explicitly clarify whether this purpose limitation would apply to Personal Information or SPDI. However, given the general scope and intent of the Privacy Rules, there is widespread consensus that this limitation applies to Personal Information and SPDI collected by a Data Collector.

  Further, the IT Act and Privacy Rules do not contain any exemptions regarding processing of Personal Information for "legitimate business purposes." It should be noted that Personal Information and/or SPDI is required to be utilized only in connection with the purpose of processing such data.

- **Are there any rules compelling downstream recipients/processors of personal information to provide additional notices?**

  There are no provisions in the IT Act and Privacy rules compelling downstream recipients/processors of Personal Information to provide additional notices.

- **Are there any issues concerning the timing of consent?**

  There are no issues concerning the timing of consent if consent requirements are met.

- **Are there distinct consent requirements for sensitive Personal Information?**

  There are no distinct consent requirements to collect SPDI. The Data Collector must obtain the prior written or electronic consent of the Data Subject.

- **Are there distinct consent requirements for profiling consumers? If a business gets consent to use personal data for "advertising and marketing" purposes, is a separate (or more specific) consent required to build an advertising profile for advertising?**

  There are no distinct consent requirements for profiling consumers. Furthermore, separate consent would not be required to build an advertising profile if the Data Subject is aware that his/her data will be used for "advertising and marketing" purposes.

- **Are there distinct consent requirements for automated decision making?**

  There are no distinct consent requirements for automated decision making.

- **Are there any age restrictions related to consent? Are there distinct consent requirements around processing children's Personal Information?**

  At present, there are no age restrictions related to consent and consent requirements around processing children's Personal Information.

- **Can consent, however manifested, be revoked?**

  As per the Privacy Rules, a Data Subject has the right to withdraw consent given to a corporate entity at any time while availing services, by giving them notice. In such cases, the corporate entity is obliged not to use the Personal Information or SPDI of the person and would have the option to discontinue its services for which such information was sought.

4.4.2. Application to Digital Advertising

No specific or distinct application to digital advertising.

4.5. Appropriate Purposes

4.5.1. Overview

N/A

4.5.2. Application to Digital Advertising

- **Does the law or legal guidance require a specific legal basis for specific digital advertising activities? Clarify for each activity (suggest using TCF/IAB CCPA "purposes") ("profiling" must be addressed here).**

  The IT Act and Privacy Rules do not require a specific legal basis for specific digital advertising activities. Also, the IT Act and Privacy Rules do not define "profiling" and do not mirror privacy provisions of the GDPR or California Consumer Privacy Act, 2018. Furthermore, the ASCI Code does not regulate issues relating to privacy.
  In India, most of the body corporates use the standards mentioned in the GDPR as a minimum standard when dealing with digital marketing/advertising and privacy. Furthermore, when dealing with aggregated data, the body corporates do not opt for "consent framework" (TCF) and consent/TCF is initiated only when specific personal data is being sought from a consumer.

- **If yes, what are the legal bases (e.g., consent, legitimate interest)? Are there any requirements related to lawful basis (need a valid legal basis to process) fairness (scope of processing is fair) transparency (transparent about the processing activity to the consumer and the lawful basis)?**

  The IT Act and Privacy Rules do not prescribe any lawful bases for processing ordinary personal data (including for digital advertising activities). At present, such information may be freely collected and processed. However, a Data Collector may collect and process a Data Subject's sensitive personal data or information (SPDI) only if:

- The SPDI is collected for a lawful purpose connected with a function or activity of the Data Collector; and
- The collection of the SPDI is considered necessary for that purpose.

- **Does the law address processing for secondary purposes/differing purposes from which it was collected?**

  As per the Privacy Rules, information collected from Data Subjects must only be used for the purposes for which it was collected. Accordingly, such information cannot be used for secondary/differing purposes. In the event where a Data Collector makes broad disclosures in the privacy policy regarding purposes for collection, it is sufficient if the disclosures are made by the Data Collector despite the disclosures being broad in nature. In practice, language incorporated in privacy policies are generally wide to cover other associated purposes of processing the collected data.

4.6. Safeguards

4.6.1. Overview

N/A

4.6.2. Application to Digital Advertising

N/A

5. DATA SUBJECT RIGHTS/EXEMPTIONS

5.1. Overview

The IT Act and the Privacy Rules do not define "Data Subject." Instead, the term "provider of information" is used under the Privacy Rules. As per the Privacy Rules, a "provider of information" has been defined as a natural person who provides SPDI to a corporate entity.

5.2. Access

Access is currently not provided to Data Subjects under the IT Act and Privacy Rules.

5.3. Rectify

Under the Privacy Rules, a Data Subject has the right to review the information they provide and ensure that any Personal Information or SPDI found to be inaccurate can be corrected by them.

5.4. Deletion/Erasure

This right is currently not provided to Data Subjects under the IT Act and Privacy Rules.

5.5. Restriction on Processing

There are no restrictions on processing of Personal Information and SPDI, as long as explicit consent is sought from the Data Subject while collecting SPDI and transferring SPDI to a third party.

5.6. Data Portability

This right is currently not provided to Data Subjects under the IT Act and Privacy Rules.

5.7. Right to Object

This right is currently not provided to Data Subjects under the IT Act and Privacy Rules.

5.8. Right Against Automated Decision-making

This right is currently not provided to Data Subjects under the IT Act and Privacy Rules.

5.9. Responding to Consumer Rights Requests

In case a Data Subject makes any request regarding his/her Personal Information or SPDI, please refer to our response in Paragraph 9.1 below.

5.10. Record Keeping Concerning Rights Requests

The IT Act and Privacy Rules do not impose any overarching data retention requirements. Instead, the Privacy Rules require a Data Controller to ensure that no SPDI that is collected is retained for longer than necessary for the purpose disclosed during collection.

5.11. Is Providing Consumers with These Rights Required by Law or Mere Suggestions?

Under the Privacy Rules, Data Subjects are only entitled to the following rights:

- To review the information they provide and ensure that any Personal Information or SPDI found to be inaccurate or deficient is corrected or amended as feasible; and/or
- To withdraw consent to use the information (where applicable).

5.12. Application to Digital Advertising

The rights of consumers in digital advertising usually flow from the moment a publisher publishes any Personal Information or SPDI. However, it is to be noted that in case data published by a publisher does not qualify as Personal Information or SPDI, the consumer in such cases will not have the rights they would otherwise have if the data were to be Personal Information. For instance, a consumer will not have the right to rectify his/her data if the data published is not Personal Information.

In case a publisher or ad tech company utilizes a consumer's Personal Information or SPDI, the consumer will have the right to request the publisher or the ad tech company to stop using his/her Personal Information or SPDI. In such instances, apart from the publisher/ad tech company refraining to use the Personal Information or SPDI, the publisher/ad tech company must also intimate the concerned service provider to stop using such data, to the extent possible.

6. DATA CONTROLLER AND PROCESSOR AGREEMENTS

6.1. Overview

Please refer to responses below.

6.2. Data Controller Outsourcing of Processing

The IT Act and the Privacy Rules do not define "data controller."

6.3. Data Processor Rights and Responsibilities

The IT Act and the Privacy Rules do not define "data processor." A Data Collector must implement such security practices and procedures as are commensurate with the Personal Information and SPDI that is collected and stored. This requirement includes implementing a documented information security program and information security policies containing managerial, technical, operational, and physical security control measures.

Notably, the Privacy Rules prescribe International Standard IS/ISO/IEC 27001 on Information Technology-Security Techniques-Information Security Management System-Requirements as a recommended data security standard.

6.4. Application to Digital Advertising

The above provisions applicable to data controllers as mentioned above would apply to Data Controllers and data processors in all instances of digital advertising.

7. DATA TRANSFER & OUTSOURCING

7.1. Overview

IT Act and Privacy Rules do not impose any restrictions or requirements on the transfer of ordinary Personal Information to third parties. However, there are certain restrictions imposed when SPDI is transferred to a third party. As per the Privacy Rules, transfer of SPDI is only allowed if:

a) The recipient ensures the same level of data protection that is adhered to by the Data Collector; and
b) The transfer of SPDI: is necessary for the performance of a lawful contract between the Data Collector and the Data Subject; or has been expressly consented to by the Data Subject.

Therefore, while explicit consent is not required for transfer of Personal Information, the same may be required for transfer of SPDI to a third party. Similarly, where SPDI is transferred to a third party, the recipient would need to ensure the same level of data protection as is provided by the Data Collector in India. Typically, this is ensured by parties by entering into a Data Transfer Agreement or Data Processing Agreement that sets out the minimum data security and protection measures to be implemented by the recipient. There are no specific rights given to Data Subjects in case of data transfers if the consent and data protection requirements are met.

7.2. Application to Digital Advertising

If the Data Collector in digital advertising intends to transfer Personal Information/SPDI collected, the entity is required to obtain consent of the consumer only for transfer of SPDI to a third party whereas there is no consent requirement for transfer of Personal Information to a third party. For transfer of SPDI to a third party, conditions mentioned in Paragraph 7.1 above will apply accordingly.

8. AUDIT/ACCOUNTABILITY

8.1. Overview

- **Audit - What audit rights are dictated by law (e.g., must companies have audit rights over their vendors? Does it matter what the classification of those vendors are?)**

  There are no such audit rights dictated by law.

- **Accountability - Must companies/vendors keep certain records to prove they have met certain requirements? What are those requirements?**

  As per the provisions of IT Act, if there is a provision for audit of documents, records, or information under any other law, that provision will be applicable for audit of documents, records, or information processed and maintained in electronic form.

8.2. Application to Digital Advertising

N/A

9. DATA RETENTION

9.1. Overview

While the Privacy Rules prescribe that collectors of information should not retain information for longer than required, they do not specify a limitation period for how long data can be stored. On the other hand, certain financial sector entities need to comply with sector-specific requirements prescribed by the Ministry of Finance and ensure that data is retained for a certain number of years. However, general practice indicates that data is retained for the duration of applicable limitation periods in relation to causes of action that may arise.

The Privacy Rules require corporate entities to appoint a grievance officer to redress the grievances that the Data Subjects may have ("Grievance Officer"). Any grievances that the Data Subjects may have with respect to the processing of information are to be addressed by corporate entities in a time-bound manner, and no later than a month from the date of the receipt of the grievance.

9.2. Application to Digital Advertising

No specific or distinct application to digital advertising.

10. DATA PROTECTION AUTHORITY | REGULATORY AUTHORITY

10.1. Overview

Please refer to responses below.

10.2. Main Regulator for Data Protection

Currently, there is no data protection authority responsible for enforcement of the Privacy Rules. The Ministry of Electronics and Information Technology ("MeitY") operates as the nodal agency for information technology in India.

10.3. Main Powers, Duties and Responsibilities

MeitY's role has been restricted to the formulation of policy. Its role has not been extended to the implementation of the IT Act or the imposition of penalties.

10.4. Application to Digital Advertising

N/A

11. SANCTIONS

11.1. Overview

Please refer to responses below.

11.2. Liability

- **Scope of liability for publishers and advertisers for processing activities of adtech companies**
  If adtech companies processing any SPDI are in breach of handling such SPDI or negligent in implementing security practices causing wrongful loss or gain to any person, then the publishers and advertisers, on whose behalf the adtech companies are conducting processing activities, will be liable to compensate the person affected by such acts.

  Furthermore, as per the Information Technology (Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013, there is an obligation on body corporates to report certain cybersecurity incidents, including any incidents of unauthorized access to IT systems/data, to CERT-In. Such reporting must be done as soon as possible to allow CERT-In to take or suggest corrective actions. However, no sanctions or penalties have been prescribed in the CERT-In rules for a failure to report cybersecurity incidents to CERT-In.

- **Scope of liability for adtech companies for collection activities of publishers and advertisers**

  As per the Privacy Rules, the adtech companies will not be responsible for the authenticity, correctness, or accuracy of Personal Information or SPDI collected by the publishers and advertisers from the Data Subject. However, any activity beyond collection that extends to handling and processing of Personal Information or SPDI will follow consequences as mentioned in our response in Paragraph 5(a) above.

11.3. Enforcement and Market Practice

- **How are claims raised under the law?**

  Claims are usually raised by providing notice. In the event the Data Collector/processor does not address the concern of the Data Subject, the Data Subject has the option of filing a civil suit. Please refer to Paragraph 11.5 herein.

- **Who enforces them?**
  There is no data protection authority under the IT Act or the Privacy Rules; clarification on either must be sought from MeitY. MeitY does not have a formal process for seeking clarifications.

- **What is their practice (quietly working with companies to fix, publicly coming out with large investigations? Fact specific?)**

  Given the number of such cases is less, we do not have sufficient information in this regard.

- **What guidance has there been to date showing how to handle requirements in the ad ecosystem? Have the regulators been educated on how the ecosystem operates? Have compliance regimes been discussed with them? Has their feedback been solicited?**

  Given the data protection regime in India is in its nascent stage, we do not have sufficient information in this regard.

11.4. Remedies

N/A.

11.5. Private Right of Action

The IT Act allows Data Subjects whose data privacy rights have been violated to seek recourse for disputes arising out of violation of privacy and cyberattacks. The victim may lodge a complaint with the adjudicating officer ("AO"), appointed for every state in India. The AO holds inquiry and adjudicates the matter regarding the contravention under the IT Act. If any party is aggrieved with the order passed by the adjudicating officer, an appeal may be made before the Telecom Disputes Settlement and Appellate Tribunal.

11.6. Digital Advertising Liability Issues

N/A

12. NOTIFICATION | CERTIFICATION | REGISTRATION

12.1. Overview

N/A.

12.2. Requirements and Brief Description

The IT Act and Privacy Rules do not require Data Collectors or data processors to be registered in India.

12.3. Application to Digital Advertising

N/A

13. DATA PROTECTION OFFICER

13.1. Overview

Please refer to responses below.

13.2. DPO – Compulsory Appointment (Yes/No)

A Data Collector must appoint a Grievance Officer. Please refer to our response in Paragraph 9.1 above.

13.3. Requirements

The Data Collector must publish the name and contact details of the grievance Officer on its website. Furthermore, the Privacy Rules do not contain any requirements that the grievance officer should mandatorily be located in India. However, as good practice, entities do appoint a grievance officer who is located in India.

13.4. Application to Digital Advertising

N/A

14. SELF-REGULATION

14.1. Overview

- **Are there any industry-self regulatory schemes in place in the jurisdiction?**

  There is no central statutory agency or overarching legislation regulating the advertising industry or, more specifically, to digital advertising in India. Notably, the Indian advertising market is regulated by a non-statutory body-the Advertising Standards Council of India ("ASCI"). The ASCI has adopted a Code for Self-Regulation in Advertising ("ASCI Code"), which applies to all persons involved in the commissioning, creation, placement, or publishing of advertisements. The ASCI Code primarily discusses the content and form of advertising and has been drawn up with a view to achieve the acceptance of fair advertising practices in the best interest of the consumers.

- **Are there any signal-based programs used in the territory to assist with digital advertising compliance?**

  There are no signal-based programs used in India to assist with digital advertising compliance.

14.2. Application to Digital Advertising

N/A

15. PENDING PRIVACY BILLS

15.1. Overview

In mid-2017, the Government constituted a Committee of Experts on Data Protection ("the Committee"). In July 2018, the Committee submitted a draft law titled, the Personal Data Protection Bill, 2018 (PDP Bill), to the Government. A revised version of the PDP Bill was subsequently introduced to the lower house of the Indian Parliament, Lok Sabha, in December 2019, and is presently under the scrutiny of a Parliamentary Joint Select Committee.

The draft provisions in the PDP Bill contain rights accorded to a Data Subject like the right to access, correct, and erase their data after the same is processed for the concerned purpose. In light of this, entities would have to create ways to allow Data Subjects to exercise their rights. Furthermore, the PDP Bill provides for data localization. This essentially means that the PDP Bill requires a data controller processing SPDI to store a copy of this information in India at all times (i.e., requiring entities to store certain categories of data only on Indian servers). Should any of the categories of data be classified as "critical personal data," upon the enactment of the PDP Bill, this type of data would need to be stored and processed exclusively in India.

The proposed PDP Bill aims to incorporate many of the rights and obligations (e.g., Data Subject rights, transfer of data, etc.) enshrined in the GDPR.

Summary of the bill. The PDP Bill applies to personal data and sensitive personal data. It goes a few steps further than the existing treatment of sensitive personal data and information under the Privacy Rules and treats identifiable data, with respect to any characteristic, attribute, trait, or other feature of a person's identity, as personal data. It is worth noting that the definition of personal data applies to both, online and offline mediums, and includes inferences drawn by the profiling of personal data.

Sensitive personal data is a subset of personal data that is subject to enhanced processing requirements. It includes health or financial data, biometric data, sex life, sexual orientation, and religious or political beliefs. The Bill allows the Government to specify further categories of sensitive personal data.

Furthermore, the PDP Bill takes into consideration privacy by design and proposes to appoint a Data Protection Authority to protect the interests of data principals. Additionally, the PDP Bill prescribes penalties for breach of the provisions based on the turnover of an entity. Such penalties can depend on the type of breach and violation of the provisions of the PDP Bill.

Much like the GDPR, and in line with Privacy Judgement, the PDP Bill provides for a consent-based approach while processing data. In the absence of consent, the Bill also provides for the following grounds of processing:

- For the necessary functioning of the State, the Parliament, or State Legislatures.
- To comply with orders or judgments of courts or tribunals.
- For purposes related to employment.
- For prompt action, such as in events of medical emergencies, disasters, and breakdowns of law and order; and
- For reasonable purposes, such as whistleblowing, mergers and acquisitions, credit scoring, debt recovery, etc.

In the absence of any existing guidance, the scope of each of these grounds of processing remains subject to governmental and judicial interpretation.

Grounds of processing sensitive personal data, however, differ slightly. For example, one of the grounds includes seeking explicit consent. While the Bill provides certain grounds under which consent will be valid (for example, it must be free, informed, clear, specific, and capable of being withdrawn), it does not provide guidance on how explicit consent is to be sought, and how it varies substantially from regular consent.

While the final form of the new law is not certain, the underlying principles appear to mimic the European Union's General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"), with a few notable deviations. Should the Bill be enacted, it will repeal the IT Act and Privacy Rules and it will require a material change in the way businesses operate in trade.

Timeline. At present, there is no clear timeline for the enactment of the PDP Bill. However, there are strong indications that the PDP Bill may be enacted in 2021.

The PDP Bill is intended to apply in the following scenarios:

- Processing of personal data that has been collected, disclosed, shared, or otherwise processed within India.
- Processing of personal data by any Indian entity, citizen, or the State (as defined under Article 12 of the Constitution); and
- Processing of personal data by data fiduciaries or data processors not present within India, if the processing is in connection with either:
- Any business carried on in India or any systematic offering of goods or services to data principals within India; or
- Profiling data principals within India.

The provisions of the Bill, however, do not apply to:

- Processing of personal data of data principals outside India by data processors incorporated under Indian laws, provided that such processing is pursuant to a contract between the data processor and any person outside India. This exemption shall come into effect upon notification by the Government; and
- The processing of anonymized data. However, the Government has the power to require data fiduciaries to share anonymized or non-personal data to enable the better targeting of delivery of services or formulation of evidence-based policies offered by the Government.

Actors (Data Principles, Data Fiduciaries, Data Processors, Social Media Intermediaries)

A data principal is a natural person to whom personal data relates. A data fiduciary is any person, including the State, a company, or a legal person/entity, who, either alone or with others, determines the purpose and means of processing. A data processor is any person who processes data on behalf of a data fiduciary. In other words, a data principal is conceptually similar to a Data Subject, and a data fiduciary is similar to a data controller under the GDPR. Separately, the PDP Bill provides for the establishment of a data protection authority ("**DPA**") which will overlook the processing activities encompassed under the PDP Bill.

The PDP Bill envisages a class of data fiduciaries called "significant data fiduciaries," who have enhanced transparency and accountability obligations. The Bill also recognizes a new category of actors termed "social media intermediaries" that primarily enable online interactions between two or more users, and allow them to create, upload, share, disseminate, modify, or access information. Intermediaries that facilitate commercial transactions, access to the internet, search engines, online encyclopedias, and email or online storage services are excluded from the scope of this definition. The Government has the power to classify social media intermediaries as significant data fiduciaries based on the minimum number of such intermediaries' users, and the likelihood of the impact of such intermediaries on electoral democracy, State security, public order, and the sovereignty and integrity of India.The PDP Bill introduces a class of data fiduciaries termed "consent managers," to be registered with the DPA, to facilitate obtaining and managing consent for other data fiduciaries through an accessible, transparent, and interoperable platform. Furthermore, any entity that allows the data principal to withdraw, review, and manage consent would be required to be registered with the DPA. However, as per the draft provisions of the PDP Bill, the details regarding registration with the DPA have not yet been formulated.

Obligations of Data Fiduciaries

Processing

The PDP Bill imposes certain obligations, detailed below, on data fiduciaries, who must comply with these obligations as well as be able to demonstrate such compliance. Personal data should be processed in a fair and reasonable manner that respects the privacy of the data principal:

- Processing should only be for specific, clear, and lawful purposes, or other incidental purposes for which the data principal would reasonably expect the personal data to be used.
- Collection of personal data should be limited to the data that is necessary for processing.
- Data should be processed only on the grounds detailed in the PDP Bill.
- The data fiduciary should provide the data principal with adequate notice of data processing.
- The data fiduciary should ensure that the personal data being processed is complete, accurate, not misleading, and updated; and
- Personal data should only be retained for as long as is necessary to satisfy the purpose for which it is processed. Thereafter, such data should be deleted.

Data Localization

The PDP Bill requires sensitive personal data to be stored in India. The PDP Bill also allows the Government to prescribe categories of "critical personal data" that must only be processed in India.

Cross-Border Transfer of Personal Data

Subject to data localization requirements, sensitive personal data may be transferred out of India in certain cases. For example, a transfer is permissible if:

- It is in accordance with contractual clauses or intra-group schemes authorized by the DPA;
- It is made to a country, sector within the country, or an international organization approved by the Government;
- The transfer is necessary, provided the DPA has approved such necessity; and
- In addition to either of the three preceding points, the data principal has explicitly consented to such transfer.

The practical mechanics of obtaining explicit consent are unclear and await clarifications from the yet to be established DPA.

The PDP Bill is silent on the cross-border transfer of personal data that is not sensitive personal data. In the absence of a specific law, we presume that the law intends to not regulate such transfers subject to such transfers satisfying the general requirements of lawful processing of personal data.

It is worth noting that critical personal data may be transferred outside India in a limited number of situations: for example, if the transfer is to a health or emergency service provider for prompt action, or to a Government-approved

country, entity, or organization. Such transfers will have to be reported to the DPA within prescribed timelines.

Breach

The PDP Bill has adopted a harm-based approach to tackling personal data breaches. For example, in the event of a breach, a data fiduciary would be required to report the breach within specified timelines to the DPA, which will determine, depending on the severity of harm that may be caused, whether such breach should be reported to data principals. Harm includes injury, be it mental/emotional or physical, identity theft, loss of employment, discrimination, and loss of reputation or humiliation, amongst others. Precise methods of how harm will be gauged remains unclear. Furthermore, the DPA shall have the right to direct the data fiduciary to take remedial action in the event of breaches, and post details of such breaches on its website.

Data Protection Officer ("DPO")

The PDP Bill requires significant data fiduciaries to appoint a DPO. In addition to functions that significant data fiduciaries may assign to their respective DPOs from time to time, the PDP Bill details certain functions that the DPO must perform such as monitor data fiduciary processing activities to ensure compliance with the Bill, provide advice, assist and cooperate with the DPA, and act as points of contact between data principals and data fiduciaries, amongst other activities. The Government may specify eligibility criteria for DPOs. In the event a data fiduciary is situated outside India, they must appoint a DPO based in India.

Transparency and Accountability Measures

Much like the GDPR, the PDP Bill introduces the concept of privacy by design by necessitating data fiduciaries adopt Privacy by Design policies, which the data fiduciaries may choose to have approved by the DPA. For example, business practices and technical systems must be designed in a manner to anticipate and avoid harm to data principals, privacy of data should be ensured from the moment it is collected until its eventual deletion, and the technology standards should be commercially acceptable or in accordance with certified standards. However, the PDP Bill does not specifically prescribe any standards.

Other obligations of transparency and accountability measures imposed on data fiduciaries include enactment of adequate security safeguards and publicizing information on the processing undertaken. Significant data fiduciaries have additional obligations that include accurate and up-to-date record keeping, conducting annual data audits, and carrying out data protection impact assessments for certain events, etc.

Rights of Data Principals

The PDP Bill provides a statutory framework for the fundamental rights affirmed in the Privacy Judgement. Data principals have the right to:

- confirm and access personal data collected;
- correct or update it;

- access their personal data in commonly used forms, similar to the concept of data portability under the GDPR; and
- erasure, if the purposes of processing are fulfilled.

Furthermore, the PDP Bill introduces a right to be forgotten, which allows data principals to prevent the disclosure of personal data if the disclosure is no longer necessary or has served the purpose for which it was made, if the consent that permitted such disclosure has been withdrawn, or if the disclosure is made contrary to applicable laws. The PDP Bill also tries to provide a balancing act between this right and the constitutional guarantee of the freedom of speech and expression and the right to information. However, the practical exercise remains to be seen.

Data Sandbox

The PDP Bill allows the DPA to include interested data fiduciaries who fulfil certain conditions in a sandbox created for encouraging innovation in artificial intelligence, machine-learning, or other emerging technology, and exempt them from specific provisions of the PDP Bill.

Penalties

Contravention of different provisions of the PDP Bill would result in different penalties. Similar to the situation under the GDPR, contravention by a data fiduciary of a category of obligations may attract a penalty of up to INR 50 million (approx. €645,000) or 2 percent of the data fiduciary's total worldwide turnover of the preceding financial year, whichever is higher. A contravention by a data fiduciary of obligations in respect of processing of personal data or sensitive personal data, cross-border transfer of personal data, and adherence to the security safeguards detailed in the PDP Bill may attract a penalty of up to INR 150 million (approx. €1.9 million) or 4 percent of the data fiduciary's total worldwide turnover of the preceding financial year, whichever is higher.

A person who re-identifies personal data that had previously been de-identified by a data fiduciary or a data processor without the consent of the data fiduciary or data processor may be punished with both, imprisonment of a term that may extend to three years and a fine of up to INR 200,000 (approx. €2,600).

iab.

Israel

Cross-Jurisdiction Privacy Project

1. THE LAW

1.1. Overview & Key Acts, Regulations, and Directives

Data protection in Israel is governed primarily by the Protection of Privacy Law, 5741-1981 ("the Privacy Law") and the regulations promulgated under it, the Basic Law: Human Dignity and Liberty, 5752-1992, and the guidelines of the Israeli regulator, the Privacy Protection Authority ("PPA") (formerly known as the Israel Law, Information and Technology Authority ("ILITA")). Asterisks are included in this section for all privacy laws that likely apply to digital advertising transactions.

Additional legislation includes:

- Protection of Privacy Regulations (Conditions for Inspection of Data and Procedures for Appeal on a Denial of a Request to Inspect) 1981 (only available in Hebrew here) ("the Data Inspection Regulations")*.
- Amendment No. 40 to the Communications Law (Telecommunications and Broadcasting), 5742-1982 ("the Anti-Spam Law")*.
- Privacy Protection Regulations (Terms of Holding Data and Its Maintenance and Procedures for Transfer of Data between Public Entities), 5746 – 1986.
- Protection of Privacy Regulations (Transfer of Information to Databases Abroad), 5761-2001 ("the Transfer of Information Regulations")*.
- Administrative Offences Regulations (Administrative Fines and Protection of Privacy) 2004 ("the Administrative Fine Regulations")*.
- Protection of Privacy (Data Security) Regulations, 5777-2017 ("the Data Security Regulations")*.
- The Credit Data Law, 5776-2016, which regulates the activities of entities that provide credit information services and regulates the privacy of data subjects whose credit information may be collected, processed, and/or transferred by such entities.
- The Genetic Information Law, 5761-2000 (only available in Hebrew here), which regulates the activities of legal persons that are authorized to conduct genetic tests and provide genetic counselling, and regulates the privacy of data subjects whose genetic information may be obtained by such entities, including by way of the collection of samples and transfer of tests results.
- The Patient's Rights Act (1996), which regulates the rights of patients and applies to any individual providing professional health services and/or medical institutions and regulates privacy matters with respect to the medical information of such patients.

1.2. Guidelines

Although the guidelines published by the PPA do not have the status of law, they reflect the PPA's interpretation of the obligations under the existing Privacy Law and therefore should be considered. The guidelines followed by an asterisk likely apply to digital advertising transactions:

- 2/2011 Use of Outsourcing Services for Personal Data Processing (only available in Hebrew here)*.
- 2/2017 Direct Mailing and Direct Mailing Services (only available in Hebrew here)*.
- Draft Guidelines on the Transfer of Ownership in a Database (only available in Hebrew here) ("the Transfer of Ownership Draft Guidelines"), which relate to database transfers in a merger & acquisition context*.
- 3/2018 Application of the Data Security Regulations to Organizations Certified Under ISO 27001 (only available in Hebrew here)*.

1.3. Case Law

The legal system in Israel is a hybrid of black letter law and case law. The legal hierarchy in Israel is as follows: Basic Laws that have been granted constitutional status, Laws and Ordinances, Regulations and PPA Guidelines. In Israel, courts have power to provide a binding interpretation of laws. Israeli Supreme Court rulings bind lower courts.

Privacy laws in Israel have not been recently updated, so courts frequently fill gaps through their rulings.

2. SCOPE OF APPLICATION

2.1. Who Do the Laws and Regulations Apply To, and What Types of Processing Activities are Covered/Exempted?

The Privacy Law applies to all business entities in Israel that hold or process personal information. Territorial application is yet to be fully determined by courts (as explained below), and the definition of "personal information" does not fully correspond with modern processing of data.

The applicable data subjects are individuals. The rights under the laws prohibit the unlawful use of information and sensitive information of an individual.

The Privacy Law does not explicitly set forth its jurisdiction; nor does it require that the data subject be a resident or citizen of Israel. Therefore, the jurisdiction of the Privacy Law is similar to those of other Israeli laws—i.e., limited to acts within Israel. It is an unsettled legal question whether the Privacy Law applies to foreign entities processing personal information of Israelis, and whether it applies to Israeli entities processing personal information of non-Israelis. However, if the restrictions on the transfer of data are breached, any subsequent use of the data outside Israel is likely to be attributed to the party in Israel who breached the transfer restrictions.

2.2. Jurisdictional Reach

As explained above, the territorial scope of the Privacy Law is unclear. While the Privacy Law does not specifically determine any extraterritorial applicability, courts in recent years tend to decide, at least at the preliminary stage of the proceedings, that multinational organizations acting in Israel and collecting personal data on Israeli citizens and residents are subject to the jurisdiction of Israeli courts and, in some circumstances, may also be subject to the provisions of the Privacy Law. The few courts that have conducted such analysis based it on the private international law concept of *lex loci deliciti*, given that a privacy violation in Israel is a civil tort. Thus, some courts assume that when an Israeli resident's right to privacy is violated via the Internet, at least part of the infringing act occurs in Israel and is therefore subject to Israeli law. However, the Supreme Court recently determined that choice of law provisions in terms of use and privacy policies, referring to California law, for example, are valid in Israel, and while Israeli courts will have jurisdiction over such cases, they will be decided according to the foreign law agreed by the parties. This was later adopted by several district courts, including with respect to English law choice of law provisions.

2.3. Application to Digital Advertising

Hypotheticals to test concerns/jurisdictional reach

Scenario 1 (*The baseline*): A user residing in Israel (determined by IP address or geo identifier) goes onto an Israeli domain and is served an ad by an Israeli advertiser. The advertiser uses the user data to build a user profile.

Israeli Law applies to all parties involved.

Scenario 2 (*User outside Israel*): A Logged-on/signed-in user, known by the publisher to be an Israeli resident, goes onto an Israeli domain but the user's IP address or geo identifier indicates the user is outside Israel. An Israeli advertiser serves an ad and uses the user data to build a user profile.

In the event that the advertiser is Israeli, the Privacy Law will likely apply regardless of the domicile or actual location of the user. This is especially so if the user is Israeli, even if temporarily outside of Israel.

- **Q1: Does the answer change if this is a signed-out user, with no way of knowing where they are domiciled?**

In the case of a signed-out user, the preliminary question would be if the data is even identified/identifiable. The Privacy Law currently applies only to identified or reasonably identifiable data, and therefore if no identifiable data is collected, it will not apply. If the data is reasonably identifiable with respect to the signed-out user, the answer will not change for an Israeli advertiser.

Scenario 3 (*Publisher domain outside Israel*): A user residing in Israel (determined by IP address or geo identifier) goes onto a domain outside of Israel. An Israeli advertiser serves an ad and uses the user data to build a user profile.

In this case, even if a lex loci delicti analysis shows that the act occurred outside of Israel, Israeli courts have already determined that when both the tortfeasor and victim are Israeli residents, Israeli law will apply even if the wrongful act was performed outside of Israel. In this case, even the publisher may be subject to Israeli Law, and it is very likely that the Israeli advertiser will be subject to Israeli law in any event.

- **Q1: Does the answer change if the site hosts content aimed at Israeli residents (e.g., a news aggregator with a section on Israeli current affairs)?**

  No.

- **Q2: Does the answer change if the advertiser is based outside of Israel?**

  Yes, if the advertiser is not Israeli and the data is processed outside of Israel, it remains an open question which law applies. Technical lex loci delicti analysis should lead to the conclusion that foreign law should apply, but some lower courts determined otherwise (see below).

Scenario 4 (*Advertiser outside Israel*): A user residing in Israel (determined by IP address or geo identifier) goes onto an Israeli domain and is served an ad by an advertiser based outside Israel. The advertiser uses the user data to build a user profile.

This is an open question under the current Privacy Law. Some lower courts applied a lex loci delicti analysis to such circumstances and determined that due to the fact that the privacy-related activity occurred partially in Israel, Israeli law should apply. This was not reviewed by the Supreme Court and therefore no final answer exists. It is likely that given that the domain is Israeli, and the advertiser activity is transparent to the user, courts will be inclined to assume that the activity is taking place in Israel and apply Israeli law.

- **Q: Does the answer change if the advertiser has an affiliate/group company based in Israel?**

  This will most likely lead to the application of Israeli law.

3. DEFINITIONS

3.1. Collect

There is no statutory definition for "collecting" personal data. However, it is likely that this will change with the implementation of the pending 14th amendment to the Privacy Protection Bill (2020) which defines many more concepts than addressed in the current laws.

- **When a publisher allows an ad tech company's pixel on its page, who is deemed to "collect" personal information and incur legal obligations (e.g., controller/co-controller obligations under GDPR or "business" obligations under CCPA) – the publisher, the ad tech company, or both?"**

There is no clear concept of joint-controllers (as explained below). Essentially, the publisher placing the pixel would be considered "collecting" the data and later transferring it to the company. It may be that both publisher and ad tech company are independent database owners and thus both will be subject to the Privacy Law and independently liable for any violations of privacy.

As such, the publisher and ad tech company will be jointly and severally liable for any violations committed under the Privacy Law. Each will be fully accountable to comply with all provisions of the Privacy Law to its fullest extent.

However, it is likely that this concept will be defined with the implementation of the pending 14th amendment to the Privacy Protection Bill (2020) which defines many more concepts than addressed in the current laws.

3.2. Data Processing

There is no equivalent definition for data processing under the Privacy Law. It defines "use" as "including transfer, disclosure and delivery."

3.3. Personal Information

Information regarding the personality, personal status, intimate affairs, state of health, economic situation, professional qualifications, opinions, and beliefs of a person.

Type of Information Collected	Does this Category Independently Constitute Personal Information? (Yes/No)	Qualifying Notes (if any)
IP Address	Yes	The PPA construes PI widely in this matter
Mobile Advertising IDs (IDFA, AAID)	Maybe	Under strict statutory language the answer is no. It may be that if the IDFA is easily readily identifiable that it would constitute PI

Consumer identifiers such as: • User device ID • Publisher persistent ID/Cross-publisher cookie ID • Household ID	Maybe (except household ID, for which the answer is no)	Under strict statutory language the answer is no. It may be that if the identifiers are easily readily identifiable that they would constitute PI
Hashed identifiers such as: • Hashed email • Hashed IP address	No	Market practice differs on this. Under a more stringent approach this will be considered PI, while some organizations take a more liberal approach considering this as non-PI
User Agent such as: • Character string identifying the application • Operating system • Browser information, vendor, and/or version of the requesting user agent	No	
Device Information such as: • Type, version, system settings, etc.	No	
Website Information such as: • Name • URL, etc.	No	
Advertisement Information such as: • Placement • Title • Creative ID, etc.	Maybe	The answer is no if standalone, but if connected to other identifiable information then yes.

Timestamps	Maybe	The answer is no if standalone, but if connected to other identifiable information then yes.
Metrics such as: • Counts • Amounts of time	Maybe	The answer is no if standalone, but if connected to other identifiable information then yes.
Event Data such as: (e.g., full URL including query string, referral URL)	Maybe	The answer is no if standalone, but if connected to other identifiable information then yes.
Precise geolocation (latitude, longitude)	Yes	
General geolocation (city, state, country)	Maybe	For country - no For city - may be identifying in small towns/rural areas

- **Are pseudonymous digital identifiers by themselves personal information (e.g., IDFA, cookie IDs, proprietary IDs, IP addresses, etc.)? Please provide context to the above chart.**

  Please see further elaboration in the chart above. The main question is if a (i) persistent digital identifier can reasonably identify a person, and if so, (iii) whether it constitutes information concerning a person's private affairs. There is no clear definition for a "person's private affairs." For example, it is clear that health and financial information are considered to be a person's private affairs. However, mere identifiers, even if reasonably identifying, but without any connection to actual personal traits, would not be considered personal information. Courts interpret this term on an ad hoc basis and market practice varies.

  Case law is not clear on the definition of "reasonable identification." Practically speaking, many organizations take a cautious approach and follow GDPR-like concepts such as identifiable information, under which any information that is reasonably identifiable (even through cross-references) would constitute personal information. This means that if the information held can be cross referenced with other information to result in identification, each bit of data independently will still be classified as personal identification since it has the capacity to reasonably identify. Others take a more liberal approach and treat

only directly identifying information as "personal information" under the Privacy Law.

- **If the answer to the above question is "no," if a Company possesses a persistent digital identifier in Database 1 and has that same identifier in Database 2 with directly identifying information, does that render the pseudonymous information in Database 1 as personal information?**

  Yes. Under the majority approach taken in Israel, if information can be cross referenced with other information to result in an identification, that would be considered personal information.

- **Is a Company's possession of a pseudonymous identifier plus other non-directly identifying data (e.g., age, gender, precise or imprecise geolocation, user agent string, timestamps) considered "personal information"?**

  Yes, if the combination of the information when cross referenced yields identification to the person.

- **Is a Company's possession of a pseudonymous identifier "personal information" if it can hire a service provider or otherwise engage in a transaction with a third party where the identifier could be matched to the person, but the Company chooses not to hire such service provider or undertake such transaction. Is the mere fact that this service is potentially available to match to the person sufficient to render that pseudonymous identifier as "personal information"?**

  As stated, the law is unclear on this matter and there are varying acceptable market practices. Notably, only under the more stringent GDPR like approach, which is taken by many in the field, the mere ability of the information to be matched renders this information personal identification.

- **What level of geolocation is personal information (precise vs. approximate)? Does it need to be associated with an identifier to be considered PI?**

  No clear answer to this question under existing law. It is likely that country-level location is not personal information, while city-level location may be considered identifying. This is determined by how geographically confined the information is. In small towns and rural areas, city-level location could be considered easily identifying while in larger metropolises this may not be the case.

- **Is a household identifier personal information? (Consider: If a company has a residential IP address (household level ID) and multiple unique device IDs (e.g., MAIDs for every mobile device in the house) associated with that IP address, would that affect whether the household identifier is considered personal information?).**

No clear answer to this question under existing law however likely it is not to be considered personal information. Market practice varies and, in practice, some take the more stringent GDPR like approach under which they view household identifiers as personal information for XXX purpose.

- **Is a hashed identifier personal information? (Consider: There are commercially available services that will take batches of emails encrypted using standard hashes and return (often a high percentage) of clear emails from them. Does that affect whether they are considered personal information, if all a company has to do is pay for the commercial service?)**

  The main question would be if the person is reasonably identifiable from the hashed identifier.
  Under a narrow approach hashed identifiers would not be considered personal information because they are not directly identifying.

  Under a broader approach, gaining wider adoption in Israel, if the hashed identifier is matched with other partially identifying data that yields personal identification each component will be construed as personal information.

  If the hashed identifier has the capacity to be matched with other data and the theoretical outcome would be identifying personal information, each individual component would be considered personal information, including the hashed identifier.

  However, if the potentially matching identifying information is not in the reasonable control of the entity storing the hash, it is likely that this would not be considered identifiable information.

3.4. Sensitive Data

Data on the personality, intimate affairs, state of health, economic situation, opinions, and beliefs of a person, and other information if designated as such by the Minister of Justice, with the approval of a parliamentary committee (no such determination has been made to date).

3.5. Pseudonymous Information

There is no statutory definition under the Privacy Law. However, it is likely that this concept will be defined with the implementation of the pending 14th amendment to the Privacy Protection Bill (2020) which defines many more concepts than addressed in the current laws.

- **Is pseudonymous information considered personal information?**

  There is no clear guidance on this issue under current law. Courts have held that in certain circumstances

data that could be reasonably identified would constitute personal information. See Section 3.3 above for clarification.

- **Are persistent digital identifiers pseudonymous information (e.g., IDFA, cookie IDs, proprietary IDs, IP addresses, etc.)?**

  No. The main question is if these are even identifiable to the person (and thus personal information), and even if so, if these are considered "information of a person's private affairs," which is the threshold criterion for violation of privacy. Many organizations take a GDPR-oriented approach and treat such persistent identifiers as "personal information". Others take a more liberal approach and hold the position that they do not reasonably identify a person, and even if they do, do not disclose information of a "person's private affairs".

- **Does the law subject pseudonymous information to fewer obligations than "regular" personal information?**

  No. There is only a binary distinction between personal information and non-personal information.

3.6. Anonymized/De-identified Information

There are no statutory definitions under the Privacy Law. However, this may change with the implementation of the pending 14th amendment to the Privacy Protection Bill (2020) which defines many more concepts than addressed in the current laws.

- **Is there a difference between anonymized or de-identified information?**

  No. The Privacy Law does not define either. If certain data is not reasonably identifiable, it will not be considered personal information. An unanswered question is the status of personal information that was later de-identified or anonymized.

- **What common information categories are passed between publishers, advertisers, and ad tech companies that fall into this category when no persistent identifier is present (e.g., browser type, device type, operating system, app name, publisher site)?**

  All such examples, if not reasonably capable of identifying the person, are outside the scope of personal information. Even if identifiable, it is questionable if these amount to "information of a person's private affairs," which is the threshold criterion for violation of privacy.

3.7. Data Controller

The Privacy Law does not use the terms "data controller" and "data processor" but rather refers to "database owner," "database holder," and "database manager." Some compare the role of the database owner to that of the data controller under the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"). Although there

are several similarities between the two, they are not the same, as the Privacy Law does not state, as a general rule, that the database owner is primarily responsible for demonstrating compliance with the Privacy Law.

3.8. Joint Controller/Co-Controller

No formal concept of joint controllers, however, given that violation of privacy is a civil tort, general joint tortfeasor doctrine may apply. The pending 14th amendment to the Privacy Protection Bill (2020) contains a definition of "joint controllers" which will become relevant if the bill passes and becomes implemented in Israeli law.

3.9. Data Processor/Service Provider (i.e., an entity that is qualified as a processor or service provider under the law because it meets certain requirements and processes data pursuant to a permissible purpose on behalf of a controller/business)

A database holder under the Privacy Law is one who holds a permanent copy of the database.

3.10. Third Party (i.e., a third party that receives data from a business for non-business purposes and does not necessarily have specific requirements under the law as to such data, such as a third party under the CCPA)

There is no statutory definition or concept under the Privacy Law. However, this may change with the implementation of the pending 14th amendment to the Privacy Protection Bill (2020) which defines many more concepts than addressed in the current laws.

3.11. Database

A collection of data, stored by magnetic or optical means and intended for computer processing, except for:

- A collection of data for personal use that is not business purposes.
- A collection of data that includes only names, addresses and contact information of persons which in itself does not create any characterization that breaches the privacy of such persons, provided that neither the owner of the collection nor any corporation under its control has an additional collection of data.

Note that contrary to previous interpretations of this exemption, on November 28, 2018, the PPA clarified that a collection containing only names and email addresses would not fall under the exemption and therefore will be considered as a database (only available in Hebrew here).

3.12. Direct Marketing

Any personal approach to a person, based on them belonging to a certain group within the population as determined according to a categorization of the subjects of "information" included in the "database" (as defined in the Privacy

Law). There is an unanswered question of whether this applies to ads placed on websites/apps (as opposed to marketing through emails, inboxes, and IMs). The customary understanding is that direct marketing does not apply to targeted ads on websites or in-app.

3.13. Electronic Message (anti-spam related)

An encoded telecommunications message, such as an email, relayed over the internet to a recipient or group of recipients and capable of being saved and restored in a computerized manner. Real time bidding is not a form of electronic message.

3.14. Marketing Message (anti-spam related)

Any of the following can be defined as a "marketing message":

- A message distributed commercially for the purpose of encouraging the acquisition of a product or service or spending money in any other method.
- A message distributed to the public with the purpose of propaganda or making a donation request.
- A message distributed to the public and which includes an offer to call a certain phone number for the purpose of receiving a certain message (all commonly referred to as spam).
- This does not cover targeted advertising relayed over website banners or in-app ads.

4. DATA CONTROLLER RIGHTS AND RESPONSIBILITIES

4.1. Overview

A database owner is required to register its database with the PPA in certain circumstances, as further detailed in section 5 below.

A database owner:

- Who collects personal data directly from data subjects, shall request their consent and inform them: if they are under a legal duty to provide the data, the purpose of collection, and details of any third party that will receive the data and for what purpose.
- Shall either allow a data subject access to any data about him/her kept in the database or refuse to allow such access to the extent permitted by law, as further detailed in section 9 below.
- Shall respond to a data subject's request to rectify or erase any data about him/her kept in the database, as

further detailed in section 9 below.

- Shall be required to appoint an information security officer ("ISO") in certain circumstances, as further detailed in section 10 below.
- Shall document any security incident, and in certain circumstances inform the PPA of such incident, as further detailed in section 11 below.
- Shall notify the Registrar and data subjects of a transfer of ownership in the database (in a merger or acquisition context or otherwise), as further detailed in section 12 below.
- May transfer, or permit the transfer of, data outside Israel in certain circumstances, as further detailed in section 13.1 below.
- Shall require any of its contractors that have access personal data to adhere to certain requirements and shall monitor their compliance with such requirements, as further detailed in section 8 below.
- Shall be required to comply with the security requirements set in the Data Security Regulations, as further detailed in sections 13.3 and 14 below.
- May be subject to administrative fines, and to civil and/or criminal liability, as further detailed in section 12 below.

4.2. Accountability

There are no applicable laws concerning accountability in the realm of privacy. The legislature has recently published new bill proposals to amend the Privacy Law which addresses questions of accountability, but for now there is no binding law in this area.

4.2.1. Overview of Accountability

N/A

4.2.2. Application to Digital Advertising

N/A

4.3. Notice

4.3.1. Overview

- **Who must receive notice? When must notice be provided? What must be in the notice in the digital advertising context? (Consider also, what notice needs to be provided when pixels fire on a webpage?)**

  Notice must be given by the entity collecting personal data whenever it asks data subjects to provide personal data, and prior to or together with such request. This mirrors the general requirement for informed consent. The notice must include the following: whether the data subject has a legal obligation to provide

the data, the types of data collected, types of third parties processing the data, and the purposes of processing. In the context of pixels and cookies, the notice presumably must be given prior to any actual data collection by the pixel/cookie, however, in practice, this is not closely followed in the market. There is still no judicial guidance on this matter.

- **Is a specific notice required for sensitive information?**

  No.

- **Are there any specific requirements for providing notice related to processing children's personal information?**

  No.

- **Are there any requirements compelling vendors directly collecting personal information or those receiving it from others to provide additional notices? Who is responsible for those notices? Publishers? The vendors?**

  No, the notice requirement applies to the collecting entity. In the case of data transfers, the recipient must make sure that the transferor complied with the notice requirement. For example, if a pixel is placed on a publisher's website, it will likely be the publisher's duty to notify. However, as explained above, in circumstances where the ad tech company is an independent controller it will still be directly liable for any failure to comply with the notice requirement. The contractual mechanism will only provide for indemnification in this scenario. We note that the representations regarding adequate notification should be circulated throughout the ad supply chain.

4.3.2. Application to Digital Advertising

- **Do third parties need to be named? For example, if a publisher gives privacy policy notice that it may share personal information with third parties for advertising purposes, does it have to specify which third parties? Do specific digital advertising activities or purposes need to be disclosed as well (e.g., TCF purposes)?**

  No, for controller-processor transfers, only categories of third parties are required, but the Privacy Protection Authority recently noted that in the context of payment services apps and websites, a clear disclosure of any ad-related cookies must be made as part of the notice. For controller-controller transfers, Article 2(a)(4) of the Protection of Privacy Regulations (Data Security) 2017, the identities of the actual transferees are required.

- **From an industry perspective it is common to distinguish data use for ad targeting vs. profile building vs. measuring ad campaigns. Does the notice requirement require separate disclosure of those things or is it enough to say something general like "advertising and related purposes"?**

  There is no explicit requirement for granular disclosure and therefore "advertising, including targeted advertising and profiling purposes" may be sufficient. There are pending cases challenging the level of disclosure required, but no guidance as of today.

4.4. Consent and Exceptions to Consent

4.4.1. Overview

Marketing messages to consumers generally require explicit opt-in consent in which the consumer is fully informed and gives full free prior consent. Approaches utilizing direct marketing services and certain direct marketing approaches generally require opt-in consent.

Section 30A(c) of the Communications Law allows for the sending of marketing messages to existing or potential customers who have shown an interest in the products or services of a business without their opt-in consent, provided that a notice is sent to such customers promptly after their inquiry with the business.

The notice should explain that:

- Such marketing messages can be sent.
- The marketing messages will be confined to the same products or services the customers was interested in.
- An opt-out option will be provided to the customers prior to the sending of any marketing messages.

The Direct Marketing Guidelines require opt-in consent for any direct marketing activity that is not directly linked to the course of business in which personal information is collected and the products or services are provided by a business, or where the direct marketing approach involves direct marketing services. However, the Direct Marketing Guidelines do allow direct marketing approaches by a business with respect to its ordinary course of business, products, and services, without opt-in consent, provided that opt-out options are presented to the recipients as well as some additional mandatory information requirements.

Direct marketing requirements do not apply to business to business ("B2B") contexts since businesses do not enjoy privacy protection under Israeli law. However, the marketing messages requirements set forth above apply to B2B contexts as well. The only difference is that a business is allowed to send one initial marketing message to another business in order to advertise their products and services without opt-in consent, provided that the mandatory notices and opt-out requirements apply. Any further marketing message is contingent on opt-in consent being provided.

Donation requests and propaganda by political parties are exempt from the opt-in consent requirement with respect to marketing messages, provided that the recipient did not inform the sender that it declines receipt of such marketing messages.

Telecommunications service providers acting as "mere conduits" are exempt from liability for marketing messages.

- **For what types of personal information or purposes of processing is consent required?**

Consent is required in the following circumstances:

1. Using personal information for the purpose of sending marketing messages and robocalls.
2. Utilizing direct marketing services and some direct marketing approaches.
3. Targeted advertisements based on the profiling of personal information.
4. Transfer of data to a new database owner.
5. Communication of advertisements by advertisers.

- **How is valid consent manifested – express consent, opt-in, implied consent, or opt-out?**

1. **Using personal information for the purpose of sending marketing messages:**
   Explicit opt-in is required, meaning, a designated non-populated checkbox or other affirmative consent.
2. **Utilizing direct marketing services and some direct marketing approaches:**
   Explicit opt-in is required, meaning a designated non-populated checkbox or other affirmative consent, and granular explanation of the purpose.
3. **First party targeted advertisements based on the profiling of personal information:**
   For targeted advertising, explicit consent is required.
4. **Transfer of data to a new database owner:**
   Prior consent is required.
5. **Communication of Spam messages by advertisers:**
   Explicit consent with an unsubscribe option is required.

- **Is specific notice required as part of the consent?**
  No.

- **Does the consent obligation require granularity (i.e., consent for distinct processing activities) similar to GDPR? Or is the consent obligation more generalized (e.g., requiring consumers to opt-in to "online behavioral advertising" more broadly, without having to consent to each constituent processing activity/ party)? Is consent different for different uses or types of data (e.g., sensitive data, profiling, automated decision making, etc.) Please provide details.**

Generally, consent under the Privacy Law does not have to be granular similar to GDPR, rather only informed (and could be obtained explicitly or implicitly). For profiling-based targeted advertising, the consent requirements may be more granular and augmented consent will be required in scenarios such as the processing of sensitive data.

- **Can personal information be processed for secondary purposes (i.e., differing purposes from which it was collected)?**

  No. The Privacy Law provides a purpose limitation principle.

- **Are there any rules compelling downstream recipients/processors of personal information to provide additional notices?**

  No.

- **Are there any issues concerning the timing of consent?**

  The applicable Israeli law does not address the timing of consent.

- **Are there distinct consent requirements for sensitive personal information?**

  No.

- **Are there distinct consent requirements for profiling consumers? For example, if a business gets consent to use personal data for "advertising and marketing" purposes, is a separate (or more specific?) consent required to build an advertising profile for advertising?**

  Processing based on the profiling of personal information is considered to fall under the scope of the Privacy Law and therefore requires opt-in consent and further formal requirements. The general purpose of advertising and marketing is not clear enough to constitute informed consent for profiling.

- **Are there distinct consent requirements for automated decision making?**

  The applicable Israeli law does not address automated decision making.

- **Are there any age restrictions related to consent? Are there distinct consent requirements around processing children's personal information?**

  There are no specific age-related restrictions.

- **Can consent, however manifested, be revoked?**

  The law does not provide a right to withdraw consent for processing.

4.4.2. Application to Digital Advertising

Israeli courts have deemed marketing messages relayed over private messages in social media platforms to be subject to the requirements set forth above in situations where exceptions apply, such as profiling consumers for digital advertising purposes. In such an instance, opt-in consent would be required under the Privacy Law. This is also true to specific "private messaging accounts" provided to users of certain services and apps.

However, targeted advertisements appearing on social media, including posts and other elements (including programmatic advertising), are not considered to be marketing messages. It is an open question whether such targeted advertisements, assuming that they are based on the profiling of personal information, should be considered within the scope of the Privacy Law, and thus require opt-in consent and further formal requirements.

Marketing messages relayed over electronic messages should include the word "Ad" in their subject line, and if relayed over a short message, at the beginning of the marketing message. The marketing message must include the name, address, and contact details of the advertiser and a simple means through which an opt-out request can be made. Direct marketing approaches should include the option to opt-out, an explanation that the approach is based on profiling, and the sources from which data was collected (including the number of the registered database on which the approach is based). Israel does not operate a national opt-out list for e-marketing.

There is no explicit statutory language with respect to viral marketing in the Communications Law. However, since the term "advertiser" is defined as whosever name or address appears in the marketing message, whosever business is promoted by the content of the marketing message, or whoever markets the subject of the marketing message for another person, the marketing message requirements may apply to entities involved in the process of viral marketing. There are proceedings pending in Israeli courts regarding the joint liability of service providers involved in the mass distribution of marketing messages. Several motions to allow class actions in this regard have been granted. However, there are no final decisions on the merits.

The use of marketing lists based on personal information and profiling is subject to requirements in connection with direct marketing. The transfer of marketing lists is subject to the general provisions of the Privacy Law with respect to any personal information included in such lists.

4.5. Appropriate Purposes

4.5.1. Overview

Israeli law adopts a general concept of limitation of purpose for personal information processing.
There is no concept of generally appropriate or inappropriate purposes.

4.5.2. Application to Digital Advertising

By and large Israeli law does not address digital advertising in depth, as such there are no normative sources from

which guidance can be provided as to digital advertising in the context of purposes for processing personal data.

Does the law or legal guidance require a specific legal basis for specific digital advertising activities? Clarify for each activity (suggest using TCF/IAB CCPA "purposes") ("profiling" must be addressed here).

The general legal basis is informed consent. There is a question regarding the level of granularity required. It is customary to explicitly inform of profiling and targeted advertising activities even if no additional consent is required.

- **If yes, what are the legal bases (e.g., consent, legitimate interest)? Are there any requirements related to lawful basis (need a valid legal basis to process)/fairness (scope of processing is fair)/transparency (transparent about the processing activity to the consumer and the lawful basis)?**
  N/A
- **Does the law address processing for secondary purposes/differing purposes from which it was collected?**
  Yes, there is a general limitation of purpose provision. Consent should be obtained for the applicable purposes.

4.6. Safeguards

4.6.1. Overview of Safeguards

The relevant Israeli law is Article 14 of the Protection of Privacy (Data Security) Regulations, 5777-2017.

Article 14(a) prohibits a database owner from connecting the database to the internet or another public network without installing appropriate safeguards to prevent unauthorized infiltration or systems which can damage the materials.

Article 14(b) requires the transfer of data from a database to be done with appropriate encryption methods.

Article 14(c) adds an additional level of protection for remote access to a database. In these instances, further safeguards must be applied for the purpose of identifying the user connecting to the database and enabling performance by remote access. For remote access to medium or high security databases, authorized access will be done with a physical medium exclusively in control of the authorized user.

4.6.2. Safeguards in Digital Advertising

The relevant Israeli law about safeguards does not specifically address digital advertising.

5. DATA SUBJECT RIGHTS/EXEMPTIONS

5.1. Overview

Israeli law provides data subjects with rights of access, rectification, and deletion. These rights are not absolute and are limited in various circumstances.

5.2. Access

A data subject may inspect any information about him/her that is kept in a database, whether in person, or by a representative or guardian. The database owner shall enable the inspection of the information in Hebrew, Arabic, or English, as requested by the data subject.

If a database is maintained by a database holder on behalf of a database owner, then the database owner must refer a data subject asking to access the information to the database holder and instruct the database holder to allow such inspection.

Pursuant to the Data Inspection Regulations, the data subject shall pay the owner or holder of the database a fee of ILS 20 (approx. €5) for the inspection. Inspection must be permitted within 30 days of the request, although the Registrar may extend the period by an additional 15 days.

The Data Inspection Regulations allow the database owner to provide a print-out of the requested information as the equivalent of permitting inspection of the data, but the print-out shall not be removed from the premises of the database owner or holder without permission.

A database owner or holder may refuse the request for inspection of data from a database if:

- The database is of one of the types of databases the Privacy Law determines shall not be subject to inspection (e.g. a database of a security authority, tax authority, the database of the Israel Prison Service, data that the disclosure of may harm Israel's security or foreign relations or is prohibited by the provisions of any legislation).
- The database is a service bureau that processes and stores data for its customers, so long as the database owner or holder refers the data subject to the owner of the data on whose behalf the processing or storage services are performed.

The data subject shall be notified if his/her request to inspect data is refused within 21 days of the request, although the Registrar may extend the period by an additional 15 days.

In the event the request is denied, the data subject requesting the data may file a suit in accordance with the procedures set forth in the Data Inspection Regulations.

A database owner may refrain from providing data to a data subject for his/her inspection if:

- The data relates to the data subject's physical or mental health, and the database owner believes that such data may endanger the life of, or cause severe harm to the data subject's physical or mental health, then the database owner shall provide the data to a physician or psychologist on behalf of the data subject.
- It will breach a legal privilege applicable to the data, as prescribed under any legislation or ruling, unless the data subject is the legal person for whose benefit the privilege is enacted.

5.3. Rectify

The Privacy Law provides that if a data subject inspects data about him/her and finds that it is inaccurate, incomplete, unclear, or not up-to-date, the data subject may request from the database owner or holder that such data be amended or deleted. This is, however, not an absolute right, and the database owner may refuse to accommodate such erasure requests.

If the database owner agrees to the request, the amendments to the data or its erasure shall be communicated to anyone who received the data from the database owner within the preceding three-year period. The data subject shall be notified if his/her request to rectify or erase the data is refused within 30 days of the request, although the Registrar may extend the period by an additional 15 days.

A data subject may demand, in writing, from the owner of a database used for direct mailing that the information about him/her be deleted from such a database.

5.4. Deletion/Erasure

No additional erasure right except for the rectification right above.

5.5. Restriction on Processing

No explicit concept of restriction of processing.

5.6. Data Portability

No concept of data portability other than the digital right to access.

5.7. Right to Object

The Privacy Law allows a data subject to object to the processing of data only by means of a civil suit based on the claim that the processing violates the data subject's right to privacy. However, there is no established concept of a general right to object processing once the personal data has been provided for processing without violation of privacy (e.g., with the consent of the data subject). As of today, it is generally understood that data subjects in Israel do not have a right to withdraw their consent for processing.

In the PPA's Transfer of Ownership Draft Guidelines (which are still subject to change), a data subject's consent to processing must be obtained prior to the transfer of the data about such data subject to the new owner of the database.

A database holder and a database manager may be subject to administrative fines, and to civil and/or criminal liability.

5.8. Right Against Automated Decision-Making

Not applicable under existing law.

5.9. Extra-territorial Data Transfers

According to the Privacy Protection (Transfer of Data to Databases Abroad) Regulations, for a database owner in Israel to transfer data outside of Israel, consent of the data subject must be obtained. In extreme cases, such as when the data must be transferred for the health or wellbeing of the data subject and consent cannot be obtained, it may be transferred without prior consent. Article 2 of the law also enumerates other exceptions to consent, such as if the data is public or the transfer is mandated by law.

5.10 Responding to Consumer Rights Requests

Database Owners must respond to data subject requests within 30 days. No explicit identification measures required, other than the form in which the data subject must file the signed request.

5.11. Recordkeeping Concerning Rights Requests

Please refer to Section 5.2 above.

5.12. Is Providing Consumers with These Rights Required by Law or Mere Suggestions?

As detailed above, some of the data subject rights are mandatory and other are not included in the legislation at all.

5.13. Application to Digital Advertising

Data subject rights are primarily exercised against database owners (controllers). Database holders (processors) only have an obligation to forward the request to the owner and provide required assistance. Database holders do not have an obligation to further communicate data subject requests. In independent controller contexts, one controller is not required to forward data subject notices to other controllers.

6. DATA CONTROLLER AND PROCESSOR AGREEMENTS

6.1. Overview

According to the Data Security Regulations, an owner of a database engaging a contractor for the provision of a service that requires granting such contractor access to the database, shall assess, prior to the engagement, the data protection risks involved in such engagement.

Considering the aforementioned risks, the Data Security Regulations require that the following matters shall be explicitly regulated in the database owner's agreement with the contractor:

- The data which the contractor will be authorized to process and the purpose of such processing.
- The type of processing which the contractor shall be authorized to perform.
- The database systems which the contractor will be authorized to access.
- The term of the contractor's engagement and how the data will be returned to the database owner at the termination of such engagement.
- Directions as to how the contractor, a database holder, shall perform its obligations pursuant to the Data Security Regulations and other obligations imposed by the database owner.
- The contractor's duty to have its personnel sign an undertaking regarding confidentiality and adherence to the agreement between the database owner and the contractor.
- The contractor's duty to inform the database owner of any security event and to provide a report to the database owner, at least annually, regarding its performance of all the above.

The database owner shall monitor the contractor's compliance with the terms of the agreement between the database owner and the contractor and with the Data Security Regulations, in the scope and to the extent appropriate considering the risks to data protection.

6.2. Data Controller Outsourcing of Processing

See Section 7 below.

6.3. Data Processor Rights and Responsibilities

A database holder and a database manager may be liable for holding or managing a database prior to its registration with the Registrar.

A database holder shall either allow a data subject access to any data about him/her kept in a database it holds according to the instructions of the database owner or refuse to allow such access to the extent permitted by law, as further detailed in section 9 below.

Additionally, a database holder shall be required to appoint an ISO in certain circumstances, as further detailed in section 10 below, and adhere to the database owner's directions and requirements, as further detailed in section 13 below.

A database manager shall inform the Registrar as to the identity of an ISO appointed in the database it manages, as further detailed in section 13 below.

A database holder and a database manager are required to comply with the security requirements set in the Data Security Regulations.

6.4. Application to Digital Advertising

It appears that in most cases, given that ad-tech companies and publishers process data for their own internal purposes, they will be considered independent Database Owners. However, if an ad tech company processes personal data also for the benefit of the publisher, it may be considered a Database Holder of that publisher thus requiring a DPA between the parties.

7. DATA TRANSFER AND OUTSOURCING

7.1. Overview

In the PPA's Transfer of Ownership Draft Guidelines, the PPA presents its proposed position with respect to the duties of database owners and the rights of data subjects in situations where the ownership of a database is transferred to another legal person due to sale of the database, or of the merger or acquisition of the database owner.

According to the Transfer of Ownership Draft Guidelines, such duties and rights include the following:

- The transferring database owner (the former owner) and the recipient database owner (the new owner) shall notify the Registrar of such transfer of ownership.
- If the characteristics of the database recipient are different from those of the transferring database owner in a significant way that may adversely affect the rights of a data subject, then the data subject's consent must be obtained prior to the transfer of the data to the database recipient. If such data subject's consent was not obtained, the data about him/her should not be transferred to the database recipient and should be erased.

- If, due to the transfer of ownership in the database, the purposes of processing of, or the processing activities performed on, the data in the database shall change, the data subject's consent must be obtained prior to the transfer of the data to the database recipient.
- If, due to the transfer of ownership in the database, the purposes of processing and the processing activities shall not change, generally notifying the data subjects of the transfer of ownership and contact details of the database recipient shall suffice.

The Transfer of Information Regulations state that data from a database in Israel shall not be transferred to another country, except if the law of such country ensures a level of protection with respect to personal data that is no less stringent than that provided by Israeli law. On July 1, 2020, the PPA notified that its position is that the law of the European Union ensures such level of protection, and therefore transfer of personal data to countries that are or were members of the European Union is permitted, provided that those countries continue to comply with the provisions of the European Union law with regard to protection of personal data.

Notwithstanding the foregoing, a database owner may transfer, or permit the transfer, of personal data to another country if:

- The data subject gave his/her consent to the transfer.
- The data subject's consent cannot be obtained, and the transfer is necessary in order to protect the data subject's health or bodily integrity.
- The data is transferred to an entity under the control of the database owner and the database owner ensured the protection of the personal data post-transfer.
- The data is transferred to an entity that is obligated in an agreement with the database owner to hold the information in accordance with the conditions required in Israel.
- The data was made public according to lawful authority or was made available for public inspection according to lawful authority.
- The transfer of the data is imperative for the protection of public safety.
- The transfer of the data is mandatory pursuant to Israeli law.
- The data is transferred to a country which is party to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108") or receives data under similar conditions.

On July 1, 2020, the PPA clarified that personal data may continue to be transferred to the United Kingdom after its withdrawal from the European Union, since the United Kingdom is party to Convention 108. This includes

transfers of data to countries who enjoy an "adequacy" status by the European Commission, or other transfers of data to non-EU countries which comply with the data transfer requirements of the GDPR (e.g., under Standard Contractual Clauses).

If data is transferred, the database owner shall obtain the recipient's written obligation that it takes measures appropriate to ensure the protection of the data and that it shall not transfer the data to any person, whether in the same country as the recipient or otherwise.

7.2. Application to Digital Advertising

The relevant Israeli law does not explicitly address this, however if by placing a pixel on an Israeli page personal data is being exported outside of Israel, the pixel-owner must provide the publisher with sufficient guarantees to meet the foregoing export requirements.

8. AUDIT/ACCOUNTABILITY

8.1. Overview

- **Audit - What audit rights are dictated by law (e.g., must companies have audit rights over their vendors? Does it matter what the classification of those vendors are?)?**

The Israeli legislation demands periodic internal audits for security purposes, the frequency varies based on the classification of the database. For example, a medium or high-security database is audited annually.

- **Accountability - Must companies/vendors keep certain records to prove they have met certain requirements? What are those requirements?**

A database owner must keep the audit records for a period of one year. A medium or high-security database must keep the records permanently in a manner that always them to be restored to their original state at any time.

Records retention periods are sectorial in Israel and practice differs between industries. In instances where this is not clearly defined by law market practice is to exercise caution in determining retention periods. Termination of retention should be non-arbitrarily decided, and it is recommended practice to document reasoning behind specified duration.

8.2. Application to Digital Advertising

The Israeli law does not address digital advertising in depth; as such, there is no guidance as to the applicability of digital advertising in this context.

9. DATA RETENTION

9.1. Overview

A data subject may request that data about him/her be erased from a database, as further detailed in section 9 above. Under the Data Security Regulations, a database owner must consider, on a yearly basis, whether the personal data included in its databases exceeds what would be considered necessary for such database owner. Effectively, this requires database owners to establish data retention policies.

9.2. Application to Digital Advertising

As with any database owner, if a digital advertising company is a database owner under the Privacy Law, it will have to consider, on an annual basis, if it retains excessive data. If data is no more updated or relevant for the business of such advertising company, it may be necessary to purge such data.

10. DATA PROTECTION AUTHORITY | REGULATORY AUTHORITY

10.1. Overview

The Privacy Protection Authority is the Israeli regulatory and enforcing authority for personal digital information, in accordance with the Privacy Protection Law. The authority is responsible for the protection of all personal information held in digital databases. The regulation includes administrative and criminal enforcement, and applies to all entities in Israel - private, business, and public - that hold or process personal digital information.

10.2. Main Regulator for Data Protection

The Israeli regulatory authority, the PPA, was founded in 2006, and is part of the Ministry of Justice. The head of the PPA also serves as the Registrar of Databases ("the Registrar"). The PPA is responsible for the protection of all personal information held in digital databases, including through the use of administrative and criminal enforcement.

10.3. Main Powers, Duties, and Responsibilities

The PPA represents Israel in the international privacy arena and participates in the legislative process. As mentioned above, the PPA publishes guidelines that reflect the PPA's interpretation of the obligations under the Privacy Law. The PPA has administrative and criminal investigatory powers and may conduct inspections and audits on any entity subject to the Privacy Law. The PPA may also impose administrative fines, in certain circumstances, as described below.

The Registrar is required to maintain the Registry of Databases and is empowered to supervise compliance with provisions of the Privacy Law and the regulations issued thereunder. The Registrar is authorized to refuse to register a database if it has reasonable grounds to assume that:

- The database is used, or might be used, for illegal activities, or as a cover for them.
- The data included in the database was obtained, accrued, or collected in breach of the Privacy Lawor any other law.

10.4. Application to Digital Advertising

The Privacy Protection Authority has competence to issue guidelines with respect to digital advertising involving personal data processing in Israel. It has not explicitly done so thus far, but it is certainly a relevant player to consider.

11. SANCTIONS

11.1. Overview

Israeli law implements both criminal and civil sanctions for violations of the Privacy Law. This is enforced by the Privacy Protection Authority as well as the police and Courts when needed.

11.2. Liability

- **Scope of liability for publishers and advertisers for processing activities of ad tech companies**
  Publishers are almost always controllers and are thus directly liable for any privacy violation. Ad tech companies can be either processors, thus liable to a limited subset of requirements under the Law (mainly information security and confidentiality), or independent controllers and as such are independently liable for any violation of the Law.
- **Scope of liability for ad tech companies for collection activities of publishers and advertisers**
  As explained above, ad tech companies acting as processors are not liable for collection activities of publishers, however they would be if independent controllers.
- **Scope of liability for ad tech companies for other ad tech companies they enable to process data (either b/c they make the decision of pub or advertisers or agency dictates it)**
  Ad tech companies disclosing personal data to other third parties (controllers or processors) will be liable for any violation by such third parties.

11.3. Enforcement and Market Practice

- **How are claims raised under the law?**
  Either criminally or administratively through the PPA or privately.

- **Who enforces them?**
  The Privacy Protection Authority ("PPA") or other law enforcement bodies.
- **What is their practice (quietly working with companies to fix, publicly coming out with large investigations? Fact specific?)**
  The practice varies from case to case, depending on the gravity of the infringement. The first step is usually an undercover or open investigation by the relevant law enforcement unit or an administrative enforcement procedure.
  If the infringement is labeled as an administrative offence there are a variety of tools that may be used against the infringers:

  (1) Rectifying the infringement under observation of the PPA.
  (2) Prohibiting the use of the information and/or the database by suspending or cancelling the registration of said database.
  (3) Fining the infringers administratively.
  In extreme circumstances: the infringement is of a criminal nature; the evidence re the infringement shows that the infringer is complicit; then the police may recommend pressing charges.
- **What guidance to date has there been on how to handle requirements in the ad ecosystem? Have the regulators been educated on how the ecosystem operates? Have compliance regimes been discussed with them? Has their feedback been solicited?**
  The PPA did not issue any guidance designated for the ad tech ecosystem. The only relevant guidance is with respect to Direct Mailing as explained in Section 17.2 below which mainly focuses on profiling and data enhancing services and respective opt-in consent requirements.

11.4. Remedies

The Administrative Fine Regulations authorize the Registrar to impose administrative fines of ILS 2,000 (approx. €500) on an individual for:

- Using, holding, or managing an unregistered database which requires registration.
- Delivering false information in a database registration application.
- Failing to deliver documents or an affidavit to the Registrar, on an annual basis, by a holder of at least five databases which require registration.
- Managing or possessing a database used for direct mail services without properly tracking the sources of the information used.

Administrative fines of ILS 3,000 (approx. €750) may be imposed for:

- Managing or possessing a database used for direct mail services without designation of such use in the database registration.
- Managing or possessing a database used for direct mail services without properly notifying data subjects or responding to requests for removal.
- Failing to deliver information or delivering false information in a notice soliciting information that will be included or used in a database.
- Failing to comply with data subjects' inspection rights.
- Granting access to a database to a legal person not authorized under a written agreement between the database holder and database owner.
- Failing to appoint an ISO for databases which are so required by law.

An administrative fine of ILS 5,000 (approx. €1,250) may be imposed for using information from a database for purposes differing from those for which the database was registered.

A five-fold fine for every type of breach listed above shall be imposed on a corporation. For continuing breaches, one-tenth of the fine can be imposed for each day of such continuance of the breach after a warning of the breach has been served, and for repetitive administrative offenses the fine is doubled.

Those found to have committed the aforementioned types of breaches may be charged with criminal liability and subjected to a one-year term of imprisonment. These are strict liability offences, as neither criminal intent nor negligence need to be proven.

Those found to be in breach may be subjected to five years imprisonment for disclosing data obtained by virtue of their position as an employee, manager, or holder of a database, except for disclosure for the purposes of performing one's duties, compliance with the Privacy Law, or under a court order in connection with legal proceedings. Violations of general privacy obligations (i.e., not specifically related to databases), such as publishing or handing over information that was obtained through breach of certain provisions of the Privacy Law, or publishing of a matter that relates to a data subject's intimate life or state of health, may entail five years imprisonment provided that such violations were conducted with malicious intent (a relatively high standard under Israeli criminal law).

11.5. Private Right of Action

A breach of privacy is actionable as a civil wrong pursuant to the Privacy Law, and a claimant may obtain monetary compensation or injunctive relief. A court may award damages amounting to ILS 50,000 (approx. €12,490) without

proof of damages for breach of privacy rights, and if such breach was intentional the damages may be doubled. Such statutory damages apply only to individual claims and cannot be the basis for class-action damages. In addition to providing that a breach of privacy is actionable as a civil wrong, the Privacy Law also specifies that an act of omission in breach of certain of its provisions may give rise to a tortious claim under the Torts Ordinance 2009 (New Version). This provision was added in order to ensure that even omissions, such as a failure to ensure data security, would also be actionable as a civil wrong. As a civil wrong, in certain cases such as business-consumer relationships, violation of privacy could be actionable as a class action under the Israeli Class Action Law, 2006 (only available in Hebrew here).

No civil or criminal action may be brought for breaches that cause no substantive harm. In addition, the Privacy Law provides the following defenses from liability:

- The violation of privacy was done through a protected publication under the Israeli Libel Law, 1965 (only available in Hebrew here).
- The infringing party performed the violation in good faith under one of the following circumstances:
    - They did not know and were not supposed to know about the potential violation.
    - The violation was committed in circumstances under which the infringer has a legal, moral, social, or professional duty to do so.
    - The violation was committed in order to protect a legitimate interest of the infringer.
    - The violation was committed in the lawful ordinary course of business of the infringer and was not publicly disclosed.
    - The violation was committed through the photography or publication of photographs taken in public places in which the plaintiff appeared incidentally.
    - There was a public interest justifying the violation, and if it was performed by publication, the publication was truthful.

11.6. Digital Advertising

The Privacy Law imposes certain obligations with respect to databases that are used for direct mailing and direct marketing services (as defined below). For example, any approach to a person in a direct mailing requires a notice that will disclose the fact that it is a direct mail, the sources of the personal information used for the direct mailing, the rights of the data subject to be deleted from the database or applicable mailing list, and similar matters. Direct mailing should be distinguished from spam activities.

The term "direct mailing" is defined as "any personal approach to a person, based on his belonging to a certain group

in the population, determined according to a categorization of the data subjects included in the database." The term "direct mailing services" is defined as "direct mailing services to others by providing lists, stickers or other personally identifiable information to others for the purpose of direct mailing."

In addition to the Privacy Law, Section 30(a) of the Anti-Spam Law provides a general prohibition on the publication of advertisement by means of distribution of spam messages. An "advertisement" is defined as a "commercially distributed message which purpose is to encourage the acquisition of a product or service or the expenditure of monies in any other way." An "advertiser" is defined as "the person whose name or address appears in the advertisement for communication purposes or for the acquisition of the subject of the advertisement, whoever the content of the advertisement may publish its business [...] or whoever markets the subject of the advertisement of another person."

The general prohibition is on the communication of advertisements by an advertiser, using certain technological means, without the explicit consent of the recipient. In addition, even if consent of the recipient is obtained, the Anti-Spam Law requires that any advertisement sent to a recipient include the word "advertisement" in the subject line as well as the contact details of the advertiser and the option for the recipient to unsubscribe from receiving future advertisements.

Liability Issues

Violation of the marketing message requirements can be punishable by:

- Civil – Statutory damages of up to NIS 1,000 (approx. €270) per message for personal claims. Eligible for class action litigation with a requirement to prove non-monetary damages.
- Criminal – Fine of up to NIS 226,000 (approx. €60,720) (and up to NIS 75,300 (approx. €20,230) for office holders and directors).

Violations of the direct marketing requirements can be punishable by:

- Civil – Personal claim with proof of non-monetary damages, and potentially class action litigation with a requirement to prove non-monetary damages; If a licensed telecommunications provider infringes a condition of the license, the Minister may restrict, revoke, or suspend their license.
- Administrative – Fine of up to NIS 15,000 (approx. €4,030) per violation.
- Criminal – Up to one-year imprisonment.

12. NOTIFICATION, CERTIFICATION, REGISTRATION

12.1. Overview

Israel currently has a database registration requirement, and databases with personal data generally need to be registered with the Privacy Protection Authority. This is a mainly bureaucratic requirement and not too onerous. The Authority and the legislator proposed to abolish this requirement, and it is expected to happen in the near future.

12.2. Requirements and Brief Description

Subject to certain exceptions (see below), a database owner is required to register its database to the extent that one of the following conditions are met:

- The database contains data in respect of more than 10,000 data subjects.
- The database contains sensitive data.
- The database includes data about persons, and such was not provided by them, on their behalf, or with their consent.
- The database belongs to a public entity.
- The database is used for direct mailing services.

A database must be registered prior to managing or holding the database unless the Registrar permits performing such acts prior to registration.

Although the Privacy Law imposes the obligation to register on the database owner, the Privacy Law also prohibits managing or holding a database that is required to be registered but has not been registered. Therefore, database managers or database holders could also face liability in connection with a database that is not registered.

Databases are exempt from the registration obligation where:

- The database only contains data made public according to lawful authority.
- The database only contains data which was made available for public inspection according to lawful authority.

12.3. Application to Digital Advertising

The Israeli law does not address digital advertising in depth; as such, there is no guidance as to the applicability of digital advertising in this context.

13. DATA PROTECTION OFFICER

13.1. Overview

The Israeli law does not require the appointment of a DPO; however, it is it considered best practice and heavily encouraged. The appointment of a DPO assists the entity to ensure they are in strict compliance with the relevant laws and guidelines. The choice to appoint a DPO is viewed as an indication that the organization is taking steps to reduce the risk of a privacy infringement and enables cooperation with the PPA.

13.2. DPO – Compulsory Appointment (Yes/No)

Appointment of a data protection officer ("DPO") is not required under the Privacy Law. However, there is a requirement to appoint an ISO by an entity meeting one of the following conditions:

- Entities holding five or more databases requiring registration.
- Public bodies.
- Banks, insurance companies, or companies involved in ranking or evaluating credit.

13.3. Requirements

The database manager must inform the Registrar as to the identity of the ISO.

Failure to nominate an ISO when required to do so may result in criminal sanctions, and or administrative fines. While the ISO is to be responsible for data security, the database owner, holder, and manager nevertheless are each held individually responsible under the Privacy Law for data security as well.

The Privacy Law does not require that the ISO should be an Israeli citizen or resident. An individual convicted of an offence involving moral turpitude or an offence stipulated in the Privacy Law may not be appointed as an ISO.

The Data Security Regulations further detail the duties of the ISO and of the database owner with respect to the ISO. The ISO shall receive resources from the database owner in order to carry out its duties and shall report directly to the database manager. The ISO shall not perform other duties if such other duties may result in a conflict of interest with its duties as an ISO. The ISO shall develop a data protection procedure, and have it approved by the database owner, and shall develop an ongoing monitoring program and notify the database owner and the database manager of its results.

13.4. Application to Digital Advertising

The Israeli law does not address digital advertising in depth; as such, there is no guidance as to the applicability of digital advertising in this context.

14. SELF-REGULATION

14.1. Overview

There is no standard for self-regulation in terms of compliance with privacy and data protection laws in Israel.

- **Are there any industry self-regulatory schemes in place in the jurisdiction?**
  No.
- **Are there any signal-based programs used in the territory to assist with digital advertising compliance?**
  No.

14.2. Application to Digital Advertising

15. PENDING PRIVACY BILLS

15.1. Overview

Due to political issues, a few pending bills are awaiting parliamentary review:

Bill to Amend the Privacy Protection Law, 2018 (Enforcement Powers) (13th Amendment):

In 2018, the bill proposal passed the first of three required readings, but unfortunately has not progressed further due to the dispersal of the Israeli Knesset.

The bill is set to introduce new offenses such as prohibitions against the use of information contrary to its intended purpose; unsolicited use of data; and initiation of contact to obtain information under false pretenses. The bill also establishes new obligations such as personal liability of corporate officers for lax observation and failure to prevent privacy violations; the duty to give administrative warnings to violators, and a duty to refrain from violation of the law.

This amendment will revolutionize the enforcement authorities of the PPA as it amplifies the PPA's powers to impose heighted financial sanctions for various offenses including the violation of the Information Security Regulations. Such sanctions may be multiplied for the prohibition of using information contrary to its intended purpose. The PPA will also have a new enforcement capacity which allows it to conduct administrative supervision and hold administrative inquiries; enforce criminal liabilities; and appoint authorized investigators and supervisors.

The bill also creates a new internal procedure to be followed by security agencies which includes financial sanctions.

The Privacy Protection Bill (14th Amendment) 2020:

A legal memorandum regarding this bill was published on 23.7.2020 and the bill is still in its draft stages.

This amendment seeks to redefine key concepts in the field of privacy:

- Information.
- Highly sensitive information.
- Database owner.
- Database controller.
- Processing of personal information.
- Biometric identifier.

The amendment significantly minimizes the registration requirement. Registration will only apply to databases which hold the information of over 100,000 information bearers, and then only if: the data is sensitive; or belongs to a public entity; or belongs to an individual involved in information sales; or if the information was collected without its owners' permission.

The amendment establishes a prohibition to operate a database in which the information was created or collected unlawfully.

Memorandum to Amend the Privacy Protection Law, 2020 (Limiting Registration Requirements and Definitions) (15th amendment):

This amendment is intended to reform the entire privacy law by introducing new core definitions to the Privacy Law.

In July 2020, a public declaration was put forth inviting the public to suggest further changes to the law.

The topics expected to be raised in the legislative discussion are as follows:

- Establishing additional bases for information processing asides from authorization and approval.
- Improvement of the rights of information owners such as the right to be forgotten; the right to information mobility; and automated information processing.
- Responsibilities of database holders - appointment of a Data Protection Officer (DPO), conducting surveys on the influence of privacy, and privacy by design.
- Privacy regarding minors and other specified groups.

15.2. Application to Digital Advertising

1. Import to the digital advertising industry.

The Israeli law does not address digital advertising in depth; as such, there is no guidance as to the applicability of digital advertising in this context.

2. Likelihood of enactment and other procedural hurdles

The 2020-2021 ongoing COVID-19 pandemic has delayed many non-healthcare related issues sitting on the legislature's desk, as such, the pending privacy bills have been put on hold.

Additionally, the Israeli government is in the process of dissolution as elections are to be held in March 2021. As such, most bills have been halted and it would be difficult to estimate how the new government will address these matters. We do expect, however, that any future amendment will be inclined towards GDPR-like standards, thus affecting digital advertising accordingly in terms of controller-processor liability, granularity of consent and notification, etc.

iab.

Japan

Cross-Jurisdiction Privacy Project

1. THE LAW

1.1. Overview, Key Acts, Regulations, and Directives

The principal data protection legislation in Japan is the Act on the Protection of Personal Information (Act No. 57 of May 30, 2003, as amended; "**APPI**"). The APPI provides the basic principles for the government's regulatory policies and authority, as well as the obligations of a "Business Operator Handling Personal Information (*Kojin Joho Toriatsukai Jigyosha*)" ("**Handling Operator**"), which means a person (corporate or otherwise) having a personal information database for use in business.

The Personal Information Protection Commission ("**PPC**") is the regulator primarily responsible for enforcing the APPI. For some industrial sectors, each ministry with jurisdiction over them has published data protection guidelines for those sectors.

The first significant amendment ("**2015 Amendment**") to the APPI came into full effect in May 2017. Further, the second significant amendment ("**2020 Amendment**") to the APPI was enacted in June 2020 based on its three-year review and will come into full effect in April 2022. This 2020 amendment will expand the scope of data subjects' rights, introduce mandatory data breach reporting, broaden extraterritorial enforcement options and impose stricter restrictions on cross-border transfers, while facilitating the use of pseudonymized data.

1.2. Guidelines

The PPC issued the guidelines ("**PPC Guidelines**") for the APPI.
The PPC Guidelines consist of the following four parts:

(a) general rules;
(b) transfers to a third party located in a foreign country;
(c) keeping records of providing or receiving personal information; and
(d) anonymously processed information.

Noncompliance with the provisions in the PPC Guidelines, which contain the term "must" or "required," may be deemed by the PPC as a violation of the APPI. On the other hand, noncompliance with the provisions which contain the term "preferable" or "desirable" is not generally deemed a violation of the APPI.

1.3. Case Law

The APPI does not provide a statutory right for individuals to receive compensation for noncompliance with the APPI. However, the protection of information regarding an individual's private life was established by case law, although there is no statute explicitly granting privacy rights. Therefore, an individual may file a lawsuit to claim compensation for damages for distress, based on tort or breach of contractual obligation

in accordance with the Civil Code. Despite the recognition of these torts, there is no relevant case law specifically related to digital advertising practices.

1.4. Application to Digital Advertising

The APPI applies to the handling of personal information by members of the digital advertising ecosystem, subject to issues of jurisdictional reach discussed below.

2. SCOPE OF APPLICATION

2.1. Who Do the Laws/Regulations Apply to and What Types of Processing Activities are Covered/Exempted?

As mentioned above, the APPI regulates a Handling Operator in the private sector, which means a legal or natural person having a personal information database for use in business. In contrast, organizations in the public sector are governed by other laws. For example, (a) the national government is governed by the Act on the Protection of Personal Information Held by Administrative Organs; (b) independent administrative agencies are governed by the Act on the Protection of Personal Information Held by Independent Administrative Agencies; and (c) local governments are governed by applicable local ordinances legislated by local governments.

The APPI applies to a Handling Operator in Japan, regardless of the location or nationality of data subjects.Furthermore, key provisions of the APPI apply to Handling Operators outside Japan if they receive personal information in connection with the provision of goods or services to individuals located in Japan (APPI, Article 75).

2.2. Jurisdictional Reach

As described in 2.1, the APPI has extra-territorial effect to the extent where the personal data relates to data subjects located in Japan.

2.3. Application to Digital Advertising

The APPI applies to the handling of personal information by members of the digital advertising ecosystem, subject to issues of jurisdictional reach discussed below.

Hypotheticals to test concerns/jurisdictional reach.

Scenario 1 (below) is the baseline scenario, where the user, publisher, and advertiser are all based in Japan and where it seems reasonable to assume the Privacy Law applies.

Scenarios 2, 3 and 4 vary the location of the user, publisher, and advertiser to test in each case the jurisdictional reach of the Privacy Laws.

For each scenario, we should ask how (if at all) does the Privacy Law apply to:

1. Serving the ad to the user.
2. Building a profile of the user.
3. The publisher's legal obligations.
4. The advertiser's legal obligations.

The application of the Privacy Laws to intermediaries has been deliberately omitted (this can be considered later if needed).

Scenario 1 (The baseline): A user residing in Japan (determined by IP address or geo identifier) goes onto a Japanese domain and is served an ad by a Japanese advertiser. The advertiser uses the user data to build a user profile.

The APPI would generally apply to the advertiser's activities and the publisher's activities because both the advertiser and publisher are considered to be Handling Operators in Japan.

Scenario 2 (User outside Japan): A Logged-on/signed-in user, known by the publisher to be a Japanese resident, goes onto a Japanese domain but the user's IP address or geo identifier indicates the user is outside Japan. A Japanese advertiser serves an ad and uses the user data to build a user profile.

The APPI would generally apply regardless of the location or nationality of data subjects because the publisher and advertiser are located in Japan.

- **Q1: Does the answer change if this is a signed-out user, with no way of knowing where they are domiciled?**

  No.

Scenario 3 (Publisher domain outside Japan): A user residing in Japan (determined by IP address or geo identifier) goes onto a domain outside of Japan. A Japanese advertiser serves an ad and uses the user data to build a user profile.

Advertiser: The APPI would apply to a Japanese advertiser.
Publisher: If a foreign publisher receives personal information in connection with the provision of goods or services to individuals located in Japan, then the APPI would apply extraterritorially to processing of such personal information by the foreign publisher.

- **Q1: Does the answer change if the site hosts content aimed at Japanese residents (e.g., a news aggregator with a section on Japanese current affairs)?**

  Yes. If the foreign site provides goods or services to individuals located in Japan and receives personal information in connection therewith, then the APPI would apply extraterritorially to processing of such personal information.

- **Q2: Does the answer change if the advertiser is based outside of Japan?**

  Yes. If the advertiser is based outside of Japan, the APPI would apply to such advertiser if it receives personal information in connection with the provision of goods or services to individuals located in Japan, regardless of whether the advertiser has affiliates located in Japan. In most cases, collection of personal information via digital advertising would be related to the provision of goods or services.

Scenario 4 (Advertiser outside Japan): A user residing in Japan (determined by IP address or geo identifier) goes onto a Japanese domain and is served an ad by an advertiser based outside Japan. The advertiser uses the user data to build a user profile.

Publisher: The APPI would apply to a Japanese publisher.
Advertiser: If a foreign advertiser receives personal information in connection with the provision of goods or services to individuals located in Japan, then the APPI would apply extraterritorially to processing of such personal information by the foreign advertiser. In most cases, collection of personal information via digital advertising would be related to the provision of goods or services.

- **Q1: Does the answer change if the advertiser has an affiliate/group company based in Japan?**

  No.

3. DEFINITIONS

3.1. Collect

No definition under the APPI.

- **When a publisher allows an ad tech company's pixel on its page, who is deemed to "collect" personal information and incur legal obligations (e.g., controller/co-controller obligations under GDPR or "business" obligations under CCPA) – the publisher, the ad tech company, or both?**

  Although there is no case law providing useful guidance on this issue, we believe that the ad tech company would be considered collecting personal information in this case. Further, the publisher may be considered to collect personal information as well if it gains access to such personal information. Please note, however, the APPI does not have the concepts of controller or co-controller.

3.2 Data Processing (i.e., collecting, capturing, retaining, recording, organizing, structuring, storing, altering, retrieving, consulting, using, disclosing, transmitting, disseminating, making available, aligning, combining, restricting, erasing, destroying, or otherwise processing)

Under the APPI, the term "handling" is comparable to the term "processing" in other jurisdictions. Although the APPI does not define "handling," it broadly covers any operation carried out with personal information, such as collection, using, distribution, storing, or otherwise processing.

3.3. Personal Information

"**Personal Information**" is defined as information about living individuals which falls under either of the following items (APPI, Article 2.1):

1) Information containing a name, date of birth, or other descriptions (i.e., any matter stated, recorded, or otherwise expressed) whereby a specific individual can be identified (including information which can be readily collated with other information and can thereby identify a specific individual).

2) Information containing an "**Individual Identification Code**," (e.g., biometric code, driver's license number) which means any character, number, symbol, or other code (a) into which a partial bodily feature of a specific individual has been converted by computers for use and which can identify that specific individual, or (b) which is assigned to services or goods provided to an individual, or is stated or electromagnetically recorded on a card or other documents issued to an individual, to identify him/her as a specific user, purchaser, or recipient of the issued document. The various types of Individual Identification Codes are listed in the Cabinet Order and include, among others, a driver's license number, passport number, and health insurance number (APPI, Article 2.2).

"**Personal Data**" means Personal Information contained in a Personal Information Database (APPI, Article 2.6).

"**Personal Information Database**" means a collection of information (which contains Personal Information) systematically organized to enable a computer or other method to search for particular Personal Information (APPI, Article 2.4).

Type of Information Collected	Does this Category Independently Constitute Personal Information? (Yes/No)	Qualifying Notes (if any)
IP Address	No.	
Mobile Advertising IDs (IDFA, AAID)	No.	
Consumer identifiers such as: • User device ID • Publisher persistent ID/Cross-publisher cookie ID • Household ID	No.	
Hashed identifiers such as: • Hashed email • Hashed IP address	No.	
User Agent such as: • Character string identifying the application • Operating system • Browser information, vendor, and/or version of the requesting user agent	No.	
Device Information such as: • Type, version, system settings, etc.	No.	

Website Information such as: • Name • URL, etc.	No.	
Advertisement Information such as: • Placement • Title • Creative ID, etc.	No.	
Timestamps	No.	
Metrics such as: • Counts • Amounts of time	No.	
Event Data such as: (e.g., full URL including query string, referral URL)	No.	
Precise geolocation (latitude, longitude)	No.	
General geolocation (city, state, country)	No.	

- **Are pseudonymous digital identifiers by *themselves* personal information (e.g., IDFA, cookie IDs, proprietary IDs, IP addresses, etc.)? Please provide context to the above chart.**

  No. Digital identifiers *per se* are not categorized as personal information.

- **If the answer to the above question is, "no," if a Company possesses a persistent digital identifier in Database 1 and has that same identifier in Database 2 with directly identifying information, does that render the pseudonymous information in Database 1 as personal information?**

  Yes. While digital identifiers per se are not categorized as personal information, they may constitute

personal information if they can be readily collated with other information and can thereby identify a specific individual. In the event where an entity possesses a persistent digital identifier in Database 1 and has that same identifier in Database 2 with directly identifying information, then the identifier in Database 1 would likely constitute personal information unless cross reference is strictly prohibited.

- **Is a Company's possession of a pseudonymous identifier plus other non-directly identifying data (e.g., age, gender, precise or imprecise geolocation, user agent string, timestamps) considered "personal information"?**

  Generally, no. A company's possession of a pseudonymous identifier plus other non-directly identifying data would not usually establish the identity of an individual unless there are exceptional circumstances where such combination leads to the identification of a specific individual.

- **Is a Company's possession of a pseudonymous identifier "personal information" if it can hire a service provider or otherwise engage in a transaction with a third party where the identifier *could* be matched to the person, *but* the Company chooses *not* to hire such service provider or undertake such transaction? Is the mere fact that this service is *potentially* available to match to the person sufficient to render that pseudonymous identifier as "personal information"?**

  Generally, no. If an engagement of a third-party service provider is required for matching persistent digital IDs (like a MAID) with other identifying information (like an email address), then it does not usually satisfy the requirement of 'can be readily collated with other information' and therefore MAIDs are not likely to constitute Personal Information unless the Company actually chooses to hire such service provider.

- **What level of geolocation is personal information (precise vs. approximate)? Does it need to be associated with an identifier to be considered PI?**

  There is no definition of what constitutes precise or imprecise geolocation. Location data (either precise or approximate) itself is not always considered Personal Information under the APPI. However, if it can identify a specific individual, then location data may be regarded as Personal Information. For example, in the context of location data collected by a smartphone application, it is argued that location data tends to make a specific individual identifiable especially in circumstances where it is continuously collected and stored for a long period of time or identifies a location as a workplace or home. Furthermore, if location data is linked or easily linkable to other information that leads to the identification of a specific individual, then it is subject to the APPI.

- **Is a household identifier personal information? (Consider: If a company has a residential IP address (household level ID) and multiple unique device IDs (e.g., MAIDs for every mobile device in the house) associated with that IP address, would that affect whether the household identifier is considered personal information?)**

Digital identifiers *per se* are not categorized as personal information unless they can be readily collated with other information and thereby identify a specific individual.

If a company has a residential IP address (household level ID) and multiple unique device IDs (e.g., MAIDs for every mobile device in the house) associated with that IP address and such unique device IDs are linked or easily linkable to other information that leads to the identification of specific individuals, then the household identifier is likely considered personal information.

- **Is a hashed identifier personal information? (Consider: there are commercially available services that will take batches of emails encrypted using standard hashes and return (often a high percentage) of clear emails from them. Does that affect whether they are considered personal information, if all a company has to do is pay for the commercial service?)**

  Hashed identifiers *per se* are not categorized as personal information unless the company has within its control other information from which it can be readily collated and thus identify a specific individual. The mere possibility that the company might (but does not) hire a service provider to unlock the identifier is not likely to render it personal information.

- **Is probabilistic information considered personal information?**

  Probabilistic information *per se* is not categorized as personal information unless they can be readily collated with other information and thereby identify a specific individual.

3.4. Sensitive Data

The APPI references "**Special Care-required Personal Information**" ('sensitive data'), which includes race, creed, social status, medical history, criminal history, and whether a person has been a victim of crime (See Article 2.3 of the APPI). The subordinate rules clarify that the following are also sensitive data: mental and physical disabilities; results of medical checks; medical advice, diagnosis or dispensing of pharmaceuticals by doctors further to medical checks; criminal procedures conducted against an individual; and juvenile delinquency cases against minors.

3.5. Pseudonymous Information

- **Is pseudonymous information considered personal information?**

  Pseudonymous information per se is not categorized as personal information unless the company has within its control other information from which it can be readily collated and thus identify a specific individual. The mere possibility that the company might (but does not) hire a service provider or otherwise obtain from a third party first party information that can be matched would not likely render it personal information. However, it may constitute personal information if it can be readily collated with other information and can thereby identify a specific individual.

The 2020 Amendment will introduce the term "**Pseudonymously Processed Information**," which is defined as personal information that can identify a specific individual only by collation with other information. Pseudonymous data can be Personal Information if it can be readily collated with other information and thereby identify a specific individual.

- **Does the law subject pseudonymous information to fewer obligations than "regular" personal information?**

  Yes. Even if Handling Operators handle Pseudonymously Processed Information which may constitute personal information, they will enjoy the following benefits under the 2020 Amendment:

  1) Internal utilization of Pseudonymously Processed Information will be permitted beyond the original purpose of use published or notified to data subjects.
  2) Exemptions from obligations with regard to data breach notification.
  3) Exemptions from complying with demands to disclose or cease the use of Personal Data.

3.6. Anonymized/De-identified Information

The concept of "**Anonymously Processed Information**" was introduced under the 2015 Amendment and is defined as information obtained by processing Personal Information such that ordinary people cannot (a) identify a specific data subject using the processed information or (b) restore any Personal Information from the processed information.

Anonymously Processed Information is not regarded as Personal Information. Thus, the regulations for personal information do not apply to Anonymously Processed Information, so long as a Handling Operator satisfies certain obligations applicable thereto.

- **Is there a difference between anonymized or de-identified data?**

  There is no concept of de-identified data under applicable law.

- **What common data categories are passed between publishers, advertisers, and ad tech companies that fall into this category when no persistent identifier is present (e.g., browser type, device type, operating system, app name, publisher site)?**

  Such information on its own may not be considered Personal Information, but when linked with information that could lead to the identification of the individual, it falls under the definition of Personal Information.

3.7. Data Controller

The APPI does not have the concepts of "Data Controller" and "Data Processor." Instead, there is only the concept of a "Handling Operator" which means a legal or natural person having a personal information database for use in business.

3.8. Joint Controller/Co-Controller

Please refer to our response in 3.6. The APPI does not have the concept of "Data Controller" and, thus, does not have a concept of "Joint Controller" or "Co-Controller."

3.9. Data Processor/Service Provider (i.e., an entity that is qualified as a processor or service provider under the law because it meets certain requirements and processes data pursuant to a permissible purpose on behalf of a controller/business)

Please refer to our response in 3.6. The APPI does not have the concept of "Data Processor," however, it does contemplate a contractual arrangement whereby a Handling Operator entrusts or consigns all or a part of the handling of personal data to a third party (please refer to Section 6).

3.10. Third Party (i.e., a third party that receives data from a business for non-business purposes and does not necessarily have specific requirements under the law as to such data, such as a third-party under the CCPA)

The APPI does not have a similar concept.

3.11 Other Definitions

3.11.1 Profiling

The APPI does not have a similar concept.

3.11.2 Automated Decision Making

The APPI does not have a similar concept.

3.11.3 Consent

Consent is not defined in the APPI. In general, consent means an indication of the individual's intention to consent to the handling of the individual's Personal Information in the manner indicated by a Handling Operator. In obtaining the consent of the individual, a reasonable and appropriate method must be used in accordance with the nature of the business and the circumstances in which the Personal Information is handled, which is considered necessary for the individual to make a decision regarding the consent. For details, please refer to our response in 4.4.

4. DATA CONTROLLER RIGHTS AND RESPONSIBILITIES

4.1. Overview

The APPI prohibits Handling Operators to obtain Personal Information through unfair methods such as fraud. Handling Operators are accountable for their handling of personal information, as well as the acts and practices of their employees and service providers. When handling Personal Information, Handling Operators must specify the purpose for which Personal Information will be used and must not use Personal Information beyond the scope necessary to achieve the Purpose of Use without obtaining the data subject's prior consent. There are several cases where Handling Operators must obtain an individual's prior consent, including (i) data sharing with or data transfer to other third parties (even within a group), (ii) obtaining sensitive information, (iii) cross-border data transfer, although there are some exceptions. Handling Operators are responsible for maintaining the security and safety of the personal information it holds.

4.2. Accountability

4.2.1. Overview

Handling Operators are accountable for their handling of personal information, as well as the acts and practices of their employees.

4.2.2. Application to Digital Advertising

Members of the digital advertising ecosystem subject to the APPI will therefore be held accountable for their handling of personal information, as well as the acts and practices of their employees.

4.3. Notice

When handling Personal Information, Handling Operators must specify the purpose for which Personal Information will be used (the "Purpose of Use") to the extent possible and must not use Personal Information beyond the scope necessary to achieve the Purpose of Use without obtaining the individual's prior consent (APPI, Articles 15,16).

4.3.1. Overview

- **Who must receive notice? When must notice be provided? What must be in the notice in the digital advertising context? (Consider also, what notice needs to be provided when pixels fire on a webpage?)**

  Once a Handling Operator has acquired Personal Information, it must promptly notify the individual/data subject of or publicly announce the Purpose of Use, except in cases where the Purpose of Use has already been publicly announced or where any of the following requirements are met:

  i. Where the notification or public announcement of the Purpose of Use is likely to cause harm to

the life, body, or property or to any rights or interests of an individual or a third party.

ii. Where the notification or public announcement of the Purpose of Use is likely to harm the rights or legitimate interests of the Handling Operator.

iii. Where cooperation with a state agency, local government, or a third party commissioned by a state or local agency is necessary to conduct certain affairs specified by laws and regulations and where the notification or public announcement of the Purpose of Use is likely to impede the execution of such affairs.

iv. Where the Purpose of Use is evident from the situation surrounding the collection of Personal Information (APPI, Articles 18.1, 18.4).

Practically, the Purpose(s) of Use are indicated in an online privacy policy of a Handling Operator. According to PPC Guidelines, online privacy policy is considered "publicly announced" when website visitors can access the policy, by clicking once or twice, from the top page of the Handling Operator's website.

- **Is there specific notice required for sensitive information?**

  As a general rule, Handling Operators must not obtain sensitive data without the individual's prior consent (APPI, Article 17.2).

- **Are there any specific requirements for providing notice related to processing children's personal information?**

  No. There are no specific requirements for providing notice related to processing children's personal information.

- **Are there any requirements compelling vendors directly collecting personal information or those receiving it from others personal information to provide additional notices? Who is responsible for those notices? Publishers? The vendors?**

  No. If a publisher allows an ad tech company to collect data on the publisher's website on behalf of the publisher, the ad tech company does not need to provide any separate notice from the privacy policy that would be on the publisher's website.

4.3.2. Application to Digital Advertising

- **Do third parties need to be named? For example, if a publisher gives privacy policy notice that it may share personal information with third parties for advertising purpose, does it have to specify which third parties? Do specific digital advertising activities or purposes need to be disclosed as well (e.g., TCF purposes)?**

  No. It is not legally required to name third parties in privacy policy/notice. However, it is practically advisable to specify the names of third parties if possible. It is not legally required to disclose "specific"

digital advertising activities or purposes under the current APPI; however, we anticipate that more granular disclosure will likely be required by the PPC Guidelines to be amended under the 2020 Amendment.

- **From an industry perspective it is common to distinguish data use for ad targeting vs. profile building vs. measuring ad campaigns. Does the notice requirement require separate disclosure of those things, or is it enough to say something general like "advertising and related purposes"?**

  Separate disclosure is not required under the current APPI. However, we anticipate that more granular disclosure will likely be required by the PPC Guidelines to be amended under the 2020 Amendment. The amended PPC Guidelines will be finalized later this year and likely reveal further details of matters to be notified by a Handling Operator.

4.4. Consent and Exceptions to Consent

4.4.1. Overview

- For what types of personal information or purposes of processing is consent required?

  For sensitive data only

  Acquisition: A Handling Operator shall not acquire sensitive data without obtaining the individual's prior consent, except in the following situations:

  (i) Based on laws and regulations.
  (ii) When it is necessary to protect a human life, body, or fortune but is difficult to obtain the individual's consent.
  (iii) When there is a special need to enhance public health or promote children's health but it is difficult to obtain the individual's consent.
  (iv) When there is a need to cooperate with state government offices, local public entities, or its trustees in the execution of their affairs as required by laws and regulations; however, obtaining the individual's consent may interfere with the execution of the aforementioned affairs.
  (v) When the special care-required personal information is publicly disclosed by the principal, state government offices, local public entities, entities specified in Article 76 (1) of the APPI, and other entities specified in the Personal Information Protection Guidelines.
  (vi) Other situations prescribed by cabinet orders as similar to those situations set forth in the preceding items.

  For Personal Data (including but not limited to sensitive data)

  Use of Personal Information within the original purpose of use: Consent is not necessary for utilizing Personal Information within the original Purpose of Use which was notified or publicly announced.

Use of Personal Information beyond the original purpose of use: A Handling Operator must obtain the individual's prior consent in utilizing Personal Information beyond the necessary scope to achieve the Purpose of Use. A Handling Operator shall not alter the Purpose of Use beyond the scope recognized as reasonably relevant to the pre-altered purpose for which it was collected (APPI, Article 15.2).

Provision to a third party: As a general rule, a Handling Operator shall not provide Personal Data to a third party without obtaining the individual's prior opt-in consent. Exceptions to the general rule include the following cases.

(i) Based on laws and regulations.
(ii) When it is necessary to protect a human life, body, or fortune but is difficult to obtain the individual's consent.
(iii) When there is a special need to enhance public health or promote children's health but it is difficult to obtain the individual's consent.
(iv) When there is a need to cooperate with state government offices, local public entities, or its trustees in the execution of their affairs as required by laws and regulations; however, obtaining the individual's consent may interfere with the execution of the aforementioned affairs.

Also, there are some other exceptions, under which receiving parties will not be considered a "third party" therefore the individual's consent is not required to provide Personal Data to the receiving party. For instance, if a Handling Operator entrusts (i.e., consigns) all or part of the handling of Personal Data to another party on a contractual basis, such party will not be considered a "third party." See Section 6.2 for data processing agreements.

Provision to a third party outside Japan: In principle, the APPI restricts the provision of Personal Data to third parties in a foreign country without the relevant individual's prior consent. Exceptions to the restriction include the items stated in (i)-(iv) above and the following:

- With respect to a third party that is a recipient of Personal Data, the prior consent requirement does not apply to the transfer of Personal Data to such recipients with a management system conforming to the standards set out in the PPC rules. The PPC rules currently provide two categories of exempt recipient operators:
    - A recipient operator, together with another operator that is the transferor of personal data to such recipient operator, ensures the recipient operator's compliance with relevant provisions of the APPI by taking appropriate and reasonable measures (such as maintaining a group company rules or executing a data handling agreement) with respect to the handling of personal information at the recipient operator.

- A recipient operator that has obtained recognition based on an international framework concerning the handling of personal information (e.g., recognition by the APEC Cross-Border Privacy Rules).

- With respect to a foreign country where a recipient is located, the prior consent requirement does not apply to countries that are specified in the PPC rules as having a system for the protection of personal information equivalent to that required under Japanese law. The EU and UK have been designated by the PPC as exempted regions as of January 2021.

See the response to two questions below for the notice requirements concerning the cross-border transfer.

- **How is valid consent manifested – express consent, opt-in, implied consent, or opt-out?**
"Consent of the individual" means an indication of the individual's intention to consent to the handling of the individual's Personal Information in the manner indicated by a Handling Operator. In obtaining the consent of the individual, a reasonable and appropriate method must be used in accordance with the nature of the business and the circumstances in which the Personal Information is handled, which is considered necessary for the individual to make a decision regarding the consent. Although implied consent is not prohibited, the PPC Guidelines do not provide specific standards as to what circumstances implied consent is permitted.

- **Is specific notice required as part of the consent?**
For the consent regarding data transfer to a third party, the PPC Guidelines state that the individual need not be notified of the specific recipients of Personal Data, but it is desirable to indicate the scope and attributes of the assumed recipients.

  The 2020 Amendment introduced new obligations for Handling Operators to disclose the following matters to the relevant individuals when the Handling Operator intends to obtain consent from the relevant individuals to transfer Personal Data to a third party outside Japan:

  i. Name of the foreign country to which Personal Data will be transferred.
  ii. A summary of the legal system for the protection of personal information in such foreign country.
  iii. An outline of specific measures implemented to protect personal information which are being or will be taken by the receiving party.

- **Does the consent obligation require granularity (i.e., consent for distinct processing activities) similar to GDPR? Or is the consent obligation more generalized (e.g., requiring consumers to opt-in to "online behavioral advertising" more broadly, without having to consent to each constituent processing activity/ party)? Is consent different for different uses or types of data (e.g., sensitive data, profiling, automated decision making, etc.) Please provide details.**

The consent obligation under the APPI is more generalized than that under GDPR. Therefore, consent for multiple advertising related purposes and can be bundled together, although sharing information will likely require separate consent.

- **Can personal information be processed for secondary purposes (i.e., differing purposes from which it was collected)?**

  Handling Operators must not use Personal Information beyond the scope necessary to achieve the Purpose of Use without obtaining the individual's prior consent (APPI, Article 16.1). A Handling Operator shall not alter the Purpose of Use beyond the scope recognized as reasonably relevant to the pre-altered purpose for which it was collected (APPI, Article 15.2).

- **Are there any rules compelling downstream recipients/processors of personal information to provide additional notices?**

  No.

- **Are there any issues concerning the timing of consent?**

  A Handling Operator must obtain the individual's PRIOR consent in utilizing Personal Information beyond the necessary scope to achieve the Purpose of Use or providing Personal Data to a third party.

  As described in Section 3.1, if a publisher allows an ad tech company's pixel on its page but the ad tech company (not the publisher) is considered as an entity collecting personal information, then consent is not required because there is no third-party data transfer.

- **Are there distinct consent requirements for sensitive personal information?**

  See above.

- **Are there distinct consent requirements for profiling consumers? If a business gets consent to use personal data for "advertising and marketing" purposes, is a separate (or more specific?) consent required to build an advertising profile for advertising?**

  No.

- **Are there distinct consent requirements for automated decision making?**

  No.

- **Are there any age restrictions related to consent? Are there distinct consent requirements around processing children's personal information?**

  The PPC Guidelines state that the specific age of children who need to obtain consent from their legal representatives, etc. should be determined on a case-by-case basis, depending on the items of personal

information to be covered, the nature of the business, etc., but, in general, it is considered necessary to obtain consent from legal representatives, etc. for children under the age of 12 to 15.

- **Can consent, however manifested, be revoked?**

  There is no APPI regulation regarding whether a data subject must be able to revoke or withdraw their consent. The APPI does not explicitly guarantee the right for data subjects to revoke or withdraw consent.

4.4.2. Application to Digital Advertising

It is possible a new regulation introduced by the 2020 Amendment will be applied to data collection for digital advertising purposes. The 2020 Amendment created a new category of information, called "Individual Related Information" (*kojin kanren jouhou*) which may include cookie information and location data. The 2020 Amendment regulates cases where a Handling Operator who has collected Individual Related Information aims to disclose such Information to a third party and such third party is expected to identify one or more specific individuals by using such Information; in such case, the receiving party would in general be required to obtain consent from the data subject and the providing party would be required to confirm whether such consent is obtained. Individual Related Information is defined as "information relating to a living individual, which does not qualify as Personal Information, Pseudonymously Processed Information, or Anonymously Processed Information."

4.5. Appropriate Purposes

4.5.1. Overview

A Handling Operator shall, in order to handle personal information, specify the Purpose of Use as much as possible. It is necessary to clarify in such a way that it is generally recognizable what kind of business the personal information is used for and for what purpose.

There is no need to list detailed and specific objectives, and some categorization is allowed.
However, the extent to which such information should actually be specified varies depending on the type and nature of the personal information, the type and nature of the Purpose of Use of the Personal Information, and the type and nature of the business Handling Operator handles the Personal Information.

4.5.2. Application to Digital Advertising

- **Does the law or legal guidance require a specific legal basis for specific digital advertising activities? Clarify for each activity (suggest using TCF/IAB CCPA "purposes") ("profiling" must be addressed here).**

  No. The Purpose of Use must be specified substantially, but there are no clear guidelines on the extent to which it should be specified. The PPC Guidelines state that statements such as "For use in marketing activities" are not specific enough.

  As for the data collection for digital advertising such as cookies and location data, please see 4.3.2 above.

- **If yes, what are the legal bases (e.g., consent, legitimate interest)? Are there any requirements related to lawful basis (need a valid legal basis to process)/fairness (scope of processing is fair)/transparency (transparent about the processing activity to the consumer and the lawful basis)?**

  N/A

- **Does the law address processing for secondary purposes/differing purposes from which it was collected?**

  A Handling Operator must obtain the individual's prior consent in utilizing Personal Information beyond the necessary scope to achieve the Purpose of Use.

4.6. Safeguards

4.6.1. Overview

Handling Operators are responsible to maintain security and safety of the personal information it holds, and exercise necessary and appropriate supervision over its employees handling the Personal Data, or any persons or entities delegated to handle Personal Data, to ensure they implement and comply with such security measures.

The PPC Guidelines illustrate high-level examples of security measures, which are categorized into:

- Establishing basic principles.
- Setting out internal rules.
- Organizational security measures (e.g., appointment of a responsible person, definition of each person's responsibility, definition of scope of data handled by each staff member, data processing operation and incident reporting line, definition of responsibilities between divisions, periodical internal and/or external audit, etc.).
- Staffing security measures (e.g., staff education and training, confidentiality provisions in work rules, etc.).
- Physical security measures (e.g., area access control (IC card, number keys), prevention of device theft, prevention of leakage from portable devices, non-recoverable deletion of data).
- Technological security measures (e.g., system access control, access authorization (user ID, password, IC card, etc.) control, prevention of unauthorized access (security software instalment and upgrading, encryption, access log monitoring), continuous review of system vulnerability, etc.).

4.6.2. Application to Digital Advertising

There are no specific safeguards for digital advertising. However, data including personal information will be frequently processed and transferred in the digital advertising industry, sufficient security measures should be taken to maintain secure management of personal data.

5. DATA SUBJECT RIGHTS/EXEMPTIONS

5.1. Overview

Data subjects have the right of access, right to rectification, right to erasure, and right to restriction of processing in accordance with requirements under the APPI. These rights may be legally enforced by court orders. However, the APPI requires a data subject to bring a request against a Handling Operator prior to filing a lawsuit. In that sense, the APPI encourages voluntary settlement between the parties to ease the excessive burden on Handling Operators to respond to lawsuits.

5.2. Access

Yes. Data subjects may request disclosure of the personal data and the purpose of use thereof (APPI, Articles 27 and 28). A Handling Operator must provide a copy of the personal data without delay and may charge a reasonable fee based on actual expenses. A data subject may file a lawsuit to enforce its rights if such a request is not responded to by the Handling Operator within two weeks of being made. The 2020 Amendment will allow data subjects to demand that their personal data be disclosed to them electronically.

A Handling Operator may refuse to provide access if:

(a) There is a possibility of harming the data subject or a third party's life, body, property, or other rights and interests.
(b) Disclosure could materially interfere with the Handling Operator's business.
(c) If disclosure would violate other laws and regulations (APPI, Article 28.2).

5.3. Rectify

Yes. Data subjects may request correction of or addition to personal data which is factually inaccurate (APPI, Article 29).

5.4. Deletion/Erasure

Yes. Data subjects may request deletion of personal data which is factually inaccurate (APPI, Article 29). Data subjects may also demand deletion of personal data if processing exceeds the purpose of use notified to the data subject, or the Handling Operator obtained the personal data using fraudulent measures (APPI, Article 30).

5.5. Restriction on Processing

Yes. Data subject may demand cessation of use of personal data if processing exceeds the purpose of use notified to the data subject, or the Handling Operator obtained the personal data using fraudulent measures. Data subjects may also demand cessation of provision of personal data to a third party if the Handling Operator transfers the personal data to the third party in violation of the APPI (APPI, Article 30).

The 2020 Amendment will expand the scope of the above rights. Data subjects will be able to exercise their rights, in addition to cases under the current law, if:

- The Handling Operator no longer needs to process the personal data.
- There was a serious data breach.
- Their rights or legitimate interests are likely to be infringed.

5.6. Data Portability

No.

5.7. Right to Object

No.

5.8. Right Against Automated Decision-Making

No.

5.9. Responding to Consumer Rights Requests

There is no specific timeline or format provided by the APPI, although a Handling Operator shall comply with a legitimate request without delay. A data subject may file a lawsuit to enforce its rights if such a request is not responded to by the Handling Operator within two weeks of being made.

5.10. Record Keeping Concerning Rights Requests

No.

5.11. Is Providing Consumers with These Rights Required by Law or Mere Suggestions?

It is not permitted to restrict the statutory data subject rights.

5.12. Application to Digital Advertising

If a member of the digital advertising ecosystem holds personal data, they may be required to deal with requests as described above.

Please note, however, that data subject rights apply only to "Retained Personal Data" that means personal data which a Handling Operator has the authority to disclose; correct, add to, or delete content from; discontinue use of; erase; or discontinue provision to a third party, at the request of the data subject. Thus, in the event where a Handling Operator entrusts (i.e., consigns) all or part of the handling of personal data to a service provider, the service provider is not usually required to deal with data subject requests because such personal data does not usually qualify as Retained Personal Data at least for the service provider. Rather, the controller should be the one to deal with data subject rights for such data entrusted to the service provider.

For example, if consumers exercise these rights to publishers, publisher's obligations do not generally flow to third parties to whom personal information has already been disclosed.

6. DATA CONTROLLER AND PROCESSOR AGREEMENTS

6.1. Overview

Please note that the APPI does not have the concepts of "Data Controller" and "Data Processor." Instead, there is only the concept of a "Handling Operator."

There is no statutory requirement to put in place written contracts with processors. However, if a Handling Operator entrusts or consigns all or a part of the handling of personal data to a third party, it must exercise necessary and appropriate supervision over that third party to have security control over the entrusted personal data. In that context, the PPC Guidelines require the Handling Operator to enter into contracts with processors, taking into consideration (a) the impact on data subjects' rights in the case of a security incident, and (b) the risks arising from the size and nature of the business and the personal data to be processed.

6.2. Data Controller Outsourcing of Processing

There is no statutory requirement to include specific terms in a data processing agreement, so long as a Handling Operator exercises necessary and appropriate supervision over the service provider processing personal data on its behalf.

That said, the PPC Guidelines state that it is desirable to include in a contract the Handling Operator's right to receive necessary information from the service provider to allow the Handling Operator to reasonably understand and evaluate how the service provider is processing the personal data.

6.3. Data Processor Rights and Responsibilities

Please refer to our response in 6.2.

6.4. Application to Digital Advertising

There is no special regulation related to digital advertising practices.

7. DATA TRANSFER & OUTSOURCING

7.1. Overview

The APPI requires the transferors of personal data to obtain the prior consent of the data subjects to transfer their personal information to a third party located in a foreign country, unless either of the exceptions below applies:

(a) The foreign country must be one designated by the PPC as a country having a data protection regime with a level of protection equivalent to that of Japan. Currently, the EU countries and the UK have been designated as such foreign countries.

(b) The recipient has a framework of data protection which meets either of the standards prescribed by the Enforcement Rules. The standards include:

1. The existence of appropriate and reasonable methodologies (such as contracts) through which the recipient will treat the personal information in accordance with the principles of the requirements for handling personal information under the APPI.
2. Obtaining a certification under an international arrangement, recognized by the PPC, regarding its framework of handling personal information (e.g., APEC CBPR System).

In addition to the existing restrictions on cross-border transfers, the 2020 Amendment will require a Handling Operator to inform data subjects of the details of a data transfer to a third party located in a foreign country.

- If a Handling Operator relies upon consent, it must inform the data subjects of certain information such as:
  - The name of the foreign countries where the data will be exported.
  - The data protection rules and regulations of the countries where the data will be exported.
  - The safeguards to be taken by the recipient to protect personal information.
- If a Handling Operator does not obtain consent and relies instead upon the fact that the third-party recipient has a system of data protection which meets the standards prescribed by the PPC rules, then it must do the following:
  - Take necessary actions to ensure that the overseas data transferee has in place continuous security measures to protect personal data.
  - Upon the request of data subjects, provide information regarding the system established by the recipient.

7.2. Application to Digital Advertising

There is no special regulation related to digital advertising practices.

8. AUDIT/ACCOUNTABILITY

8.1. Overview

- Audit - What audit rights are dictated by law (e.g., must companies have audit rights over their vendors? Does it matter what the classification of those vendors are?)

  Handling Operators must, in case of outsourcing a whole or a part of handling of Personal Data to others (such as vendors or independent contractors), exercise "necessary and appropriate" supervision over them, to ensure the security control over the Personal Data. As a part of such "necessary and appropriate" supervision, it is recommended by the APPI guideline to have periodical audit rights on the outsourced parties pursuant to the outsourcing agreement. APPI and relevant guidelines do not focus on the classification of vendors.

- Accountability - Must companies/vendors keep certain records to prove they have met certain requirements? What are those requirements?

  Handling Operators must keep a record of the provision of Personal Data to third parties including the following, subject to some exceptions:

  - The date of the provision of Personal Data.
  - The name of the third party or other information sufficient to identify such third party (if the Personal Data is provided to many and unspecified persons, such fact).
  - The data subject's name and other information sufficient to identify such data subject.
  - The categories of Personal Data.
  - The fact that the consent from the data subject has been obtained.

8.2. Application to Digital Advertising

There is no special regulation related to digital advertising practices.

9. DATA RETENTION

9.1. Overview

Handling Operators must endeavor to delete Personal Data without delay when its use is no longer required. There are no specific rules for the retention period.

9.2. Application to Digital Advertising

There is no special regulation related to digital advertising practices.

10. DATA PROTECTION AUTHORITY | REGULATORY AUTHORITY

10.1. Overview

Please refer to responses below.

10.2. Main regulator for data protection

Personal Information Protection Commission ("PPC") is the main independent regulator for data protection in Japan.

10.3. Main powers, Duties, and Responsibilities

PPC has a power to demand Handling Operators to report and to submit documents to PPC. Also, PPC personnel can enter Handling Operators' offices and other places, make inquiries, and examine relevant documents. PPC also has the power to make necessary recommendations, order, and advise to Handling Operators. The PPC Guidelines are issued by PPC (and jointly with government ministries, depending on the relevant industry sector).

10.4. Application to Digital Advertising

PPC is the main regulator for digital advertising business. In addition, METI (Ministry of Economy, Trade, and Industry) and Japan Fair Trade Commission (FTC) are also important regulators in connection with personal data to be processed by digital advertisers.

11. SANCTIONS

11.1. Overview

When a Handling Operator provides personal data to a third party, in principle, the consent of the person concerned is required in advance (APPI, Article 23). However, if the information provided is user information such as cookies that does not fall under "personal data," this provision does not apply. Therefore, when a Handling Operator provides user data that does not correspond to personal data to a third party, it is not necessary to obtain the consent of the data subject even if the provider knows in advance that the user data will be treated as personal data by collating with other information.

Recently, however, with the development and spread of technology that accumulates a large amount of user data

and instantly collates it into personal data, which is to provide non-personal information to third parties while knowing in advance that it will be personal data at the destination. Schemes to conceal the purpose of Article 23 of the APPI, which is to provide non-personal information to third parties while knowing in advance that it will be personal data at the destination, have been increasing and there are concerns about the spread of methods to collect personal information without personal involvement.

Under the 2020 Amendment, the new concept of "Individual Related Information" has been established, and regulations have been established regarding restrictions on third-party provision (Article 26), as further discussed below. This "Individual Related Information" refers to information about a living individual that does not fall under any of the categories of personal information, anonymously processed information or pseudonymously processed information and include Internet browsing history, location information, cookies, etc., that are not linked to names.

11.2. Liability

- **Scope of liability for publishers and advertisers for processing activities of ad tech companies:**

  The 2020 Amendment requires the discloser of data to confirm user consent for third party transfers if it is anticipated that the recipient may be able to identify an individual, even if the discloser cannot identify the individual.

  For example, if a publisher provides Individual Related Information to an ad tech company, then the publisher needs to confirm user consent only when it is anticipated that the ad tech company will then identify specific individuals by linking to other information.

- **Scope of liability for ad tech companies for collection activities of publishers and advertisers:**

  Under the 2020 Amendment, for example, if a publisher provides Individual Related Information to an ad tech company, then the ad tech company would in general be required to obtain consent from the data subject when it is anticipated that the ad tech company will then identify specific individuals by linking to other information.

- **Scope of liability for ad tech companies for other ad tech companies they enable to process data (either b/c they make the decision of publishers or advertisers, or agency dictates it):**

  Ad tech companies are not generally liable for processing by other ad tech companies.

11.3. Enforcement and Market Practice

- **How are claims raised under the law?**

  The APPI does not provide a statutory right for individuals to receive compensation for a Handling Operator's noncompliance with the APPI. However, the protection of information regarding an individual's private life was established by case law although there is no statute explicitly granting privacy rights. Therefore, an individual may file a lawsuit to claim

compensation for damages or distress, based on tort or breach of contractual obligation in accordance with the Civil Code.

- **Who enforces them?**

  Civil and criminal sanctions are enforced by courts.

  Administrative sanctions are enforced by the PPC, along with ministries for specific industries.

- **What is their practice (quietly working with companies to fix, publicly coming out with large investigations? Fact specific?)**

  Non-compliance may lead to the PPC rendering guidance/advice, recommendations to cease/correct violations and take certain necessary measures and investigate through audit. Criminal sanctions such as imprisonment and/or fines are also possible if the business misuses personal information for the purpose of unlawful gains, refuses to cooperate with an administrative investigation, or breaches an order issued as part of an administrative sanction.

- **What up to date guidance has there been on how to handle requirements in the ad ecosystem? Have the regulators been educated on how the ecosystem operates? Have compliance regimes been discussed with them? Has their feedback been solicited?**

  No specific guidance on cookies has been issued, nor is there any Japanese case law specifically addressing the use of cookies. The amended APPI however will regulate 3rd party transfers of data if it is anticipated that a recipient of the data may be able to identify an individual, which is expected to affect targeted advertising.

11.4. Remedies

Administrative Sanctions:

The PPC may take the following administrative sanctions when a Handling Operator does not comply with its obligations under the APPI:

1. The PPC may render guidance (*shido*) or advice (*jogen*) to the Handling Operator (Article 41).
2. The PPC may recommend (*kankoku*) that the Handling Operator cease the violation and take other necessary measures to correct the violation (Article 42.1).
3. The PPC may order the Handling Operator to take certain necessary measures (Article 42.2 and 42.3).

The APPI does not provide for administrative fines.

Criminal Sanctions:

The APPI provides for the following criminal penalties:

1. When a Handling Operator (if the Handling Operator is a legal entity, the representative or officer of the Handling Operator) or its employee provided or fraudulently used a Personal Information Database for the purpose of improper profits of itself or a third party, it may be subject to imprisonment of up to one year, or a fine of up to JPY 0.5 million (JPY 100 million in case of a legal entity).
2. Handling Operators which breach an order rendered by the PPC as administrative sanctions may be subject to a criminal sanction of imprisonment of up to 1 year or a fine of up to JPY 1 million (JPY 100 million in case of a legal entity).
3. Handling Operators which refuse to make a report or which makes a false report in response to a PPC investigation may be subject to a criminal sanction of a fine of up to JPY 0.5 million.

The criminal sanctions above may be imposed on the individual who committed the breach as well as the Handling Operators themselves.

Civil Sanctions:

The APPI does not provide a statutory right for individuals to receive compensation for noncompliance with the APPI. However, the protection of information regarding an individual's private life was established by case law although there is no statute explicitly granting privacy rights. Therefore, an individual may file a lawsuit to claim compensation for damages or distress, based on tort or breach of contractual obligation in accordance with the Civil Code.

The damages that may be awarded to a data subject are usually based on compensation for "mental damages" (i.e., consolation money) because there are usually no concrete economic damages which a data subject may incur. As for mental damages, there is no requirement to prove actual damages. In past judicial precedents, the awarded damages generally ranged from several thousands to several tens of thousands Japanese yen per individual.

11.5. Private Right of Action

The APPI does not provide a statutory right for individuals to receive compensation for noncompliance with the APPI. However, the protection of information regarding an individual's private life was established by case law although there is no statute explicitly granting privacy rights. Therefore, an individual may file a lawsuit to claim compensation for damages or distress, based on tort or breach of contractual obligation in accordance with the Civil Code.

11.6. Digital Advertising Liability Issues

The above liability applies similarly to the digital advertising ecosystem and there are no specific liability issues and exemptions unique to digital advertising.

11.7. Application to Digital Advertising

The above sanctions apply similarly to the digital advertising ecosystem and there are no specific liability issues and exemptions unique to digital advertising.

12. NOTIFICATION | CERTIFICATION | REGISTRATION

12.1. Overview

There is no general requirement that a Handling Operator be registered under the APPI or related regulations. A Handling Operator which wishes to use an Opt-Out for disclosure of Personal Data to a third party must file the opt-out provision prescribed in the order described below in section 6 under 'transfers pursuant to an Opt-Out' (but not the rest of its privacy policies) with the PPC. The PPC will then review the provision to ensure it is appropriate in accordance with the requirements of the APPI and make it available to the public. If the opt-out is not sufficient in terms of clarity, easy-readability, and formality, the PPC may require it to be improved and re-filed.

12.2. Requirements and Brief Description

There is no general requirement that a Handling Operator be registered under the APPI or related regulations.

12.3. Application to Digital Advertising

There is no general requirement that a Handling Operator be registered under the APPI or related regulations.

13. DATA PROTECTION OFFICER

13.1. Overview

The APPI does not specifically require a Handling Operator to appoint a data protection or similar officer. However, the General Guidelines provide that a Handling Operator must take security measures for the handling of Personal Information, an example of such a security measure being 'appointment of a person in charge of the handling of Personal Information and the definition of the responsibilities of the person'. The guidelines state that whether measures should be taken depends on the materiality of the damage which may be suffered by data subjects in the event of a data leakage, the size and nature of the business, and the general nature of the data handling (including the nature and volume of data handled). Some industry-sector guidelines also provide such requirements.

13.2. DPO – Compulsory Appointment (No)

A Handling Operator has no legal obligation to appoint a data protection or similar officer although a Handling Operator must take security measures for the handling of Personal Information. Certain private organizations or associations have created qualifications as 'data protection officer' or equivalent, and issue them to persons who have passed examinations set by them (e.g., Japan Consumer Credit Association issues a Personal Information Handling Officer qualification, and the Information-Technology Promotion Agency issues an Information Systems Security Administrator qualification). These qualifications are not acknowledged, supported, or required by law, but are industry-driven efforts to enhance data privacy.

13.3. Requirements

Since a Handling Operator has no legal obligation to appoint a DPO, there are no statutory requirements (such as location requirements) for the DPO.

13.4. Application to Digital Advertising

A Handling Operator has no legal obligation to appoint a DPO.

14. SELF-REGULATION

14.1. Overview

- **Are there any industry-self regulatory schemes in place in the jurisdiction?**

  Japan Interactive Advertising Association ("JIAA"): In 2017, JIAA partnered with IAB and became the 43rd national IAB licensee and is now also known as IAB Japan.

- **Are there any signal-based programs used in the territory to assist with digital advertising compliance?**

  No.

14.2. Application to Digital Advertising

There is no special regulation related to digital advertising practices.

15. PENDING PRIVACY BILLS

15.1. Overview

As described above, the current APPI regulates a Handling Operator in the private sector. In contrast, organizations in the public sector are governed by other laws. For example, (a) the national government is governed by the Act on the Protection of Personal Information Held by Administrative Organs; (b) independent administrative agencies are governed by the Act on the Protection of Personal Information Held by Independent Administrative Agencies;

and (c) local governments are governed by applicable local ordinances legislated by local governments.

In May 2021, a bill implementing the amendments necessary to integrate these public data protection laws into the APPI was enacted but has not come into force yet. These amendments will uniform administration of national data protection regulations.

15.2. Application to Digital Advertising

The bill to amend the APPI as described in 15.1 will not have impact for members of the digital advertising ecosystem.


iab.
Mexico
Cross-Jurisdiction
Privacy Project
Mexico

1. THE LAW

1.1. Overview & Key Acts, Regulations, and Directives

Like most data protection regimes, the laws in Mexico generally require: (i) the protection of individual data subject's personal data; (ii) complying with specific principles and duties when processing personal data; (iii) providing notice to and getting consent from data subjects regarding certain data collection practices in certain circumstances; and (iv) notifying data subjects of certain data breaches or data incidents.

1.2. Key Acts, Regulations, and Directives

In Mexico, data protection is a fundamental right protected by the Constitution. Furthermore, the data protection laws that are particularly relevant for digital advertising include:

i. The *Ley Federal de Protección de Datos Personales en Posesión de los Particulares* (Federal Law on Protection of Personal Data Held by Private Parties or the "DP Law"); the DP Law's Regulations (the "DP Regulations") and the *Lineamientos del Aviso de Privacidad* (privacy notice Guidelines, the "PN Guidelines" and jointly with the DP Law and DP Regulations, the "Mexican DPL"); and

ii. In connection specifically to the protection of consumer's privacy, the *Ley Federal de Protección al Consumidor* (Federal consumers Protection Law or "LFPC") and its Regulations (the "LFPC Regulations" and together with the LFPC, the "Consumer Protection Laws."

In addition, in 2017, Mexico passed the *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados* (General Law on Protection of Personal Data Held by Responsible Parties or the "General Data Protection Law") to regulate the processing of Personal Data by any governmental authority, entity, body and agency of the executive, legislative and judicial powers, autonomous bodies, political parties, trusts and public funds, unions and any other natural or legal person that receives and exercises public resources. However, this overview is only focused on the ones above we have identified as applicable to the private sector.

1.3. Guidelines

The PN Guidelines, which are binding and mandatory for "Controllers" (defined below), were published by the Ministry of Economy on January 17, 2013 and detail further the requirements regarding the content and scope for all privacy notices.

Moreover, the Mexican data protection authority, the National Institute for Transparency, Access to Information and Protection of Personal Data (*Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*) (the "INAI" for its acronym in Spanish), issued several non-binding guidelines and recommendations on subjects such as self-regulation schemes, minimum criteria for the contracting of cloud computing services for the processing of Personal Data, recommendations for handling Personal Data security incidents, for the processing of biometric data, code of good practices to guide the online processing of Personal Data of minors, guidelines for the preparation of privacy impact assessments, amongst others.

1.4. Case Law

Mexico is a civil law country; therefore, codified statutes predominate. Notwithstanding the foregoing, there is jurisprudence and isolated resolutions called (isolated thesis) issued by Mexican tribunals regarding privacy issues, particularly in connection with procedural and constitutional issues, but none really relevant to digital advertising.

1.5. Application to Digital Advertising

Digital advertising is regulated as any other type of advertising, per the Consumer Protection Laws and the Mexican DPL, as described above. There are no relevant signal-based programs used in the territory to assist with digital advertising compliance.

2. SCOPE OF APPLICATION

2.1. Who Do the Laws/Regulations Apply to and What Types of Processing Activities are Covered/Exempted?

The Mexican DPL applies to (i) private individuals or corporations that process Personal Data, which are considered as "Controllers" under the law, i.e., the individual or company who decides on the processing of Personal Data ("Controllers"); and (ii) their "Processors", which are the individuals or entities, independent of the organization of Controller, who shall process Personal Data on behalf of the Controller as a result of a legal relationship which defines the scope of the services to be provided by the Processor ("Processors").

The Mexican DPL protects all individuals to "whom the Personal Data corresponds" ("Data Subjects") (the law fails to state so, but most practitioners believe that the individual needs to be physically present in the territory). Personal Data is defined as all information related to an identified or identifiable individual ("Personal Data").

The Mexican DPL has the following broad exceptions:

- The Mexican DPL is not applicable to credit information companies and persons who collect and store Personal Data for personal use, with non-disclosure and non-commercial purposes.
- The Mexican DPL is not applicable to information of individuals acting as merchants or professionals.
- The Mexican DPL is not applicable to information related to individuals who provide services for entities or individuals engaged in business activities and/or in the provision of services consisting only of their first names and last names, job title, physical address, electronic address, telephone and fax numbers. The foregoing provided that such data is indeed used for purposes of representing his/her employer/contractor.
- DP Law states that its principles and obligations are limited by the protection of national security, order, public security and safety, as well as the rights of third parties.

DP Regulations further state that its provisions (i) will be applicable to the processing of Personal Data on physical or electronic media, which make it possible to access Personal Data in accordance with specific criteria,

regardless of the form or modality of its creation, type of support, processing, storage and organization; and (ii) will not be applicable when disproportionate periods or activities are required to access the Personal Data.

The Consumer Protection Laws apply to (i) "suppliers", a term defined as any individual or legal entity (as such legal figures are defined in the Mexican Civil Code), that regularly or periodically, offers, distributes, sells, grants the use or enjoyment or rents any goods, products or services; and (ii) "consumers", a term defined as the physical or moral person who acquires, carries out or enjoys goods, products or services as the final beneficiary. Micro-companies or members of micro-industries (as defined per the applicable laws) may be consumers under the LFPC if they acquire, store, use or consume goods or services with a purpose to integrate them into any process of production, transformation, marketing, or the provision of services to third parties. In this second case, the LFPC only grants the micro-companies or members of micro-industries the possibility of exercising certain rights set forth in such law.

The Consumer Protection Laws regulate the use of Personal Data for marketing purposes and include certain rights for consumers in connection with the use of their data for marketing purposes and obligations for suppliers in connection to the use of such data and limitations thereof.

2.2. Jurisdictional Reach

The Mexican DPL has an extraterritorial application in very limited cases; this means that it is not applicable to Controllers that process Personal Data outside of the Mexican territory, except in the events set forth in article 4 of the DP Regulations, which states that the Mexican DPL applies to Personal Data processing when:

i. It is carried out in an establishment of the Controller located in Mexican territory.
ii. It is carried out by a Processor, regardless of the Processor's location, if the processing is performed on behalf of a Mexican Controller.
iii. Mexican law is applicable as a consequence of international law or of the execution of a contract, even if the Controller is not located in Mexico.
iv. The Controller is not located in Mexican territory but uses means/resources located in Mexico to process Personal Data (e.g., if the advertiser's server was located in Mexican territory), unless such means are used exclusively for transit purposes.

It is also relevant to mention that under a strict interpretation of the LFPC, if a supplier sells products or provides services to Mexican consumers or a foreign advertiser displays ads on a Mexican domain, then the applicability of the LFPC is triggered as to the supplier and the foreign advertiser, since it is a public order law and it expressly states that all suppliers and consumers are obliged to comply with such law. Furthermore, considering that the definition of individual and legal entity in the Mexican Civil Code includes foreign individuals and legal entities, it could be construed that they could also be considered as supplier if they carry out the above-mentioned activities in the Mexican territory.

2.2.1 Application to Digital Advertising

Scenario 1 (below) is the baseline scenario, where the user, publisher and advertiser are all based in Mexico and where it seems reasonable to assume the Privacy Law applies.

Scenarios 2, 3 and 4 vary the location of the user, publisher, and advertiser to test in each case the jurisdictional reach of the Privacy Laws.

For each scenario, we should ask how (if at all) does the Privacy Law apply to:

1. **Serving the ad to the user.**
2. **Building a profile of the user.**
3 **The publisher's legal obligations.**
4. **The advertiser's legal obligations.**

NB. The application of the Privacy Laws to intermediaries has been deliberately omitted (this can be considered later if needed).

Scenario 1 (The baseline): A user residing in Mexico (determined by IP address or geo identifier) goes onto a Mexican domain and is served an ad by a Mexican advertiser. The advertiser uses the user data to build a user profile.

In this scenario, the Mexican DPL would be applicable when the procedure of serving the ad by the Mexican advertisers to users is based on processing of their Personal Data and when advertiser uses the user data to build a user profile, if such data should be considered as data of an identified or an identifiable individual. The Mexican DPL would also be applicable if a Mexican publisher uses this Personal Data to build a user profile if such data should be considered as data of an identified or an identifiable individual.

Scenario 2 (User outside Mexico): A Logged-on/signed-in user, known by the publisher to be a Mexican resident, goes onto a Mexican domain but the user's IP address or geo identifier indicates the user is outside Mexico. A Mexican advertiser serves an ad and uses the user data to build a user profile.

In this scenario, the Mexican DPL would be applicable when the procedure of serving the ad by the Mexican advertisers to users is based on processing of their Personal Data and when advertiser uses the user data to build a user profile, if such data should be considered as data of an identified or an identifiable individual. The Mexican DPL would also be applicable if a Mexican publisher uses this Personal Data to build a user profile if such data should be considered as data of an identified or an identifiable individual.

- **Q1: Does the answer change if this is a signed-out user, with no way of knowing where they are domiciled?**

  No.

Scenario 3 (Publisher domain outside Mexico): A user residing in Mexico (determined by IP address or geo identifier) goes onto a domain outside of Mexico. A Mexican advertiser serves an ad and uses the user data to build a user profile.

In this scenario, the Mexican DPL would be applicable when the procedure of serving the ad by the Mexican advertisers to users is based on processing of their Personal Data and when advertiser uses the user data to build a user profile, if such data should be considered as data of an identified or an identifiable individual.

The Mexican DPL would also be applicable if a Mexican publisher uses this Personal Data to build a user profile, if such data should be considered as data of an identified or an identifiable individual.

Mexican DPL would not be applicable for publishers outside of Mexico unless they use means/resources located in Mexican territory to process the Personal Data, or if any of the other exceptions where the Mexican DPL has an extraterritorial application (please refer to Section 2.2.).

- **Q1: Does the answer change if the site hosts content aimed at Mexican residents (e.g., a news aggregator with a section on Mexican current affairs)?**

  No.

- **Q2: Does the answer change if the advertiser is based outside of Mexico?**

  Yes. In this case the Mexican DPL would not be applicable to the advertiser, unless the advertiser uses means/resources located in Mexican territory to process the Personal Data, or if any of the other exceptions where the Mexican DPL has an extraterritorial application (please refer to Section 2.2.).

Scenario 4 (Advertiser outside Mexico): A user residing in Mexico (determined by IP address or geo identifier) goes onto a Mexican domain and is served an ad by an advertiser based outside Mexico. The advertiser uses the user data to build a user profile.

In this scenario, the Mexican DPL would have an extraterritorial applicability only if the advertiser located outside the Mexican territory is using means/resources located in Mexico, to process the applicable Personal Data, unless such means are used exclusively for transit purposes (e.g., if the advertiser's server was located in Mexican territory).

- **Q1: Does the answer change if the advertiser has an affiliate/group company based in Mexico?**

  In such a scenario, the Mexican DPL could be applicable if the affiliate/group company based in Mexico processes the user's Personal Data.

3. DEFINITIONS

3.1. Collect

This term is not defined in the Mexican DPL.

- **"When a publisher allows an ad tech company's pixel on its page, who is deemed to "collect" personal information and incur legal obligations (e.g., Controller/co-Controller obligations under GDPR or "business" obligations under CCPA) – the publisher, the ad tech company or both?"**

The Mexican DPL does not consider co-Controller obligations.

The Mexican ad tech company would be considered a Controller under the Mexican DPL, if it processes data of an identified or identifiable individual through the pixel.

The Mexican DPL does not regulate expressly if the Mexican publisher in this scenario would be considered as a Controller and the INAI has not issued any recommendation regarding this topic, so there is a lack of legal clarity. Furthermore, privacy experts in Mexico differ on how this scenario should be interpreted under the Mexican DPL.

Based on (i) the fact that the INAI has taken European resolutions as an example for their own resolutions; and (ii) the definition of Controller (please refer to section 3.6), some consider that it could be interpreted that the Mexican publisher would indeed be considered as a Controller in this scenario, since the publisher decided indirectly how the Personal Data would be processed, by allowing the ad tech company's pixel, if such the latter processes data of an identified or identifiable individual through the pixel.

Others are of the opinion that a Mexican publisher would not be a Controller in this scenario, provided it ensures that the page's users are informed that the ad publisher will be the one that processes their Personal Data collected through automated means (including pixels and/or cookies).

3.2. Data Processing (i.e., collecting, capturing, retaining, recording, organizing, structuring, storing, altering, retrieving, consulting, using, disclosing, transmitting, disseminating, making available, aligning, combining, restricting, erasing, destroying, or otherwise processing)

Under the Mexican DPL, data processing shall be understood as the obtention, use, disclosure, or storage of Personal Data by any means. Furthermore, the term "use" includes any action of access, management, exploitation, transfer, and/or disposal of Personal Data.

DP Regulations further state that such instrument will be applicable to the processing of Personal Data on physical

or electronic media, which make it possible to access Personal Data according to certain criteria, regardless of the form or modality of its creation, type of support, processing, storage, and organization.

3.3. Personal Information

The Mexican DPL defines the term "Personal Data," not "Personal Information." Personal Data is defined as: "information concerning an identified or identifiable natural person." DP Regulations further state that Personal Data may be expressed in numerical, alphabetical, graphic, photographic, acoustic, or any other type.

DP Regulations define an identifiable natural person as "a person whose identity can be determined, direct or indirectly, by any information," but states that if a Controller requires disproportionate "periods of time" or activities to identify an individual, such individual will not be considered as an identifiable natural person.

Considering the way "identifiable natural person" is defined, it could be interpreted that, if any person could identify the Data Subject through the Personal Data processed by the Controller (even when the Controller cannot or does not), then such information would be considered Personal Data. The foregoing is consistent with the analysis of such term in the "Data Protection Dictionary" recently published by the INAI but drafted by authors that are unrelated to such organism, which is not considered as a recommendation by the INAI but provides an indication of INAI's interpretations of the terms defined therein (the "Data Protection Dictionary").

The Mexican DPL does not define what constitutes disproportionate terms or activities to identify an individual, but the Data Protection Dictionary states, making reference to European standards, that "disproportionate terms or activities," should consider all objective factors such as costs and time required for the identification, depending on available technology and technological advances.

Type of Information Collected	Does this Category **Independently** Constitute Personal Information? (Yes/No)	Qualifying Notes (if any)
IP Address	No	There is no definition in the Mexican DPL for this term nor the INAI has issued any information thereof. However, if the IP Address can be traced back to an identified or identifiable user, it would be considered as Personal Data.

Mobile Advertising IDs (IDFA, AAID)	No	There is no definition in the Mexican DPL for this term nor the INAI has issued any information thereof. However, if the Mobile Advertising IDs can be traced back to an identified or identifiable user, it would be considered as Personal Data.
Consumer identifiers such as: • User device ID • Publisher persistent ID/Cross-publisher cookie ID • Household ID	No	There is no definition in the Mexican DPL for this term nor the INAI has issued any information thereof. However, if the consumer identifier can be traced back to an identified or identifiable user, it would be considered as Personal Data.
Hashed identifiers such as: • Hashed email • Hashed IP address	No	There is no definition in the Mexican DPL for this term nor the INAI has issued any information thereof. However, if the hashed identifiers can be traced back to an identified or identifiable individual, it would be considered as Personal Data.
User Agent such as: • Character string identifying the application • Operating system • Browser information, vendor, and/or version of the requesting user agent	No	There is no definition in the Mexican DPL for this term nor the INAI has issued any information thereof. However, if the User Agent can be traced back to an identified or identifiable user, it would be considered as Personal Data.

Device Information such as: • Type, version, system settings, etc.	No	There is no definition in the Mexican DPL for this term nor the INAI has issued any information thereof. However, if the Device Information can be traced back to an identified or identifiable user, it would be considered as Personal Data.
Website Information such as: • Name • URL, etc.	No	There is no definition in the Mexican DPL for this term nor the INAI has issued any information thereof. However, if the Website Information can be traced back to an identified or identifiable user (which could be the case if the information is an individual's full name or a person's email address is visible in the URL), it would be considered as Personal Data.
Advertisement Information such as: • Placement • Title • Creative ID, etc.	No	There is no definition in the Mexican DPL for this term nor the INAI has issued any information thereof. However, if the Advertisement Information can be traced back to an identified or identifiable user, it would be considered as Personal Data.
Timestamps	No	There is no definition in the Mexican DPL for this term nor the INAI has issued any information thereof. However, if the Timestamp can be traced back to an identified or identifiable user, it would be considered as Personal Data.

Metrics such as: • Counts • Amounts of time	No	There is no definition in the Mexican DPL for this term nor the INAI has issued any information thereof. However, if the Metrics can be traced back to an identified or identifiable user, these would be considered as Personal Data.
Event Data such as: (e.g., full URL including query string, referral URL)	No	There is no definition in the Mexican DPL for this term nor the INAI has issued any information thereof. However, if the Event Data can be traced back to an identified or identifiable user (which could be the case for query strings), it would be considered as Personal Data.
Precise geolocation (latitude, longitude)	Yes	There is no definition in the Mexican DPL for this term nor the INAI has issued any information thereof. However, the precise geolocation would probably be able to be associated with an identified or identifiable individual.
General geolocation (city, state, country)	No	There is no definition in the Mexican DPL for this term nor the INAI has issued any information thereof. However, if the general geolocation can be traced back to an identified or identifiable user, it would be considered as Personal Data.

- **Are pseudonymous digital identifiers by themselves (e.g., IDFA, cookie IDs, proprietary IDs, IP addresses, etc.) considered personal information?**

  Cookies may not be personal information in and of themselves, but when cookies are used to store unique identifiers for the purpose of profiling a user, the information could become information about an identifiable individual. Other pseudonymous digital identifiers could be considered as Personal Data, if they are information related to an identifiable individual.

- **If the answer to the above question is, "no," if a Company possesses a persistent digital identifier in Database 1 and has that same identifier in Database 2 with directly identifying information, does that render the pseudonymous information in Database 1 as personal information?**

  Yes.

- **Is a Company's possession of a pseudonymous identifier plus other non-directly identifying data (e.g., age, gender, precise or imprecise geolocation, user agent string, timestamps) considered "personal information"?**

  No, unless the combination of the pseudonymous identifier plus the other non-directly identifying data can be associated with an identified or identifiable individual.

- **Is a Company's possession of a pseudonymous identifier "personal information" if it can hire a service provider or otherwise engage in a transaction with a third party where the identifier could be matched to the person but the Company chooses not to hire such service provider or undertake such transaction. Is the mere fact that this service is potentially available to match to the person sufficient to render that pseudonymous identifier as "personal information"?**

  Yes.

- **What level of geolocation is personal information (precise vs. approximate)? Does it need to be associated with an identifier to be considered PI?**

  This is not expressly regulated in the Mexican DPL, but any level of geolocation would be Personal Data if it can be associated to an identified or identifiable individual.

- **Is a household identifier personal information? (Consider: If a company has a residential IP address (household level ID) and multiple unique device IDs (e.g., MAIDs for every mobile device in the house) associated with that IP address, would that affect whether the household identifier is considered personal information?)**

  This is not expressly regulated in the Mexican DPL, but an identifier that connects to a specific household

would be deemed to be personal information if it can be associated to an identified or identifiable individual.

- **Is a hashed identifier personal information? (Consider: there are commercially available services that will take batches of emails encrypted using standard hashes and return (often a high percentage) of clear emails from them. Does that affect whether they are considered personal information, if all a company has to do is pay for the commercial service?)**

  Hashed identifiers can be personal information to the extent that they are about an identifiable individual. The mere act of hashing personal information may not—in and of itself—render him/her non-identifiable.

- **Is probabilistic information considered personal information?**

  If the probabilistic information refers to an identified or identifiable individual, it would be considered as Personal Data under the Mexican DPL.

3.4. Sensitive Data

Sensitive Personal Data ("Sensitive Data") is defined in the Mexican DPL as Personal Data that affects the most intimate sphere of a Data Subject's life, or information that could lead to discrimination, or entail a serious risk for a Data Subject if misused. The Mexican DPL states that data that may reveal personal aspects such as racial or ethnic origin, current or future state of health, genetic information, religious, philosophical, or moral beliefs, labor union membership, political opinions, and/or sexual orientation should be considered as Sensitive Data.

3.5. Anonymized/Deidentified/Pseudonymous Information

- The Mexican DPL fails to refer to pseudonymized or anonymized data. However, DP Law defines "dissociation" as the procedure by which Personal Data cannot be associated with the Data Subject or allow, due to its structure, content or degree of disaggregation, his/her identification. "Dissociated" Personal Data is still considered Personal Data under the law, but it can be used freely without consent of the Data Subject. The definition of the term "disassociation" is close to the anonymization definition under the GDPR, since the disassociation procedure should not allow the association of Personal Data with the Data Subject.
- **Is pseudonymous information considered personal information?**

  As mentioned before, pseudonymization is not regulated under the Mexican DPL, so pseudonymous information should be considered as Personal Data if the data may be re-identified with the Data Subject.
- **Are persistent digital identifiers pseudonymous information (e.g., IDFA, cookie IDs, proprietary IDs, IP addresses, etc.)?**

  As mentioned before, pseudonymization is not regulated under the Mexican DPL, so pseudonymous

information should be considered as Personal Data if the data may be re-identified with the Data Subject.

- **Does the law subject pseudonymous information to fewer obligations than "regular" personal information?**

  As mentioned before, pseudonymization is not regulated under the Mexican DPL, so pseudonymous information should be considered as Personal Data if the data may be re-identified with the Data Subject.

3.6. Controller and Processor

Pursuant to the Mexican DPL, Controller is defined as the individual or private entity who decides on the processing of Personal Data.

The Joint Controller/Co-Controller figure is not regulated under the Mexican DPL.

For the definition of Processor, please refer to Section 2.1.

Third Party (i.e., a third party that receives data from a business for non-business purposes and does not necessarily have specific requirements under the law as to such data, such as a third-party under the CCPA):

"Third party" is defined in the Mexican DPL as a Mexican or foreign individual or legal entity other than Data Subject, Controller, and Processor, depending on the context.

3.7. Other Definitions

Profiling:
This term is not defined in the Mexican DPL.

Automated Decision Making:
Automated Decision Making is not defined per se in the Mexican DPL, but it does state that, when Personal Data is processed as part of a decision-making process, without involving the assessment of an individual, the Controller must inform the Data Subject that this situation occurs. The Data Subjects may additionally also exercise their (i) right of access, in order to know the Personal Data that was used as part of the corresponding decision-making; and (ii) if applicable, the right to rectification, when the Data Subject considers that any of the Personal Data used was inaccurate or incomplete, so that, in accordance with the mechanisms that the Controllers has implemented for this purpose, he/she be able to request a reconsideration of the decision taken.

Consent:
Consent is defined as the manifestation of the will of the Data Subject of the Personal Data pursuant which the processing of such data is carried out.

4. DATA CONTROLLER RIGHTS AND RESPONSIBILITIES

4.1. Overview

Under the Mexican DPL, when processing Personal Data, all Controllers must abide by: (i) the principles of legality, consent, information, quality, purpose, loyalty, proportionality, and accountability; and (ii) the duties of confidentiality and security. Those principles and duties are the foundation of the Controller's main obligations under the law.

Principles

- *Legality*: Requires the Controllers to ensure that processing follows and complies with the provisions of Mexican and international law.
- *Consent*: The Controllers must obtain consent for the processing of Personal Data unless it is not required by law. Depending on the type of Personal Data to be processed, Data Subjects can provide such consent explicitly, verbally, in writing, electronically, or through any other technological means available, or tacitly, if the Data Subject has been provided of the applicable privacy notice and no opposition is expressed. In the case of Personal Data collected through the Internet for digital advertising, if no sensitive or financial Personal Data is processed by the applicable Controller, the Controller may rely on tacit consent and the Data Subjects could express his/her opposition through the mechanisms described in the privacy notice (which is information that must be included therein per law; please refer to Section 4.3.1.).
- *Information*: The Controllers must provide (*poner a dispocisión*) the applicable privacy notice to the Data Subject, which shall include specific information regarding the processing to which his or her Personal Data will be submitted to. The privacy notice must communicate any processing for marketing, advertising, or commercial exploration.
- *Quality*: The Personal Data collected and processed by the Controllers needs to be correct, relevant, and up to date, per the purposes for which it was collected. This principle also considers the obligation to block and delete the Personal Data when it is no longer necessary for the fulfillment of the purposes set forth in the privacy notice and the Mexican DPL (please refer to Section 9.1).
- *Purpose*: Personal Data may be processed only to comply with the purpose or purposes set forth in the applicable privacy notice, which shall distinguish between the purposes that are necessary to comply with the legal relationship between the Controller and the Data Subject (primary purposes) from those that are not (secondary purposes).

- *Loyalty*: The Controllers shall prioritize the protection of the interests of the Data Subjects and their reasonable expectation of privacy, during the processing of their Personal Data.
- *Proportionality*: The Controllers can only process Personal Data that are necessary, appropriate, and relevant in connection with the purposes for which they were obtained. This also refers to the reasonable efforts to limit the Personal Data to the minimum necessary regarding the purpose(s) set forth in the privacy notice.
- *Accountability*: The Controllers shall ensure compliance with the principles set forth in the Mexican DPL and shall protect and be responsible for the processing of the Personal Data that are in its custody or in its possession.

Duties

- *Confidentiality*: In any stage of the Personal Data processing, the Controllers shall maintain the confidentiality with respect to such data, and its obligations will continue after the end of the relationship with the Data Subject.
- *Security*: Establishing and keeping security, administrative, technical, and physical measures that allow the protection of the Personal Data from any harm, loss, alteration, destruction, or non-authorized processing and having a catalogue of such measures.

4.2. Accountability

4.2.1. Overview

Controllers are obligated to ensure the proper processing of the Personal Data in their possession and are accountable for the foregoing, including the processing carried out by its Processors. Controllers may use standards, best international practices, corporate policies, self-regulation arrangements, or any other adequate mechanism for such purpose.

The Controllers need to take all necessary measures that guarantee the proper processing of Personal Data, which include, among others, the following:

i. Implementing binding and enforceable privacy policies and programs, as well as sanctions for a breach thereof, assign resources for such implementation and periodically review such policies and programs.
ii. Establish procedures to receive and respond Data Subjects' inquiries and complaints.
iii. Implementing a training program regarding Personal Data protection for its personnel.
iv. Implementing a supervision/auditing system.
v. Designating a Data Protection Officer or Department.
vi. Implementing agreements or legal instruments with transferees or Processors.
vii. Establishing and keeping security, administrative, technical, and physical to protect the Personal Data

during the all the processing, including tracing the Personal Data while being processed.

4.2.2. Application to Digital Advertising

These requirements are applicable to any type of advertising, including digital advertising.

4.3. Notice

4.3.1. Overview

To comply with the above-mentioned Information (Notice) Principle, Controllers must have evidence that they provided a privacy notice to the Data Subjects, to inform them that Personal Data will be processed and the purposes of such processing, in addition to other specific information that needs to be included therein per the Mexican DPL.

- **Who must receive notice? When must notice be provided? What must be in the notice in the digital advertising context? (Consider also, what notice needs to be provided when pixels fire on a webpage?)**

Per the Mexican DPL, Controllers must communicate to Data Subjects the applicable privacy notice and, if required by law, obtain consent prior to the processing of their Personal Data. Under the Mexican DPL, privacy notices need to include, in general terms, the following:

- Identity and address of the Controller.
- Processed Personal Data, and if such data is considered as Sensitive Data.
- Primary purpose(s) and any secondary purposes (including direct marketing) for processing the Personal Data.
- Mechanism available so the Data Subject can indicate his/her objection to the processing of his/her Personal Data for secondary purposes (including digital advertising).
- The options and means to limit the use or disclosure of Personal Data offered to Data Subjects.
- The means available for Data Subjects to exercise the access, rectification, cancelation, or opposition rights and revoke his/her consent for the processing of their Personal Data.
- If Personal Data will be transferred, to whom, and for what purpose.
- If the Controller uses remote or local electronic, optical, or other technological means of communication mechanisms that allow Personal Data to be obtained automatically and simultaneously at the time the Data Subject has contact with the mechanisms (e.g., cookies, web beacons, and other tracking technologies), as well as the Personal Data collected by those mechanism and the purposes for processing such Personal Data.
- The procedure and means that will be used by the Controller to inform Data Subjects of changes in the privacy notice.

Considering that pixels are a mechanism that "allow Personal Data to be obtained automatically and simultaneously at the time the Data Subject has contact," the Controller must inform the Data Subjects about the use of this technology in its privacy notice. Furthermore, Controllers must immediately inform the Data Subjects, through a communication or warning placed in a visible place (e.g., a cookie banner or pop-up), the use of these technologies and the fact that Personal Data is obtained from them, as well as how they can be disabled (except if these technologies are necessary for technical purposes).

- **Is there specific notice required for sensitive information?**

No.

- **Are there any specific requirements for providing notice related to processing children's personal information?**

According to Mexico's Federal Civil Code, individuals under 18 years old must be represented by their parents or guardian (legal representatives), as they do not have the legal capacity to assume obligations (including, entering into agreements) or exercise their rights. If there is any processing of minors' Personal Data, then the Controller will need to provide to a parent/guardian the applicable privacy notice that informs the conditions for processing the Personal Data collected, plus obtain his/her consent, if so, required by law.

- **Are there any requirements compelling vendors directly collecting personal information or those receiving it from others personal information to provide additional notices? Who is responsible for those notices? Publishers? The vendors?**

The Controllers are always responsible for providing Data Subjects their privacy notice. So, if vendors are acting on behalf of publishers or any other Controllers, then vendors would not be responsible under the law for providing notice. If the vendors are Controllers, then they would be responsible for providing notice as to the Personal Data for which the vendors act as Controllers.

4.3.2. Application to Digital Advertising

- **Do third parties need to be named? For example, if a publisher gives privacy policy notice that it may share personal information with third parties for advertising purpose, does it have to specify which third parties? Do specific digital advertising activities or purposes need to be disclosed as well (e.g., TCF purposes)?**

The Mexican DPL makes a distinction, and regulates differently, disclosures of personal information by Controllers to Processors (defined as transmissions (remisiones) under the Mexican DPL) and those from Controllers to third parties (defined as transfers). When Controllers transfer Personal Data to third parties, they need to comply with specific requirements set forth in the Mexican DPL. All transfers need to be informed and, excluding certain exceptions listed in the Mexican DPL, consented per the applicable privacy notice. Transmissions from Controllers to Processors do not need to be notified to, nor consented by the Data Subjects.

All privacy notices need to state if the Controller intends to transfer any Personal Data to national or foreign third parties (identified by name or type, category, or sector of activity) and the use (purposes) that the latter shall give to such data. Furthermore, all transfers (national or international) are subject to the Data Subject's consent (depending on the type of data to be transferred, the consent needs to be tacit, express, or express and written).

Considering the real-time bidding current trends, supply-side platform (SSP) and demand-side platform (DSP) would probably be considered as Controllers and in such case, the transfer of Personal Data to such actors would need to be stated in the privacy notice per the terms mentioned in this document.

Please refer to Section 7.1, for more information in connection to national and international transfers.

- **From an industry perspective, it is common to distinguish data use for ad targeting vs. profile building vs. measuring ad campaigns. Does the notice requirement require separate disclosure of those things, or is it enough to say something general like "advertising and related purposes"?**

The Mexican DPL expressly states that the list of purposes described in the privacy notice must be (i) specific, i.e., when the privacy notice states clearly, without creating confusion and objectively for what purpose(s) the Personal Data will be processed and (ii) complete and abstain from using inaccurate, ambiguous, or vague phrases, such as "among other purposes," "other similar purposes," or "for example." Therefore, the privacy experts in Mexico prefer to be as specific as possible when describing the processing purposes in the privacy notices.

4.4. Consent and Exceptions to Consent

4.4.1. Overview

In Mexico, consent is the only lawful basis for processing Personal Data, with certain exceptions set forth by law.

- **For what types of personal information or purposes of processing is consent required?**

Consent is necessary to process any type of data, except in the following cases, amongst others: (i) when provided by law; (ii) when processing information that is publicly available; (iii) when the purpose of the Personal Data processing has the purpose to comply with obligations that arise from a legal relationship between the Data Subject and Controller; (iv) Personal Data is "dissociated"; (v) when it is essential for medical attention, prevention, diagnosis, health care delivery, medical treatment, or health services management when no consent can be given by the Data Subject, in the understanding that the processing of such Personal Data must be carried by a person subject to a duty of professional secrecy; or (vi) when a resolution is issued by a competent authority.

Even if a Controller does not require consent to process Personal Data, it must inform Data Subjects through its privacy notice the purpose(s) for acquiring and processing Personal Data.

- **How is valid consent manifested – express consent, opt-in, implied consent, or opt-out?**

The Mexican DPL considers and allows three types of consent:

a. Express Consent: required for the processing of (i) financial or property data or other data, if so, required by a different law, or (ii) is so required per an agreement between the Data Subject and the Controller; such consent is communicated by a Data Subject, in writing, by electronic or optical means or via any other technology or unmistakable indication.

b. Express and Written Consent: required for the processing of Sensitive Data and is granted through a handwritten, digital signature or other identification procedure.

c. Tacit Consent: required for processing of Personal Data other than Sensitive Data, financial, or property Personal Data and is considered to be granted if a Data Subject has been provided with the Controller's privacy notice and no opposition is expressed.

- **Is specific notice required as part of the consent?**

  Yes, notice should be provided through a privacy notice, which must comply with the requirements set forth in the Mexican DPL.

  Please note that Controllers must provide Data Subjects a new privacy notice, and obtain consent thereof if so required by law, if the Controller:

  a. Changes identity.

  b. Collects Sensitive Data, property, or financial data additional not included in the original privacy notice, if such data is not obtained personally or directly from the Data Subject and consent to process that information required by law.

  c. Changes the primary purposes included in the original privacy notice or new purposes are incorporated that require the consent of the Data Subject.

  d. Modifies the conditions of the transfers described in the original privacy notice or if new transfers will be carried out, if such transfers need to be consented per law.

- **Does the consent obligation require granularity (i.e., consent for distinct processing activities) similar to GDPR? Or is the consent obligation more generalized (e.g., requiring consumers to opt-in to "online behavioral advertising" more broadly, without having to consent to each constituent processing activity/ party)? Is consent different for different uses or types of data (e.g., sensitive data, profiling, automated decision making, etc.) Please provide details.**

Under the Mexican DPL, consent does not need to be granular; the foregoing, in the understanding, however, that the privacy notice needs to include all Personal Data the Controller will process and for which purposes. No Personal Data can be processed for any purpose not established in the privacy notice and all Data Subjects may revoke his/her consent at any time. Additionally, privacy notices must include the mechanisms available so the Data Subject can indicate his/her objection (opt-out) to the processing of his/her Personal Data for secondary purposes.

Finally, privacy notices need to include a clause in which the Data Subject consent the transfer of their Personal Data per the terms described in the document.

Consent is not different for different uses of Personal Data, but it is for different types of Personal Data, as mentioned previously.

- **Can personal information be processed for secondary purposes (i.e., differing purposes from which it was collected)?**

Yes, provided that the secondary purposes are described in the applicable privacy notice and an opt-out mechanism for such purposes is included therein.

- **Are there any rules compelling downstream recipients/Processors of personal information to provide additional notices?**

Depends on the relationship amongst the Controller and such other person processing the Personal Data. Processors do not need to provide additional notices, but national recipients (transferees) do.

- **Are there any issues concerning the timing of consent?**

Yes, as a general rule, consent must be given prior to processing Personal Data.

- **Are there distinct consent requirements for sensitive personal information?**

Consent must be express and written, i.e., granted through handwritten, digital signature, or other identification procedure.

- **Are there distinct consent requirements for profiling consumers? If a business gets consent to use Personal Data for "advertising and marketing" purposes, is a separate (or more specific) consent required to build an advertising profile for advertising?**

No distinct consent requirements for profiling consumers, provided that the purpose for which the profiling is carried out is described in the privacy notice. If the profiling is used exclusively for advertising purposes, then it would be covered under "advertising and marketing" purposes.

- **Are there distinct consent requirements for automated decision making?**

No, but the notice requirements mentioned in Section 3.7 need to be met.

- **Are there any age restrictions related to consent? Are there distinct consent requirements around processing children's personal information?**

Please refer to Section 4.3.1. There are no rules applicable specifically to Personal Data processing, however, the INAI has issued some recommendations on the processing of Personal Data for children and teenagers.

- **Can consent, however manifested, be revoked?**

Yes, the Data Subject has the right to revoke his/her consent, at any time. The procedure to revoke his/her consent must be established in the corresponding privacy notice.

4.5. Appropriate Purposes

4.5.1. Overview

In accordance with the Purpose Principle, Controllers and any third party who acts per its request or on its behalf, must only process Personal Data to comply with the purposes set forth in the privacy purpose, and those that are compatible or analogous.

4.5.2. Application to Digital Advertising

- **Does the law or legal guidance require a specific legal basis for specific digital advertising activities? Clarify for each activity (suggest using TCF/IAB CCPA "purposes") ("profiling" must be addressed here).**

Consent is the only legal basis for processing Personal Data per the Mexican DPL, with the exceptions set forth in the law, which conceptually do not consider marketing or advertising activities.

- **If yes, what are the legal bases (e.g., consent, legitimate interest)? Are there any requirements related to lawful basis (need a valid legal basis to process)/fairness (scope of processing is fair)/transparency (transparent about the processing activity to the consumer and the lawful basis)?**

In addition to obtaining consent for processing Personal Data for advertising activities, the Controllers must comply with the principles previously described.

Furthermore, suppliers under the LFPC must comply with the following requirements in connection to the use of Personal Data for advertising purposes:

- If so required by consumers: (i) to inform them, at no cost, the information the supplier has in its databases of such consumers and to whom that information has been transmitted; (ii) stop contacting them for marketing purposes and sending advertising; and (iii) stop transferring their information to third parties.
- Publicity sent to consumers by suppliers must include the name, address, telephone number, or alternatively email, of the supplier and the contact data of the *Procuraduría Federal del Consumidor* (Federal Consumer Protection Agency or "PROFECO").
- PROFECO administers the Public Consumer Registry (the "REPEP"), where consumers who do not want to receive publicity can register their phone number and, per a very recent legal reform to the LFPC Regulations that has yet to be implemented by PROFECO, their email. PROFECO provides suppliers access to this list. Per the LFPC, suppliers and marketing companies must not send advertising to persons that

have expressed that they do not want to receive publicity and those who are registered in the REPEP.

- Suppliers must avoid misleading advertising in publicity or any other misleading information in connection to their services, products, and/or goods.

- **Does the law address processing for secondary purposes/differing purposes from which it was collected?**

As mentioned before, privacy notices must distinguish between the primary purposes, which are necessary to comply with the legal relationship between the Controller and the Data Subject, from those that are not, which are considered as secondary purposes. Marketing purposes are indeed considered as secondary purposes under the Mexican DPL. Both primary and secondary purposes need to be informed to the Data Subject before the collection of their Personal Data.

If Controllers want to change the primary purposes included in the privacy notice or include new ones that require the consent of the Data Subject, the Controller must obtain the Data Subjects' consent thereto.

4.6. Safeguards

4.6.1. Overview

The Mexican DPL requires Controllers and Processors to establish and maintain administrative, physical and, if applicable, technical, security measures to protect Personal Data. Such security measures also mean security control or group of controls to protect Personal Data.

To determine the appropriate security measures for the protection of the Personal Data, the Controllers shall consider the following factors, as stated in the Mexican DPL:

- Inherent risks and the sensitivity of the Personal Data.
- Technological development.
- Possible consequences for Data Subjects in case of a violation to their rights.
- Amount of Data Subjects.
- Previous data breaches in their systems.
- Risks as a result of potential quantitative or qualitative value of the Personal Data, in case of unauthorized access or processing of the data.
- Other factors that might have an impact upon the level of risk or which result from other legislation applicable to the Controller.

4.6.2. Application to Digital Advertising

These requirements are applicable to any type of advertising.

5. DATA SUBJECT RIGHTS/EXEMPTIONS

5.1. Overview

Data Subjects have the right to, among other: (i) revoke their consent at any time; (ii) access, rectify, cancel, or oppose the use of their Personal Data in possession of the Controller, which are referred to as "ARCO Rights" and are described in the Mexican DPL; (iii) limit the use or disclosure of their Personal Data; and (iv) opt-out of any secondary purposes.

5.2. Access

Data Subjects have the right to access their Personal Data in a Controllers' possession and information regarding the conditions and generalities of their processing, through an Access Request.

5.3. Rectify

Data Subjects have the right to request that Controllers rectify their Personal Data, if inexact or incomplete, through a *Rectification Request*.

5.4. Deletion/Erasure

Under the Mexican DPL, this right is known as *Cancelation* and the Data Subjects have the right to request Controller to cancel, totally or partially, their Personal Data. Cancelling data means that the Controller must stop processing such data, starting with "blocking" (as such term is defined in Section 9.1) it and afterwards deleting it, per specific terms and rules set forth in law.

5.5. Restriction on Processing

Controllers must provide Data Subjects options or mechanisms so they can limit the Controller's use and disclosure of their Personal Data and the mechanism available so the Data Subject can indicate his/her objection (opt-out) to the processing of his/her Personal Data for secondary purposes, as informed in the privacy notice. In both cases, the INAI has provided examples of how to comply with such requirements. In the first case, the examples include incorporating in the privacy notice (i) a reference to Data Subjects' prerogative to subscribe to the REPEP or the similar registry for financial institutions called REUS; or (ii) an email to send the Controller the applicable request. In the second case, the examples include providing a link or a check-in-the-box in the privacy notice that allows the Data Subjects to inform the Controller of such objection.

5.6. Data Portability

Under the Mexican DPL, there is no right to data portability. But the right of portability is included in the General Data Protection Law, as applicable to regulated (public) entities.

5.7. Right to Object

Data Subjects have the right to oppose the processing of their Personal Data by a Controller, e.g., for specific purposes, through an *Objection* Request.

5.8. Right Against Automated Decision-Making

This right is not regulated *per se* under the Mexican DPL, but Data Subjects could exercise other of their rights under law to oppose or limit the processing of their Personal Data in automated decision making.

5.9. Responding to Consumer Rights Requests

Data Subjects may, at any time, exercise any of the ARCO Rights or revoke their consent. As of the day such request is received, the Controller shall notify the Data Subject within 20 business days the determination made by the Controller regarding the request. If positive, such determination needs to be implemented within 15 business days as of the day such notice is given.

The 15-business day term can be extended one time only by an equal period, if justified by the corresponding circumstances.

Exercising a Data Subject's ARCO Rights must be free of charge to the Data Subject, and Data Subject will only have to pay justified expenses of shipping or such costs for providing or copying the applicable Personal Data in certain situations.

If the determination issued by the Controller is deemed insufficient by the Data Subject or no determination is made at all, the Data Subject may then have the right to initiate a procedure before the INAI to ensure the exercise of his/her rights.

Additionally, as mentioned in Section 4.5.2, if so, required by consumers, suppliers must inform them, at no cost, the information the supplier has in its databases of such consumers and to whom that information has been transmitted. If such information exists, suppliers must respond within 30 days of such request. If the consumer considers there is any ambiguity or inaccuracy in such information, it can inform the supplier, and the supplier must correct that information and notify any third parties that received such information of such correction, within 30 days of such notice.

5.10. Record Keeping Concerning Rights Requests

The Mexican DPL does not establish specific obligations regarding how Controllers should keep the records concerning Data Subject's rights requests, other than stating that it must include the date of reception of Data Subject's request in the applicable acknowledgement of receipt.

5.11. Is Providing Consumers with These Rights Required by Law or Mere Suggestions?

All the rights mentioned in this section are required by law, although the law establishes limits to such rights.

5.12. Application to Digital Advertising

The Mexican DPL and the LFPC do not make any distinctions between marketing and electronic marketing, as such the same rules for marketing apply to digital advertising. One problematic concept under the Mexican DPL is the process the Data Subjects need to carry out to exercise their ARCO Rights when their Personal Data have been transferred. For example, if a Data Subject requests a Controller to *Cancel* (blocking and later deletion) his/her Personal Data, such request would only be applicable to that Controller. If that Controller transferred the Personal Data to a third party, the request would not be obligatory for the latter. Therefore, to make sure his/her Personal Data is deleted by third-party transferee(s), the Data Subject would need to request the Controller information regarding the transfer of his/her Personal Data through an Access Request. The Data Subject would then need to submit the appropriate request with each of the transferees who received his/her Personal Data from the Controller.

6. DATA CONTROLLER AND PROCESSOR AGREEMENTS

6.1. Overview

A Processor is an entity or individual, not a part of the organization of the Controller, that alone or together with others, processes Personal Data on behalf of a Controller because of a legal relationship between the parties, which limits the scope of the services to be rendered. Any communication between a Controller and a Processor are considered as transmissions (*remisiones*) of Personal Data and do not need to be notified to nor consented by the Data Subject.

6.2. Controller Outsourcing of Processing

Any of Processor's outsourcing of services related to processing needs to be authorized by the Controller and be carried out in its name and on its behalf. The Processor will have the obligation to evidence that the subcontracting was duly authorized by the Controller, either in the agreement or legal instruments that have formalized its relationship with the Controller or prior to the subcontracting. The persons who provide these services are considered as "subcontractors" under the Mexican DPL.

Processors need to formalize the relationship with the subcontractor to define the existence, scope, and contents related to the processing of the Personal Data and, per law, the subcontractor will assume the same obligations as Processors have under the Mexican DPL.

6.3. Processor Rights and Responsibilities

Processors have the following obligations in connection to the Personal Data it processes on behalf of the Controller, among others:

i. Only process the Personal Data per the written instructions provided by the Controller and the Controller's privacy notice.
ii. Abstain from processing the Personal Data for purposes other than those instructed by the Controller.
iii. Implement and maintain physical, administrative, and technical security measures in accordance with the Mexican DPL.
iv. Keep confidentiality of the Personal Data.
v. Delete the Personal Data once the legal relationship with the Controller has been fulfilled or as instructed by it, provided that there is no legal provision that requires the conservation of the Personal Data.
vi. Abstain from transferring the Personal Data, except if the Controller determines so or the transfer arises from subcontracting, or when required by the competent authority.

The Mexican DPL considers a special regime for the processing of Personal Data through cloud-based services and allows Controllers to hire their services only if certain requirements are met.

6.4. Application to Digital Advertising

The Mexican DPL and the LFPC do not make any distinctions, so the same rules for marketing apply to digital advertising.

7. DATA TRANSFER & OUTSOURCING

7.1. Overview

A transfer of Personal Data is any communication of Personal Data from the Controller to any third party (the "Transferee"), other than communications between the Controller and Processors. The Transferee assumes the same obligations as the Controller that transferred the Personal Data. Controllers must include in the applicable privacy notice if it will transfer Personal Data, to whom, and for what purpose.

Furthermore, all transfers are subject to the Data Subjects' consent and shall be limited in line with the purpose that justifies it. There are some exceptions to this rule, the most relevant being that no consent is required for transfers to holding companies, affiliates, subsidiaries, or any other company of the Controller that operates under the same privacy policies and procedures.

The foregoing is applicable to both national and international transfers. But the Mexican DPL requires the compliance of different formalities for international and national transfers.

For national transfers, the transferor must inform the transferee of its privacy notice and processing purposes consented by the applicable Data Subject, as well as the conditions under which the Data Subject consented the processing of his/her Personal Data.

For international transfers, the transferor and the transferee must execute an agreement or other legal instrument/ clauses, whereby the transferee undertakes to comply with the same obligations the transferor has in connection with the protection of the Personal Data, as well as any conditions pursuant to which the applicable Data Subjects consented the processing of their Personal Data.

Please refer to Section 4.5.2 for consumer's rights under the LFPC in connection with the transfer of their Personal Data.

7.2. Application to Digital Advertising

The Mexican DPL and the LFPC do not make any distinctions, so the same rules for marketing apply to digital advertising.

8. AUDIT/ACCOUNTABILITY

8.1. Overview

To comply with the Principle of Accountability, Controllers must adopt measures described in Section 4.2 for the proper processing of the Personal Data.

- **Audit - What audit rights are dictated by law (e.g., must companies have audit rights over their vendors? Does it matter what the classification of those vendors are?)**

The Mexican DPL does not expressly dictate audit rights for Controller's vendors. But considering the Controller's obligations under the accountability principle, Controller's should audit its Processors, just like Controllers need to audit their own processing of Personal Data.

- **Accountability - Must companies/vendors keep certain records to prove they have met certain requirements? What are those requirements?**

Controllers have the obligation to prove that they comply with the Mexican DPL, so under the accountability principle, all Controllers should keep the records that evidence their fulfillment of their contractual obligations under the Mexican DPL, including those that relate to the Processors processing activities.

8.2. Application to Digital Advertising

The Mexican DPL and the LFPC do not make any distinctions, so the same rules for marketing apply to digital advertising.

9. DATA RETENTION

9.1. Overview

To comply with the Quality Principle, Controllers must establish and document procedures for the retention, blocking and suppression of the Personal Data. The retention periods do not exceed the necessary time to fulfill the purposes that justified their processing (as stated in the privacy notice), must comply with the Mexican DPL or any other applicable legislation, and must consider the administrative, accounting, tax, legal, and historical aspects applicable to the Personal Data. Once these processing purposes have been fulfilled, provided there is no legal or regulatory provision that establishes otherwise, the person in charge must proceed to cancel the applicable Personal Data, i.e., blocking them, for their subsequent deletion.

Per the Mexican DPL:

- "blocking" means: the identification and conservation of Personal Data once the purpose(s) for which they were collected has been fulfilled, with the sole purpose of determining potential liabilities thereto, until their statutory period has expired. During the "blocking" period, Personal Data may not be processed and once this time has elapsed, the Personal Data will be canceled (sic.) in the corresponding database.
- "deleting" means: the activity consisting of eliminating, erasing, or destroying the Personal Data, once the blocking period has concluded, per the security measures previously established by the Controller.

9.2. Application to Digital Advertising

The Mexican DPL and the LFPC do not make any distinctions, so the same rules for marketing apply to digital advertising.

10. DATA PROTECTION AUTHORITY | REGULATORY AUTHORITY

10.1. Overview

Pursuant to the Political Constitution of the United Mexican States, the protection of Personal Data shall be in charge of the INAI, an independent constitutional body (*organismo constitucional autónomo*).

The PROFECO oversees the compliance of the suppliers' obligations established in the LFPC in connection to the processing of Personal Data.

10.2. Main Regulator for Data Protection

The main regulator for data protection in Mexico is the INAI.

10.3. Main Powers, Duties and Responsibilities

The main purpose of the INAI, regarding Personal Data held by private parties, is to disseminate information on the right of Personal Data protection in Mexico, by promoting its exercise and overseeing the compliance of the Mexican DPL.

INAI's main responsibilities vis a vis the processing activities of private parties are the following, among others:

- Oversee and verify compliance of the provisions of the Mexican DPL.
- Interpret Mexican DPL.
- Provide technical support to the Controllers as requested.
- Issue opinions and recommendations for purposes of the function and operation of the Mexican DPL.
- Disseminate international best practices and standards for information security, in view of the nature of the data, the processing purposes, and the technical and financial capacity of the Controllers.
- Hear and issue decisions in rights protection and verification procedures and impose sanctions as appropriate.
- Cooperate with other domestic and international bodies and supervisory authorities, to assist in the area of Data Protection.
- Submit an annual activity report to the Mexican Congress.
- Participate in international forums regarding Personal Data protection.
- Carry out studies of the impact on privacy prior to the implementation of new types of processing of Personal Data or material modification of existing types of processing.
- Develop, promote, and disseminate analyses, studies and research in the area of protection of Personal Data held by third parties and provide training to the obligated parties.

10.4. Application to Digital Advertising

INAI regulates the protection of Personal Data on digital advertising. The foregoing in the understanding, however, that the PROFECO can also intervene in connection to the consumer's related rights under the LFPC.

11. SANCTIONS

11.1. Overview

Sanctions for infractions of the Mexican DPL range from mere fulfilment requirements, to fines and even prison.

11.2. Liability

Data Subjects can file criminal claims or civil claims in connection with any damage or loss caused by the improper processing of their Personal Data. For example, the improper use of Personal Data could result in a "moral damage"

for a Data Subject, i.e., an affectation that a person suffers in his/her feelings, affections, beliefs, decorum, honor, reputation, private life, configuration, and physical appearance, or in the consideration that others have of himself/herself. In such event, the affected Data Subject could file a claim against the Controller in a civil court requesting the payment any damages and losses that resulted from the moral damage caused by the improper use of his/her Personal Data.

Administrative Penalties

Sanctions for infractions of the Mexican DPL range from mere fulfilment requirements, to fines from approximately USD $470 to USD $1,502,000, which can be increased if the violation related to the processing of Sensitive Data. These sanctions are imposed without limitation to any civil or criminal liabilities that results from the applicable infraction.

The following are considered as infractions of the Mexican DPL, among others:

- Failure to comply with a Data Subject's ARCO Rights' request, without well-founded reason, in terms of the Mexican DPL.
- Acting negligently or fraudulently when responding or processing a Data Subject's ARCO Rights' request.
- Omitting any or all the required items in the privacy notice, as required per the Mexican DPL.
- Failure to comply with the duty of confidentiality.
- Process Personal Data infringing the principles established in the Mexican DPL, referred in section 4.1.
- Transfer Personal Data to third parties without providing them with the applicable privacy notice to process such data.
- Transfer or hand over Personal Data outside of the cases permitted under the Mexican DPL.
- Collect or transfer Personal Data without Data Subject's express consent, in cases when consent is required.
- Materially change the primary purposes to process the Personal Data, failing to comply with the requirements established in the Mexican DPL.
- Collect Personal Data in a fraudulent or deceptive manner.
- Obstruct verification procedures initiated by the INAI.
- Create databases with Sensitive Data, without proving that those were created for legitimate and concrete purposes, in accordance with the activities carried out by the data Controller.
- Any failure of the data Controller to comply with its obligations under the Mexican DPL.

Criminal Penalties

Imprisonment can be imposed from three months to five years if a Controller, looking for profit, causes a security breach in its Personal Data database or if someone, through deception, acquires or processes Personal Data for such reason. These sanctions will be doubled for Sensitive Data.

- **Scope of liability for ad tech companies for collection activities of publishers and advertisers.**

Liability in this case would depend on the role of the ad tech company in these collection activities, i.e., if it acts as a Controller or a Processor. In the first case, where the ad tech company acts as a Controller, the liability of ad tech companies is as explained above. In latter case, where the ad tech company acts as a Processor, if the ad tech company (i) complies with all its obligations as a Processor, its only liability would be contractual to the Controller, if any; but (ii) if the ad tech company fails to process the Personal Data for the purposes authorized by the Controller or breaches any of the Controller's instructions, then the ad tech company would be considered as a Controller and would processing the applicable Personal Data illicitly and have the corresponding liability under the Mexican DPL.

- **Scope of liability for ad tech companies for other ad tech companies they enable to process data (either b/c they make the decision of publishers or advertisers or agency dictates it).**

Considering that subcontractors have the same obligations as Processors under the Mexican DPL, if the second ad tech company (i) complies with all its obligations as a Processor, there would be no liability for neither of them; but (ii) if the subcontractor fails to process the Personal Data for the purposes authorized by the Controller or contravenes any of Controller's instructions, then the second ad tech company would be considered as a Controller and would processing the applicable Personal Data illicitly and have the corresponding liability under the Mexican DPL.

The foregoing, assuming that the first ad tech Company had the Controller's authorization to enable the second ad tech Company to process the applicable Personal Data.

11.3. Enforcement and Market Practice

- **How are claims raised under the law?**

Data Subjects can initiate a procedure of protection of rights before the INAI when he/she considers that the Controller did not address an ARCO Rights' request appropriately.

The INAI could initiate a data protection verification procedure per the Data Subjects' requests or ex officio, to determine if any breach of obligations to protect Personal Data had occurred. Furthermore, any person can report to the INAI alleged violations to the Mexican DPL (other than the ones described in the previous paragraph) and the INAI can also initiate a data protection verification procedure.

When the INAI has issued a resolution for any breach of the Controller's obligations regarding the processing of the Data Subject's Personal Data, the Data Subjects can file a claim before the competent judicial authorities to request for an indemnification from the party responsible of such breach, if applicable.

- **Who enforces them?**

The INAI is in charge of determining any liability arising from Controller's violations of the Mexican DPL and the judicial authority will be in charge to determine any criminal or civil liability caused by the Controller as a result from such violations.

- **What's their practice (quietly working with companies to fix, publicly coming out with large investigations? Fact specific?)**

When a Data Subjects initiates a procedure of protection of rights before the INAI, the INAI must promote conciliation between the parties, per law. INAI's practice regarding verification procedures depends on a case-by-case basis, there have been several times that the INAI has announced that it started an investigation against a company, particularly in high-profile cases.

- **What guidance has been issued to date on how to handle requirements in the ad ecosystem? Have the regulators been educated on how the ecosystem operates? Have compliance regimes been discussed with them? Has their feedback been solicited?**

No specific enforceable guidance has been issued by the INAI.

11.4. Remedies

The remedies under the Mexican DPL include administrative proceedings in front of INAI, but no damages awarded since they need to be awarded through civil or criminal courts.

The remedies in connection with advertising practices available under the LFPC include administrative proceedings in front of PROFECO, bonifications and compensations, reimbursements and indemnifications of damages and losses.

11.5. Private Right of Action

Data Subjects can file civil or criminal related claims in connection with any damage or loss regarding the improper use of their Personal Data.

11.6. Digital Advertising Liability Issues

Digital Advertising has the same liability issues as any other type of Personal Data processing.

12. NOTIFICATION | CERTIFICATION | REGISTRATION

12.1. Overview

Controller does not have to be certified or registered before any authority nor has to give any notice in order to collect and process Personal Data. Privacy notices do not have to be registered or certified before their use by a Controller.

12.2. Requirements and Brief Description

N/A

12.3. Application to Digital Advertising

N/A

13. DATA PROTECTION OFFICER

13.1. Overview

Pursuant to the Mexican DPL, all Controllers must appoint a data protection officer or a data protection department, who oversees processing any Data Subjects requests in connection with their rights under the Mexican DPL, as well as of fostering the protection of Personal Data within the company.

13.2. DPO – Compulsory Appointment (Yes/No)

Yes.

13.3. Requirements

The only obligation for Controllers in connection to this issue is the one stated in Section 13.1. The INAI has issued recommendation in connection to data protection officers or department which establish, among other suggestions, that such person or department must:

- Have experience in data privacy: usually the compliance and audit departments are familiarized with data privacy.
- Have sufficient authorities within the entity to implement data privacy policies which promote the protection of Personal Data.
- Have sufficient resources to process the requests by the Data Subjects and implement any and all data privacy policies.
- Be knowledgeable on the subject, i.e. the person(s) has to be familiar with any and all applicable data protection regulations.

13.4. Application to Digital Advertising

There are no specific provisions for digital advertising regarding this matter.

14. SELF-REGULATION

14.1. Overview

- **Are there any industry-self regulatory schemes in place in the jurisdiction?**

Mexican DPL allows individuals or legal entities to establish binding self-regulation schemes, which complement the provisions of the law. Such schemes must comply with minimum requirements determined by the INAI. Self-regulation schemes may be translated into codes of ethics or good professional practice, trust stamps, or other mechanisms and will contain specific rules or standards that allow harmonizing the data processing carried out by the adherents and facilitate the exercise of the rights of the Data Subjects. Said schemes must be notified simultaneously to the corresponding sectoral authorities and the INAI.

Are there any signal-based programs used in the territory to assist with digital advertising compliance?

No.

14.2. Application to Digital Advertising

Same as described hereinabove, there are no specific provisions for digital advertising.

15. PENDING PRIVACY BILLS

15.1. Overview

As of the first quarter of 2021, there are 21 initiatives, pending approval, to amend the Mexican DPL.

Such pending bills attempt to cover various issues including, data breach notifications, cybersecurity matters (the regulation of this matter is imminent, the Mexican constitution has just been amended to allow our legislative power to issue legislation to regulate this subject), modifications to the Mexican DPL to add obligations and modify definitions, recognition and protection of digitized Personal Data, criminalization of offenses related to the undue processing of Personal Data, prohibition of advertising telephone calls, Personal Data of minors, biometrics, among many others.

15.2. Application to Digital Advertising

There is currently an initiative, pending approval, to issue the Federal Law for the Protection of Digital Users. One of the objectives of this law would be to protect digital users against misleading and abusive advertising, coercive and unfair commercial methods, as well as against abusive or imposed practices and clauses in the provision of digital services.

iab.

Nigeria

Cross-Jurisdiction Privacy Project

1. THE LAW

1.1. Overview & Key Acts, Regulations, and Directives

Data protection in Nigeria is codified in a number of statutes and common law. These laws include data protection statutes of general application, as well as sector-specific statutes. An asterisk notation is included for those likely applying to digital advertising transactions:

- The Constitution of Federal Republic of Nigeria 1999 (as amended) (the "**Constitution**")
- Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 (the "**Cybercrimes Act**")
- National Information Technology Development Agency ("**NITDA**") Act 2007*
- National Health Act, 2014 (the "**Health Act**")
- Federal Competition and Consumer Protection Act 2019 ("**FCCPA**")*
- Nigerian Communications Commission ("**NCC**") Act, 2003
- National Identity Management Commission ("**NIMC**") Act 2007
- Data Protection Bill 2020 (the "**Proposed Bill**")
- Advertising Practitioner's (Registration, Etc.) Act No. 55 of 1988, CAP A7 Laws of the Federation of Nigeria 2004 (the "**APCON Act**")
- Credit Reporting Act, 2017 ("**CRA**")

In addition, there are legislations relating to privacy, personal health information, and public sector institutions, however, for the purpose of this report ("Report"), we have focused on privacy laws that mainly apply to the private sector.

1.2. Guidelines

The National Information Technology Development Agency (NITDA) issued the following guidance in respect to the processing of personal information:

- Nigerian Data Protection Regulation 2019 ("**NDPR**")*
- NDPR Implementation Framework 2020 ("**Data Framework**")*
- Guidelines for the Management of Personal Data by Public Institutions in Nigeria, 2020 (the "**Guidelines**")
- Draft National Outsourcing Strategy, 2020
- Guidelines for Nigerian Content Development in Information and Communication Technology, 2019
- Nigeria e-Government Interoperability Framework, 2019
- Nigeria Cloud Computing Policy, 2019

- Framework and Guidelines for Information and Communication Technology (ICT) Adoption in Tertiary Institutions, 2019
- Public Key Infrastructure (PKI) Regulations (Code of Practice for Accredited Certified Authorities (CAs)
- National ICT Policy, 2012
- Framework and Guidelines for Public Internet Access (PIA)
- Nigeria e-Government Interoperability Framework (Ne-GIF)
- The National Digital Economy Policy and Strategy for A Digital Nigeria (2020 - 2030)

The NCC issued the following guidance:

i. Consumer Code of Practice Regulations, 2007 ('the **NCC Consumer Code of Practice**')
ii. Consumer Protection Framework 2016
iii. Guidelines for the Provision of Internet Service
iv. Framework and Guidelines for Public Internet Access 2019

Finally, the National Insurance Commission (NAICOM) issued the Nigerian Insurance Industry ICT guideline (N3IG 1.0) Version 1.0

1.3. Case Law

The introduction of the NDPR and its objective of protecting the data of data subjects, has raised questions about the nature of the rights conferred by same. There is a school of thought that the rights of a data subject should be enforced similar to the fundamental rights under the Constitution through the use of the enforcement procedure provided under the Fundamental Rights (Enforcement Procedure) Rules ("FREP Rules"). This argument was considered in ***The Incorporated Trustees of Digital Rights Lawyers Initiative and L.T Solutions & Multimedia Limited (DRLI VS LTSM).***[1]

The facts of this suit occurred on the back of an alleged tweet by LTSM offering for sale, over 200 million Nigerian and international mailing lists. DRLI brought the suit under the FREP Rules and contended that LTSM does not have the right or legal basis to process Personal Data. in the manner that it purportedly did. The central issue was whether LTSM invaded or was likely to invade DRLI's rights to privacy provided under Section 37 of the Constitution and the NDPR. The court held that the right to privacy under Section 37 of the Constitution ought to be

[1] Suit No. AB/83/2020 (Unreported)

interpreted expansively to include protection of personal data under the NDPR and therefore, the suit was properly situated under the FREP Rules.

Conversely, there are those opposed to this view who argue that a data subject's rights under the NDPR are neither constitutional rights nor fundamental human rights under the African Charter, and as such, cannot be enforced under the procedure provided in the FREP Rules. This position received judicial approval in the matter of ***Incorporated Trustees of Laws and Rights Awareness Initiative and The National Identity Management Commission10 (RAI vs NIMC)***[2].

The suit was filed in connection with the initiative of the Nigerian Government to establish a national identity database pursuant to the National Identity Management Commission ("NIMC") Act enacted in 2007. NIMC is the public body established to, among others, maintain this database and issue National Identification Numbers to registered persons. RAI, a public interest litigant purportedly suing for and on behalf of one Daniel John, claimed that the processing of personal data by NIMC is likely to interfere with Daniel John's right to privacy guaranteed under Section 1.1(a) of the NDPR and Section 37 of the Constitution. On the basis of this contention, RAI sought to injunct NIMC from further releasing digital identity cards pending an independent report of external cyber security experts on the safety and security of the Respondent's applications. The suit was brought under the FREP Rules. One of the central issues that came up for consideration was whether the claim for breach, or rather, potential breach of the provisions of the NDPR was properly brought under the FREP Rules having been lumped together with a claim for breach, or potential breach of the right to privacy under Section 37 of the Constitution? The FHCN, after a careful review of the arguments on both sides, held that the suit was wrongly brought as a fundamental right enforcement action under the FREP Rules.

Please see the link to the Templars Thought Leadership on this issue for further information:

Templars-Thought-Leadership-Publication-on-Enforcing-Data-Subject-Rights-Under-Nigeria's-Data-Protection-Regulation-The-Wrong-Way-And-The-Right-Way.pdf (templars-law.com)

1.4. Application to Digital Advertising

1.4.1. The NDPR

This is the principal legislation that governs data protection in Nigeria. The NDPR is applicable to digital advertising as it regulates the collection, storage, dissemination, utilization, and processing of personal data of any natural persons residing in Nigeria or Nigerian citizens resident outside Nigeria.

[2] Suit No. FHC/AB/CS/79/2020 (Unreported)

1.4.2. NDPR Implementation Framework 2020

The Data Framework provides guidance on the implementation of the NDPR for private and public organizations that engage in the collation and processing of personal data. In doing so, the Data Framework introduces concepts and elaborates on issues that were briefly addressed in the NDPR. For instance, the Data Framework elaborates on the types of consents that should be utilized by data processors, and the requirements of valid consent.

The Proposed Bill

The Proposed Bill seeks to provide codified data protection granted under the NDPR into statutory legislation as well as expand the NDPR's scope of activity and regulation. It also seeks to establish a Data Protection Commission ("Commission") to be tasked with the protection of personal data and the rights of data subjects, the regulation of the processing of personal data, etc.
For instance, in relation to digital advertising, the Proposed Bill states that data subjects shall have the right to object to the processing of their personal data for the purpose of direct marketing[3] at any time and at no cost, and that a data controller shall not provide, use, obtain or procure information related to a data subject for the purposes of direct marketing without the prior written consent of the data subject.[4]

2. SCOPE OF APPLICATION

2.1. Who Do the Laws/Regulations Apply to and What Types of Processing Activities are Covered/Exempted?

2.1.1.NDPR

Overview

i. The NDPR applies to all actions connected with the collating and processing of personal data of natural persons in Nigeria or Nigerian citizens resident outside Nigeria, irrespective of the data processing method adopted. Thus, the NDPR applies to any person involved in any element of data processing including data collection, data preparation, data input, data output or interpretation, data processing, data storage, and data transfers.[5]

---

[3] Direct marketing is defined to mean that which "*includes the communication by whatever means of any advertising or marketing material which is directed to particular data subjects.*"

[4] Section 21(2), section 21(3) the Proposed Bill

[5] Article 1.2 NDPR

ii. By implication, the NDPR regulates the activities of individuals, organizations or businesses including website operators, advertisers, tech vendors, and other persons involved in the collection or processing of natural persons residing in Nigeria or Nigerian citizens residing outside Nigeria. The NDPR does not exempt any type of processing activity, however, by virtue of its scope of application, i.e., being limited to the personal data, it could be implied that the law does not apply to non-personal data.

Application to Digital Advertising

The NDPR is applicable to digital advertising that entail the use of personal data, sensitive data, personal identifiable information, or other type of data described therein.

2.1.2. The Proposed Bill

Overview

The Proposed Bill is intended to apply to the collection, storage, processing, and use of personal data relating to the following persons:

a. A Nigerian data subject.
b. A data subject that resides in Nigeria.
c. A body incorporated under the laws of Nigeria.
d. An unincorporated joint venture or association operating in part or in whole in Nigeria.
e. Any person who maintains an office, branch, or agency through which business activities are carried out in Nigeria.
f. Foreign entities targeting persons residing in Nigeria.

Proposed Exemptions:

a. The Proposed Bill seeks to exempt personal data from its provisions on the grounds of public order, public safety, public morality, national security, public interest, the prevention or detection of crime, the apprehension or prosecution of an offender, the assessment or collection of a tax or duty or of an imposition of a similar nature, or the publication of a literary or artistic material.[6]

2.1.3 The Constitution

The Constitution guarantees and protects the privacy of citizens, their homes, correspondences, telephone conversations, and telegraphic materials.[7]

[6] Section 35(1) of the Proposed Bill.

[7] Section 37 of the Constitution.

Application to Digital Advertising

Please refer to summary in paragraph 1.5 above.

2.2. Jurisdictional Reach

Overview

The NDPR applies to all transactions intended for the processing of personal data of natural persons residing in Nigeria or Nigerian citizens residing in foreign jurisdictions.[8]

Application to Digital Advertising

Hypotheticals to test concerns/jurisdictional reach

Scenario 1 (*below*) is the baseline scenario, where the user, publisher, and advertiser are all based in Nigeria and where it seems reasonable to assume the privacy law applies. Scenarios 2, 3, and 4 vary the location of the user, publisher, and advertiser to test in each case the jurisdictional reach of the privacy laws.
For each scenario, we should ask how (if at all) does the Privacy Law apply to:

Q - Serving the ad to the user.
Q - Building a profile of the user.
Q - The publisher's legal obligations.
Q - The advertiser's legal obligations.

Scenario 1 (The baseline): A user residing in Nigeria (determined by IP address or geo identifier) goes onto a Nigerian domain and is served an ad by a Nigerian advertiser. The advertiser uses the user data to build a user profile.

Q - Serving the ad to the user:
A - Where this activity entails the collection of the user's personal data, the user's consent must be obtained prior to such collection.

Q - Building a profile of the user:
A - The user must be informed of and must consent to the use of their data.

Q - The publisher's legal obligations:
A - The publisher is required to comply with the data controller's obligations stated in our response to Section 4 below.

Q - The advertiser's legal obligations:
A - The advertiser is required to comply with the data controller's obligations stated in the NDPR, some of which have been summarized in Section 4 below.

[8] Article 1.2(xxi) of the NDPR.

Scenario 2 (User outside Nigeria): A logged-on/signed-in user, known by the publisher to be a Nigerian resident, goes onto a Nigerian domain but the user's IP address or geo-identifier indicates the user is outside Nigeria. A Nigerian advertiser serves an ad and uses the user data to build a user profile.

A - The NDPR is applicable to Nigerian subjects, even those that are not residents in Nigeria, thus, the provisions of the NDPR should apply.

Q1 - Does the answer change if this is a signed-out user, with no way of knowing where they are domiciled?
A - The answer remains unchanged where the user is a Nigerian citizen as the NDPR will nevertheless apply. Theoretically, this law should apply even though the IP address does not indicate that the user is a Nigerian, however, from a practical perspective it may be difficult to enforce this provision if the identity of the data user is unknown.

Scenario 3 (Publisher domain outside Nigeria): A user residing in Nigeria (determined by IP address or geo identifier) goes onto a domain outside of Nigeria. A Nigerian advertiser serves an ad and uses the user data to build a user profile.

The advertiser is expected to comply with the provisions of the NDPR, including obtaining the user's consent prior to collecting and processing his or her data.

Q1 - Does the answer change if the site hosts content aimed at Nigerian residents (e.g., a news aggregator with a section on Nigerian current affairs)?
A - The answer remains unchanged on account of the NDPR's requirement that same should be applicable to Nigerian citizens irrespective of location.

Q2 - Does the answer change if the advertiser is based outside of Nigeria?
A - The answer remains unchanged provided the user is a Nigerian citizen as the NDPR will nevertheless apply.

Scenario 4 (Advertiser outside Nigeria): A user residing in Nigeria (determined by IP address or geo identifier) goes onto a Nigerian domain and is served an ad by an advertiser based outside Nigeria. The advertiser uses the user data to build a user profile.

According to the NDPR, the advertiser is required to obtain the consent of the subject prior to collecting or processing his or her data.

Q - Does the answer change if the advertiser has an affiliate/group company based in Nigeria?
A - The answer remains unchanged where the user is a Nigerian citizen.

3. DEFINITIONS

3.1. Collect

The law does not define this.

- **When a publisher allows an ad tech company's pixel on its page, who is deemed to "collect" personal information and incur legal obligations (e.g., controller/co-controller obligations under GDPR or "business" obligations under CCPA) -- the publisher, the ad tech company, or both?**

  The NDPR does not define "collection" of personal information and it does not indicate who is deemed to "collect" same in this circumstance. Although the law recognizes that data can be processed (a term defined below), from a holistic reading of the NDPR and the Data Framework, its focus appears to be on the treatment of personal data in the possession of any person that processes same.

3.2. Data Processing (i.e., collecting, capturing, retaining, recording, organizing, structuring, storing, altering, retrieving, consulting, using, disclosing, transmitting, disseminating, making available, aligning, combining, restricting, erasing, destroying, or otherwise processing)

i. Data Processing:

The NDPR

This means any operation which is performed on personal data whether or not by automated means, such as collection, recording, organizing, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.[9]

The Proposed Bill[10]

"Data processing" means any operation or set of operations performed on personal data, such as (a) collection, recording, organization, structuring, storage or preservation; (b) adaptation or alteration; (c) access, retrieval or consultation; (d) transmission, disclosure, sharing or making available; or (e) restriction, erasure, or destruction of, or the carrying out of logical or arithmetical operations.

[9] Article 1.3 of the NDPR.

[10] Section 66 of the Proposed Bill.

According to the Proposed Bill, "data processing" where automated processing is not used, means an operation or set of operations performed upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria.

3.3. Personal Information

The NDPR does not define personal information. Rather, it defines "personal identifiable information" as information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in a context. It also defines "personal data," which means any information relating to an identified or identifiable natural person (referred to as a 'data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information (PII) and others."[11]

i. Personal Data Breach

NDPR

This means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.

ii. Data Subject:

NDPR

An identifiable natural person, that is, one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. Such identifier can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM, and others.[12] Data subject also means an identified or identifiable living natural person to whom personal data relates.[13]

---

[11] Article 1.3(xix) of the NDPR

[12] Article 1.3(xiv) of the NDPR.

[13] Section 66 of the Proposed Bill.

Type of Information Collected	Does this Category Independently Constitute Personal Information? (Yes/No)	Qualifying Notes (if any)
IP Address	Yes	
Mobile Advertising IDs (IDFA, AAID)	No	We understand that there are instances where mobile advertising IDs may contain personal identifiable information but this information is typically pseudonymized or altered in a manner that cannot be used to identify a data subject directly or indirectly. Based on this understanding, mobile advertising IDs are unlikely to constitute personal information.
Consumer identifiers such as: • User device ID • Publisher persistent ID/Cross-publisher cookie ID • Household ID	Yes	These would likely constitute personal information if such can be used in identifying a person.
Hashed identifiers such as: • Hashed email • Hashed IP address	No	If the hashed data becomes anonymized or altered in a manner that cannot be traced or linked to a data subject, it will not form personal information.
User Agent such as: • Character string identifying the application • Operating system • Browser information, vendor, and/or version of the requesting user agent	No	Provided that this information cannot be utilized to identify a data subject, same will not constitute personal information.

Device Information such as: • Type, version, system settings, etc.	No	A device, in and of itself, does not constitute personal data. However, when the same is registered by a data subject and this registration includes the data subject's personal details, the device would likely constitute personal information as such information could potentially be used to directly or indirectly identify a data subject.
Website Information such as: • Name • URL, etc.	No	The name of the website is not personal information because it does not typically contain any personal data whilst the URL will not constitute personal data if the information is linked to a corporate entity and not a data subject.
Advertisement Information such as: • Placement • Title • Creative ID, etc.	No	This would constitute personal information if it contains any information that can be used to identify a person.
Timestamps	No	Timestamps would be unlikely to constitute personal information if the information therein is not identifiable information although can be used to determine who logged into a system.
Metrics such as: • Counts • Amounts of time	No	This would not constitute personal information if the information cannot be used to identify a data subject.

Event Data such as: (e.g., full URL including query string, referral URL)	Yes	Some URLs contain personal data, and in that regard, will constitute personal information.
Precise geolocation (latitude, longitude)	Yes	
General geolocation (city, state, country)	No	The NDPR does not appear to address general geolocation but in the absence of additional information that can identify a specific subject, a general location may not constitute personal information.

- **Are pseudonymous digital identifiers by *themselves* personal information (e.g., IDFA, cookie IDs, proprietary IDs, IP addresses, etc.)? Please provide context to the above chart.**

  No, pseudonymous digital identifiers by themselves do not constitute personal information. However, if there is a way or possibility that pseudonymous information can be easily cracked or if there is a key to easily identifying the pseudonymous information, it potentially becomes personal information.

- **If the answer to the above question is, "no," if a Company possesses a persistent digital identifier in Database 1 and has that same identifier in Database 2 with directly identifying information, does that render the pseudonymous information in Database 1 as personal information?**

  Our understanding of this scenario is that although both databases contain the same information, Database 1 is pseudonymized whilst Database 2 contains directly identifying information. This scenario does not render the pseudonymous information in Database 1 personal information, and, provided that there are adequate measures in place that ensure that the information in Database 2 cannot be linked or traced to Database 1, Database 1 will likely not constitute personal data.

- **Is a Company's possession of a pseudonymous identifier plus other non-directly identifying data (e.g., age, gender, precise or imprecise geolocation, user agent string, timestamps) considered "personal information"?**

  The NDPR and the Framework do not speak directly to this issue, and there appears to be a lack of judicial interpretation on this point. However, from a holistic reading of the law, possession of a pseudonymous identifier plus other non-directly identifying data would potentially be considered personal information.

- **Is a Company's possession of a pseudonymous identifier "personal information" if it can hire a service provider or otherwise engage in a transaction with a third party where the identifier *could* be matched to the person *but* the Company chooses not to hire such service provider or undertake such transaction? Is the mere fact that this service is *potentially* available to match to the person sufficient to render that pseudonymous identifier as "personal information"?**

  Our understanding of this scenario is that two different parties have two different databases and both databases contain the same information, Party A's Database is pseudonymized whilst Party B's Database contains directly identifying information. This scenario is unlikely to render the pseudonymous information in Party A's Database personal information, and, provided that there are adequate safeguards that ensure that the information in Party B's Database cannot be linked or traced to Party A's Database, Party A's Database will likely not constitute personal data.

- **What level of geolocation is personal information (precise vs. approximate)? Does it need to be associated with an identifier to be considered personal information?**

  The law does not specify the level of geolocation that would be considered personal data.

- **Is a household identifier personal information?**

  Personal data as defined under the NDPR is any information relating to an identified or identifiable natural person. While household identifiers are not expressly listed under examples of personal data provided in the NDPR, if they contain unique information pertaining to households or the data subjects residing therein, such identifiers should be classed as personal data.

- **Is a hashed identifier PI?**

  Our understanding is that hashing protects the integrity of the data. Although hashed, the information will likely still be considered personal information unless the data is altered in a manner that cannot be traced to a data subject.

- **Is probabilistic information considered personal information?**

  The NDPR does not address this.

3.4. Sensitive Data

The NDPR

The NDPR defines sensitive personal data as data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trades union membership, criminal records, or any other sensitive personal information.[14]

This is also defined in the Proposed Bill as:

- Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data.
- Biometric data for the purpose of uniquely identifying a natural person's data concerning health.
- Data concerning a natural person's sex life.
- Personal data concerning the data of a child who is under the age of 16.
- Such other personal data that may be designated as sensitive data by guidelines made by the Commission.[15]

3.5. Pseudonymous Information

Nigerian law does not define pseudonymous information.

3.6. Anonymized/De-identified Information

Nigerian law does not define anonymized/de-identified information.

3.7. Data Controller

NDPR: A person who either alone, jointly with other persons or in common with other persons, or as a statutory body determines the purposes for and the manner in which personal data is processed or is to be processed.[16]

The Proposed Bill: The natural or legal person, public authority, service, Commission, or any other body which, alone or jointly with others, has decision-making power concerning determining the purposes and means of data processing, and where a data controller also serves as a data processor, the provisions regarding the activities of a data controller under this Act shall apply.[17]

---

[14] Article 1.3(xxv) of the NDPR.

[15] Section 66 of the Proposed Bill.

[16] Article 1.3(x) of the NDPR.

[17] Section 66 of the Proposed Bill.

3.8. Joint Controller/Co-Controller

The NDPR appears to recognize the concept of the joint controller.

Nigerian law does not indicate whether the relationship between a publisher and an ad-tech company would be considered joint or co-controller. However, from the definition of data controller above, if the publisher and the ad-tech company both determine the purpose for and the manner of processing the data, it may be inferred that they will both be seen as joint controllers of data.

3.9. Data Processor/Service Provider (i.e., an entity that is qualified as a processor or service provider under the law because it meets certain requirements and processes data pursuant to a permissible purpose on behalf of a controller/business)

The NDPR does not define "processor" but defines a data administrator as a person or an organization that processes data.

3.10. Third Party (i.e., a third party that receives data from a business for non-business purposes and does not necessarily have specific requirements under the law as to such data, such as a third-party under the CCPA)

Under the NDPR, a third party is "any natural or legal person, public authority, establishment or any other body other than the data subject, the data controller, the data administrator and the persons who are engaged by the data controller or the data administrator to process personal data."[18] Data processing by a third party is required to be governed by a written contract between the third party and the data controller. Accordingly, any person engaging a third party to process the data of data subjects is to ensure adherence to the NDPR.[19]

4.DATA CONTROLLER RIGHTS AND RESPONSIBILITIES

4.1. Overview

The NDPR: the obligations of the data controller include:

- Ensuring that the consent of a data subject is obtained, and without fraud, coercion, or undue influence.[20]

[18] Article 1.3(xxvii) of the NDPR.

[19] Article 2.7 of the NDPR.

[20] Article 2.3(2), NDPR

- Designating a data protection officer ('DPO') for the purpose of ensuring adherence to the NDPR, relevant data privacy instruments and data protection directives of the data controller.[21]
- Ensuring continuous capacity building for its DPOs and other personnel that engage in data processing.[22]
- Filing a summary of its data protection audit at the NITDA where it processes the personal data of more than 1,000 data subjects within a six-month period[23], or 2,000 data subjects within a 12-month period. These reports should include information on the purpose of collection of personal data, confirmation that data subjects' consent was obtained prior to the collection, use, transfer or disclosure of such data, the purpose and use of the data, etc.
- Taking appropriate measures to provide any information relating to processing to the data subject in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, including in relation to information relating to a child.[24]
- Providing the data subject with relevant information prior to data processing (including collection) of personal data[25] such as information on the data controller; the purpose of the processing, the legitimate interests[26] pursued by the controller and the recipients or categories of recipients of the personal data (if any).

The Proposed Bill

The obligations of the data controller under the Proposed Bill[27] include:

- Ensuring the processing of personal data is proportionate and having regard to the interests, rights, and freedoms of the data subject or the public interest.
- Considering the risks arising from the interests, rights, and fundamental freedoms of data subjects, according to the nature, volume, scope, and purpose of processing the data.

---

[21] Article 4.1(2), NDPR

[22] Article 4.1(3), NDPR

[23] Article 4.1(6), NDPR

[24] Article 3.1 (1), NDPR

[25] Article 3.1(7), NDPR

[26] However, we understand that there is a temporary suspension of "legitimate interest" due to the ambiguities arising from its interpretation.

[27] Section 30 – 31, the Proposed Bill.

- Examining the likely impact of the intended processing of personal data on the rights and fundamental freedoms of data subjects prior to the commencement of such processing.

4.2. Accountability

4.2.1. Overview

The NDPR sets out mechanisms to ensure accountability from organizations and data processors. It provides that any person entrusted with or in possession of personal data shall be accountable for his acts and omissions in respect of the processing of such data.[28] A party to any data processing contract, (other than the data subject), is required to take reasonable measures to ensure the counter party does not have a record of violating the rights of data subject contained in the NDPR, and that the counterparty is accountable to NITDA or any other data protection regulatory authority outside Nigeria.[29] The NDPR further stipulates that every data processor or controller shall be liable for the actions or inactions of third parties handling the personal data of data subjects.[30]

4.2.2. Application to Digital Advertising

Any person seeking to engage in digital advertising is required to comply with the rights and obligations contained in the NDPR.

4.3. Notice

4.3.1. Overview

- **Who must receive notice? When must notice be provided?**

  The NDPR:

  Notice should be given to the data subjects prior to obtaining consent and prior to the collection of data.[31]

  In addition, the data controller is obligated to provide the data subject with all the following information prior to collecting personal data from a data subject:

  - The identity and the contact details of the controller.;
  - The contact details of the Data Protection Officer.;

---

[28] Article 2.1(3), NDPR

[29] Article 2.4(b), NDPR

[30] Article 2.4(b), NDPR

[31] Article 2.3(1) NDPR, Article 4.1 (5) NDPR

- The purpose(s) of the processing for which the personal data are intended as well as the legal basis for the processing.[32]

- **Is there specific notice required for sensitive information?**

  The NDPR does not provide for specific notice requirement for sensitive information. Rather, personal data (sensitive or not) is required to be collected and processed only with the prior consent of the data subject in accordance with the specific, legitimate, and lawful purpose contained in the notice provided to the data subject.[33]

- **Are there any specific requirements for providing notice related to processing children's personal information?**

  The Data Framework

  The Data Framework provides that consent must be sought and obtained from the parent or guardian of a child before the child's personal data is processed.[34]

  The Proposed Bill

  The Proposed Bill contains the same requirement as the Data Framework stated above, However, it goes further to define a child as a person under the age of 16.

- **Are there any requirements compelling vendors directly collecting personal information or those receiving it from others to provide additional notices? Who is responsible for those notices? Publishers? The vendors?**

  Consent must be obtained prior to the collection and processing of personal data whether obtained by vendors directly or from other vendors. The data controller has an obligation to provide to the data subjects all, including additional notices necessary or as requested by the data subject.

4.3.2. Application to Digital Advertising

- **Are there specific requirements related to providing notice of data collection for digital advertising purposes?**

---

[32] Article 3.1(7) NDPR Section 26(1) the Proposed Bill

[33] Article 2.1(a) NDPR

[34] Article 6.2(d) The Data Framework

The Data Framework

The Data Framework provides that consent is required for any direct marketing activities[35] however, it does not appear to set out any separate or marketing-specific notification requirements.

The Proposed Bill

The Proposed Bill provides that a data controller shall not provide, use, obtain, or procure information related to a data subject for the purposes of direct marketing without the prior written consent of the data subject.[36] The Proposed Bill defines direct marketing as including "*the communication by **whatever means of any advertising** or marketing material which is directed to particular data subjects.*" The implication of this is that notice must be given to the data subject for the collection of data for digital advertising purposes.[37]

- **Does the law or guidance distinguish between analytics vs. direct sold campaigns vs. allowing third parties to build or enhance profiles?**

  The NDPR makes no express distinction. However, it makes a distinction between the data controller and the data processor. It states that data processing by a third party shall be governed by a written contract between the third party and the data controller.[38] Accordingly, any person engaging a third party to process the data obtained from data subjects is required to ensure that that person adheres to the provisions of the NDPR or any other law that provides adequate data protection in their home country in respect of such data.

4.4. Consent and Exceptions to Consent

4.4.1. Overview

As noted in paragraph 1.5.2 above, consent of the data subject must be freely given, specific, informed, and unambiguous. indication of the data subject's wishes by which they, through a statement or a clear affirmative action, signifies agreement to the processing of their data.

Except where an exemption is applicable as described below, personal data can only be collected and processed in accordance with specific, legitimate, and lawful purpose consented to by the data subject. In procuring consent, the

[35] Article 6.2 The Data Framework

[36] Section 22(3) The Proposed Bill

[37] The NDPR also provides that the data subject has an option to object to the processing of Personal Data relating to him which the Data Controller intend to process for the purpose of marketing (Article 2.8(a))

[38] Article 2.7 NDPR

purpose of collection of such data must be made known to the data subject. Additionally, such consent must be obtained in the absence of fraud, coercion, or undue influence.

- **For what types of personal information or purposes of processing is consent required?**

  Consent is required for the processing of all personal identifiable information. However, the NDPR has made provisions for instances where lawful processing can occur without prior consent of the data subject. This exemption is applicable in the following instances:[39]

  a) Where processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract.

  b) Where processing is necessary for compliance with a legal obligation to which the controller is subject.

  c) Processing is necessary in order to protect the vital interests of the data subject or of another natural person.

  d) Processing is necessary for the performance of a task carried out in the public interest or in exercise of official public mandate vested in the controller.

- **How is consent manifested – express consent, implied consent, or opt-out?**

  It is important to state that as a starting point, consent must be given freely, specific, informed, and unambiguous. In addition, consent cannot be bundled i.e., there must be separate data consent request for different types of data use and data class. In this regard, the Data Framework stipulates that:

  a. A request for consent should be prominent, concise, separate from other terms and conditions, and easy to understand, and should include the name of the organization and any third parties, the reason for and the purpose of the data collection, and an explanation that consent may be withdrawn at any time.

  b. Consent should be expressed, or it may be opt-in. Data subjects must be asked to actively opt-in, and the use of pre-ticked boxes, opt-out boxes or default settings is discouraged.

  c. The data processor should keep records evidencing the consent granted and the details of the person granting same.

  d. Data controllers should make it easy for people to withdraw consent at any time they choose.

  e. Details of consent should be kept under review and updated if changes occur.

  f. Build regular reviews into the business processes.[40]

---

[39] Article 2.2 (b-e) NDPR

[40] Article 6.4 of the Data Framework.

- **Does the consent obligation require granularity (i.e., consent for distinct processing activities) similar to GDPR? Or is the consent obligation more generalized (e.g., requiring consumers to opt-in to "online behavioral advertising" more broadly, without having to consent to each constituent processing activity/party)?**

  The Data Framework provides that the data controller must give granular options for obtaining consent separately for different purposes and different types of processing.

- **Can personal information be processed for secondary purposes (i.e., differing purposes from which it was collected)?**

  Yes, but only in very limited circumstances, such as for archiving purposes, the purpose of scientific or historical research, statistical purposes for public interest[41].

- **Are there any rules compelling downstream recipients/processors of personal information to provide additional notices?**

  There appear to be no specific rules compelling downstream recipient/processors of personal information to provide additional notice.

- **Are there any issues concerning the timing of consent?**

  The NDPR provides that consent must be obtained prior to collecting and processing a data subject's personal data.

- **Are there distinct consent requirements for sensitive personal information?**

  The Data Framework

  Under the Data Framework, a specific consent described as a "higher standard consent" is required for the processing of sensitive personal data such as ethnic, political affiliation, religious beliefs, trade union membership, biometric, genetic, sexual orientation, health.[42] The Data Framework does not offer an insight into what connotes a higher standard consent.

  The Proposed Bill

  Under the Proposed Bill, the data subject's consent to processing of sensitive information which relates to religious or philosophical beliefs, ethnic origin, race, political opinions, health, sexual orientation, or behavior of the data subject must be obtained prior to processing. The Proposed Bill also provides that

[41] Article 2.1(1)(a) NDPR

[42] Article 6.2 the Data Framework

where the sensitive information is that of a child under parental or guardian control, the prior consent of the parent or guardian must be obtained before processing.[43]

- **Are there distinct consent requirements for profiling consumers?**

  NDPR

  The NDPR provides that the data controller must inform the data subject of the existence of profiling and provide meaningful information on the logic involved as well as the significance and the envisaged consequences prior to obtaining consent.[44]

  The Proposed Bill

  The Proposed Bill provides that the data controller must inform the data subject of the existence of profiling and the consequences of such profiling and the right to object prior to obtaining consent.[45]

- **Are there distinct consent requirements for automated decision making?**

  The data controller is required to inform the data subject of the existence of automated decision-making (including profiling), the significance and consequences of the processing for the data subject, prior to obtaining consent.[46]

  The Proposed Bill

  The Proposed Bill provides that where a decision which significantly affects a data subject is based solely on automated processing, the data controller shall, as soon as reasonably practicable (a) notify the data subject that the decision was taken on that basis, and (b) the data subject is entitled, by notice in writing to require the data controller to reconsider the decision within 21 days after receipt of the notification from the data controller[47]. This implies that the data subject must be notified of the automated decision making and the data subject's consent first obtained.

- **Are there any age restrictions related to consent? Are there distinct consent requirements around processing children's personal information?**

---

[43] Section 26(1) the Proposed Bill

[44] Article 3.1.(7)(l) NDPR

[45] Section 6.3(i) The Proposed Bill

[46] Article 3.1.(7)(l) NDPR

[47] Section 28 (2) The Proposed Bill

The Data Framework and the NDPR

a. The Data Framework stipulates that in processing the personal data of a child, the consent should be obtained from a data or guardian. For the purposes of the NDPR, a child is any person below the age of 13.[48]

b. The NDPR provides that the data controller has an obligation to ensure that consent of a data subject has been obtained without fraud, coercion, or undue influence, and the data subject has the legal capacity to give consent.[49] The NDPR also states that consent shall not be sought, given, or accepted in any circumstance that may engender direct or indirect propagation of atrocities, hate, child rights violation, criminal acts, and anti-social conducts.[50]

The Proposed Bill

This is seeking to classify the information of any child below 16 as sensitive data.[51] Thus, if passed, a person under 16 may be considered a child from the perspective of data protection regulation. Similarly, it requires that the prior consent of a parent or guardian must be obtained when processing sensitive information of a child.[52] Please note that the Data Protection Bill, being a Bill, is subject to change.

- **Can consent, however manifested, be revoked?**

  Yes, consent can be revoked at any time. Prior to giving consent, the NDPR provides that the data subject must be informed of his right to and method of withdrawing consent at any time, the withdrawal of which does not affect the lawfulness of processing the data based on the consent before its withdrawal.[53]

4.4.2. Application to Digital Advertising

Consent is critical to digital advertising because it is a condition precedent that must be fulfilled or provided prior to processing of personal data to the extent the data is required for digital advertising. The requirement of consent under the NDPR and the Proposed Bill must therefore be complied with.

---

[48] Paragraph 6.2(d), The Data Framework

[49] Article 2.3 (2) NDPR

[50] Article 2.4 (a) NDPR

[51] This is provided for in the definition section

[52] Section 26(1) the Proposed Bill

[53] Article 3.1(7)(i) NDPR

4.5. Appropriate Purposes

4.5.1. Overview

The NDPR provides that personal data shall be:

a) Collected and processed in accordance with specific, legitimate, and lawful purposes consented to by the data subject; provided that further processing may be done only for archiving, scientific research, historical research or statistical purposes for public interest;

b) Adequate, accurate, and without prejudice to the dignity of human persons;

c) Stored only for the period within which it is reasonably needed; and

d) Secured against all foreseeable hazards and breaches such as theft, cyberattack, viral attack, dissemination, manipulations of any kind, damage by rain, fire, or exposure to other natural elements.[54]

4.5.2. Application to Digital Advertising

- **Does the law or legal guidance require a specific legal basis for specific digital advertising activities? Clarify for each activity (suggest using TCF/IAB CCPA "purposes") ("profiling" must be addressed here).**

  The NDPR and the Proposed Bill do not provide for a specific legal basis requirement for specific digital advertising activities.

- **If yes, what are the legal bases (e.g., consent, legitimate interest)? Are there any requirements related to lawful basis (need a valid legal basis to process)/fairness (scope of processing is fair)/transparency (transparent about the processing activity to the consumer and the lawful basis)?**

  N/A

- **Does the law address processing for secondary purposes/differing purposes from which it was collected?**

  The law provides that no data should be obtained except the specific purpose of collection is made known to the data subject.[55]

4.6. Safeguards

4.6.1. Overview

The NDPR provides that any person involved in data processing or in the control of data shall develop security measures to protect data against all foreseeable hazards and breaches such as theft, cyberattack, viral attack,

[54] Article 2.1(1)(d) NDPR

[55] Article 2.3 (1) NDPR

dissemination, manipulations of any kind, damage by rain, fire, or exposure to other natural elements.[56] A data controller is also required to adopt measures including, protecting the data from hackers, storing data securely with access to specific authorized individuals utilizing data encryption technologies, etc.[57]

4.6.2. Application to Digital Advertising

The safeguards contained in the law should be adhered to in the processing of personal data. If such processing involves the transfer of data to a foreign country or an international organization, any extant guidelines or safeguards regulating that transfer should be adhered to, and in the absence of such, the processor or responsible party should adhere to the NDPR's requirements on international transfer of data.

5. DATA SUBJECT RIGHTS/EXEMPTIONS

5.1. Overview

Under the NDPR[58] and the Proposed Bill[59], data subjects rights are summarized into the following:

- Right to be informed of the processing of data.
- Right to complain or send a request to the data controller.
- Right to obtain information about his/her data from the data controller free of charge except as otherwise provided by regulation or public policy.
- Right to know the details of the data controller.
- Right to withdraw consent; right to access his/her personal data.
- Right to data portability.
- Right to data rectification; right to restrict or object the processing of his/her data.
- Right to be informed where his/her data is being processed for additional purposes.
- Right to be informed about the transfer of his/her data to another country.
- Right to complain to relevant authority.

---

[56] Article 2.1 (1) (d) NDPR

[57] Article 2.6 NDPR

[58] Article 3.1 NDPR

[59] Part 5 (Section 17 – 25)

- Right to data deletion.
- Right to judicial remedy if these rights are violated.

5.2. Access

Yes, the NDPR provides for the right of access. Prior to collecting personal data, the controller has an obligation to inform the data subject of the data subject's right to request for access to its personal data for rectification, erasure, restriction of or objection to processing, as well as the right to data portability.[60]

5.3. Rectify

Data subjects have the right to the rectification of inaccurate personal data. The NDPR also gives the data subject the right to have incomplete personal data completed, including by means of providing a supplementary statement.[61] The NDPR does not stipulate a timeframe within which this should be done, rather, it provides that it shall be done without "undue delay."

The Proposed Bill provides the data subject has the right to the rectification, blockage, or erasure of inaccurate, false, or unlawfully processed personal data without delay and free of charge from the data controller.[62]

5.4. Deletion/Erasure

Data subjects have the right to the deletion or erasure of their data, and same must be deleted "without delay" by the data controller. In the event the personal data has been made public, the data controller is obliged to delete the personal data and take all reasonable steps to inform controllers processing the personal data of the data subject's request.[63]

5.5. Restriction on Processing

Data subjects have the right to obtain from the controller restriction of processing where one of the following

applies: a) the accuracy of the personal data is contested by the data subject for a period enabling the controller to verify the accuracy of the personal data; b) the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise

[60] Article 3.1 (7)(h) NDPR

[61] Article 3.1 (8) NDPR

[62] Section 20(1) The Proposed Bill

[63] Article 3.1 (10) NDPR

or defense of legal claims; and d) the data subject has objected to processing, pending the verification whether the legitimate grounds of the controller override those of the data subject.[64]

5.6. Data Portability

The NDPR provides that a data subject has the right to data portability and in exercising that right, the data subject can have the personal data transmitted directly from one controller to another, where technically feasible. Provided that this right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.[65] The NDPR does not stipulate a timeframe.

The Proposed Bill also provides for the right to data portability.[66]

5.7. Right to Object

The NDPR gives a data subject the right to object to processing of its personal data.[67]

The Proposed Bill also provides that a data subject has the right to object at any time, on grounds relating to the processing of personal data, including profiling for the purposes of direct marketing at any time and at no cost.[68]

5.8. Right Against Automated Decision-Making

A data subject is expected to receive its personal data provided to a controller, in a structured, commonly used, and machine-readable format. The subject also has the right to transmit the data to another controller without hindrance from the controller to which the personal data have been provided, where:(a) the processing is based on consent, or (b) on a contract, and (c) the processing is carried out by automated means.[69]

5.9. Responding to Consumer Rights Requests

In responding to consumer rights requests, the data controller is required to address the data subject in a concise, transparent, intelligible, and easily accessible form, using clear and plain language either in writing and where appropriate, by electronic means or when requested by the data subjects, orally.[70]

---

[64] Article 3.1 (11) NDPR

[65] Article 3.1 (15) NDPR

[66] Section 25, The Proposed Bill

[67] Article 3.1 (7)(h) NDPR

[68] Section 22(1-2) the Proposed Bill

[69] Article 3.1 (14) NDPR

[70] Article 3.1 (1) NDPR

5.10. Record Keeping Concerning Rights Requests

The NDPR does not provide an explicit timeframe for retention of rights requests. Rather, it gives a general guideline for data controllers and processors to utilize where this issue is not regulated by contract.

5.11. Is Providing Consumers with these Rights Required by Law or Mere Suggestions?

They are required by law.

5.12. Application to Digital Advertising

Digital marketers and advertisers should be aware of the data subject's rights and their obligations towards a data subject. The NDPR provides that the consent of a data subject must be sought and obtained before the data subject's personal data are passed unto a third party.[71] Data processing by a third party shall be governed by a written contract between the third party and the data controller and any person engaging a third party to process the data obtained from the data subject is required to ensure adherence to the provisions of the Law in this regard.[72]

6. DATA CONTROLLER AND PROCESSOR AGREEMENTS

6.1. Overview

A data controller and processor have a duty to take reasonable measures to ensure that a party to a data processing contract (other than the data subject) does not have a record of violating the rights of a data subject.[73]

Moreover, every data controller and processor shall be liable for the actions or inactions of third parties which handle the personal data of data subjects under the NDPR.

6.2. Data Controller Outsourcing of Processing

There must be a written contract between the data controller and the data processor where there is an outsourcing of data processing.[74]

---

[71] Article 2.3 (2)(e) NDPR

[72] Article 2.7 NDPR

[73] Article 2.4(b) of the NDPR

[74] Article 2.7 of the NDPR

The Proposed Bill provides that the agreement between the data controller and processor must set out the nature of the processing agreement, the personal data to be processed, the purpose of processing, the obligations and restrictions imposed on the data processor and the penalties for breach.[75] In addition, the data controller must ensure that there is adherence to the NDPR where there is an outsourcing of data processing to a third party.

The data controller is vicariously liable for the processing of the data by the data processor.[76]

6.3. Data Processor Rights and Responsibilities

The duties of a data processor include to:

- Process personal data on behalf of a data controller only on the written instructions of the data controller.
- Not engage another data processor without the prior written authorization of the data controller.
- Inform the data controller of changes concerning the addition or replacement of data processors.
- Inform the data controller of any legal requirement that may create risks to the rights and fundamental freedoms of data subjects, unless the law prohibits such notice.
- Take appropriate technical and managerial security measures pursuant to Section 34 of the Proposed Bill.
- Assist the data controller by putting in place the appropriate technical and managerial measures for the fulfilment of the data controller's obligations to respond to the rights under the Proposed Bill.
- Assist the data controller in ensuring compliance with its security obligations, including security breach notification.
- At the request of the data controller, delete or return all personal data to the data controller at the end of the provision of services, and delete any copies of personal data unless prohibited by law.
- Make available to the data controller all information necessary to assist the data controller demonstrate compliance with its obligations under this Act and facilitate audits conducted by the data controller or a third-party auditor determined by the data controller[77]

A data processor must ensure continuous capacity building for its data protection officers and the generality of its personnel involved in any form of data processing.[78]

---

[75] Section 31(3) of the Proposed Bill

[76] Section 31 of the Proposed Bill

[77] Section 32(1) of the Proposed Bill

[78] Article 4.1(3) of the NDPR

6.4. Application to Digital Advertising

These provisions apply to digital advertising most especially where there is cross border transfer of the data of the data subject to a data processor for determining the kind of advert that should be directed to the data subject (target marketing using data subject's preferences). In such instance, the data controller is expected to execute an agreement with the data processor and further ensure that there is full compliance with the provisions of the NDPR and the Proposed Bill.

7. DATA TRANSFER & OUTSOURCING

7.1. Overview

The transfer of data to foreign country falls under the supervision of the Honorable Attorney General of Federation ('AGF').[79] For data to be transferrable, the foreign country or the international organization must ensure an adequate level of protection, as determined by NITDA and the AGF. In determining the adequacy of a third country or organization, the following considerations will be borne in mind:

- The legal system of the foreign country notably as it relates to human rights protection, rule of law and relevant legislation.
- Implementation of such legislation.
- The existence and effectiveness of an independent supervisory authority in the foreign country or to which an international organization is subject responsible for compliance with data protection, assisting and advising the data subjects in exercising their rights and for cooperation with the relevant authorities Nigeria.
- The commitments of the foreign country or international organization to data protection through conventions, instruments, and participation in multilateral or regional systems.

The exceptions to the above requirements are:

- Where the data subject consents after being informed of the risk.
- Where the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request.
- Where the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; where the

[79] Article 2.11 of the NDPR

transfer is necessary for important reasons of public interest.

- Where the transfer is necessary for the establishment, exercise or defense of legal claims.
- Where the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.[80]

The data subject must be made aware of possible violation of his rights in the foreign country.

The Proposed Bill[81] sets out conditions for the transfer of personal data abroad, including mechanisms such as an adequacy assessment, ad-hoc or standardized safeguards, explicit data subject consent, prevailing data subject interests, and legitimate interests. The Data Protection Commission (Commission) would also have the authority to request information on transfers and that organizations evidence appropriate safeguards, as well as to prohibit transfers and to regulate onward data transfers beyond the initial recipient.

Where a public institution seeks to process the personal data of Nigerians from another public institution, private entity or an international organization, the following must be demonstrated:

- Compliance with international information security standards such as ISO 27001:2013 or any similar standard.
- Compliance with the provisions of the NDPR.
- Conduct of a Data Protection Impact Assessment and submission of same to NITDA.
- Retention of a Data Protection Compliance Organization (DPCO) to guide it in the use of the personal data and for compliance purposes.[82]

7.2. Application to Digital Advertising

Where there is an outsourcing of data for digital advertising purposes, the above mentioned considerations provided in the NDPR and the Proposed Bill (if eventually passed into law) are applicable and as such must be complied with so as to guarantee the security of the data being transferred. The consent of the data subject will be required at all instances (that is, where NITDA under the supervision of the AGF has decided that the recipient's location or territory has some level of protection for the data of the data subject or where there is no

[80] Article 2.12 of the NDPR

[81] Part X.

[82] Section 2.6 of the Guidelines

such decision from NITDA) where his personal data is to be outsourced. The NDPR[83] and Proposed Bill[84] requires disclosure of either the recipients or categories of recipients of personal data. The use of coordinating conjunction 'or' implies either the specific identity of the recipient or categories of recipients, if any, should be made known to the data subject(s). Therefore, we can rightly conclude that the disclosure of categories of recipients will suffice if there are such categories otherwise, specific disclosure is required.

8. AUDIT/ACCOUNTABILITY

8.1. Overview

The NDPR mandates every organization whether public or private in control of data of natural persons to carry out privacy and data protection compliance audit annually. All public or private organizations in Nigeria that control data of natural persons must within three (3) months after the date of the issuance of the regulation make available to the general public their respective data protection policies which must be in accordance with the NDPR.[85]
Where a Data Controller processes the personal data of more than 1000 in a period of six months, a soft copy of the summary of the audit containing information in Article 4.1(5) of the NDPR shall be submitted to NITDA[86] and where the processed personal data is more than 2000 in a period of 12 months, a summary of the data protection audit containing the information shall be submitted to NITDA not later than 15th of March of the following year.
The content of the audit report which includes:

i. The personally identifiable information the organization collects on employees of the organization and members of the public.
ii. Any purpose for which the personally identifiable information is collected.
iii. Any notice given to individuals regarding the collection and use of personal information relating to that individual.
iv. Any access given to individuals to review, amend, correct, supplement, or delete personal information relating to that individual.
v. Whether or not consent is obtained from an individual before personally identifiable information is collected, used, transferred, or disclosed, and any method used to obtain consent.

[83] Article 3.1 (7)(e) NDPR

[84] Section 6(3)(e) Proposed Bill

[85] Article 4.1 of the NDPR

[86] Article 4.1.6 and 4.1.7 of NDPR

vi. The policies and practices of the organization for the security of personally identifiable information.

vii. The policies and practices of the organization for the proper use of personally identifiable information.

viii. Organization policies and procedures for privacy and data protection.

ix. The policies and procedures of the organization for monitoring and reporting violations of privacy and data protection policies.

x. The policies and procedures of the organization for assessing the impact of technologies on the stated privacy and security policies.[87]

Furthermore, every data controller or processor shall not later than 30th March of the following year, submit a report of its data protection audit to the Commission.[88] The Commission shall compile and publish an annual report containing the list of organizations who have submitted the audit report. It is instructive to note that the Commission has the power to impose administrative fines or sanction where data controllers and data processers infringe any provisions of the Bill.[89]

Furthermore, Paragraph 3.2(viii) of NDPR Implementation Framework imposes on the controller or processor the duty to conduct a Data Protection Impact Assessment ('DPIA') in accordance with the provisions of the NDPR (A DPIA is a process to identify, evaluate and minimize possible data protection risks in an existing or new business or organizational activity. Where the organization intends to embark on a project that would involve the intense use of personal data, a DPIA should be conducted to identify possible areas where breaches may occur and devise a means of addressing such risks. Organizations are expected to conduct a DPIA on their processes, services, and technology periodically to ensure continuous compliance).

8.2. Application to Digital Advertising

Digital advertising by virtue of using cookies and similar technologies to collect individuals' personal data makes it fall under the purview of these regulations, Framework, and the Proposed Bill. Therefore, data controllers that engage in digital advertising are also required to comply with the relevant sections of the Regulations, Framework, and Proposed Bill by carrying out periodic audits and submitting same to the relevant agencies.

[87] Article 4.1(5) of the NDPR

[88] Section 2(5) of the Proposed Bill

[89] Section 9 (e)(v) of the Proposed Bill

9. DATA RETENTION

9.1. Overview

Under Nigerian law, there are no restrictions on cookie retention or the use of similar technology to obtain data from the data subject, provided that the consent of the data subject is obtained. Such data must be processed for specific, legitimate, and lawful purpose. However, the data subject has the right to request the controller to delete the personal data without delay and the controller must delete personal data where:

- The personal data are no longer necessary in relation to the purpose for which they were collected or processed.
- The data subject withdraws consent on which the processing is based.
- The data subject objects to the processing and there are no overriding legitimate grounds for the processing.
- The personal data have been unlawfully processed.
- The personal data have to be erased for compliance with a legal obligation in Nigeria.[90]

Furthermore, the data subject also has the right to restrict the processing of his personal data, where:

- The accuracy of personal data is contested.
- The processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of its use.
- The data controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise, or defense of legal claims.
- The data subject has objected to processing pending a verification on whether the legitimate grounds of the controller override those of the data subject.[91]

A service provider shall keep all traffic data and subscriber information as may be prescribed by the relevant authority (responsible for the regulation of communication services in Nigeria), for the time being for a period of two (2) years.[92]

---

[90] Article 3.1(9) of the NDPR

[91] Article 3.1(11) of the NDPR

[92] Section 38(1) of the Cybercrimes Act

Non-compliance with the Cybercrimes Act is an offence, punishable upon conviction with imprisonment for a term of not more than three (3) years or fine of not more than NGN 7 million (approx. €15,470).[93]

Also, the Proposed Bill empowers data subjects with the right to have their personal data blocked or erased where it is inaccurate, false, or unlawfully processed, and transmit his data to another data controller provided it is not contrary to public interest or will affect the rights and freedom of others.[94]

Every Data Controller Report shall specify the duration of storage clearly in its terms of service or other binding document. Where retention of personal data is not provided by applicable law or agreement between the parties, the retention period shall be:

a) Three (3) years after the last active use of a digital platform;
b) Six (6) years after the last transaction in a contractual agreement;
c) Upon presentation of evidence of death by a deceased relative;
d) Immediately upon request by the data subject or his/her legal guardian where: (i) no statutory provision provides otherwise; and (ii) the data subject is not the subject of an investigation or suit that may require the personal data sought to be deleted.[95]

Personal data which are not in use or which have exceeded the statutory required period are to be destroyed by the data controller in line with global best practices.[96]

9.2. Application to Digital Advertising

The NDPR does not explicitly impose a period for the retention of personal data. However, it is advised that data controllers state the retention period in their privacy policy. Where the retention period is not provided in any contractual agreement or any applicable law, the retention period will be determined by Paragraph 8 of Implementation Framework as reproduced above.

[93] Section 38(6) of the Cybercrimes Act

[94] Sections 20 and 25 of the Proposed Bill

[95] Section 8 of the Data Framework

[96] Section 8.3 of the Data Framework

10. DATA PROTECTION AUTHORITY | REGULATORY AUTHORITY

10.1. Overview

There is currently no central regulatory body for data protection apart from NITDA and other sectoral bodies.

10.2. Main Regulator for Data Protection

At the moment, there is no specific regulator for data protection in Nigeria. Thus, the regulatory body for each sector has been responsible for protecting data. For instance, the Central Bank of Nigeria (CBN) oversees matters relating to protecting financial data; the NCC regulates data collected or processed by internet service providers and telecommunications companies.

Moreover, under the NDPR, NITDA can set up an administrative redress panel to investigate breach of the NDPR and issue administrative orders.

As mentioned above, the Proposed Bill seeks to establish the Commission, which would be responsible for data protection in Nigeria.

10.3. Main Powers, Duties, and Responsibilities

If the Proposed Bill is passed into law, the Commission will exercise regulatory powers.

The functions of the Commission are to:

- Protect the personal data and privacy of data subjects by regulating the processing of personal information.
- Provide the process to obtain, store, process, use, or disclose personal information.
- Ensure that data controllers and data processors adhere to the data protection principles as provided for by the Proposed Bill in order to protect the fundamental rights and freedoms, particularly privacy of natural persons in relation to the processing of their personal data.
- Assist the facilitation of the free flow of personal data through consultation and cooperation with other relevant agencies in compliance with established data security best practices.
- Act as the supervisory authority, and exercise regulatory, powers to:
    - Advise and approve risk management processes and systems for data controllers and data processors to ensure compliance with the provisions of the Proposed Bill.

- Issue directives in the event that their operations are likely to infringe the provisions of the Proposed Bill.
- Receive and process complaints from data subjects whose rights have been infringed.
- Order the rectification, completion, or deletion of personal data and impose a temporary or definitive limitation, including a ban, on processing operations.
- Impose administrative fines or sanctions where data controllers and data processors infringe any provision of the Proposed Bill.

- Act with complete independence and impartiality in performing its functions and exercising its powers.
- Promote public awareness of the rights of data subjects and the exercise of their rights and shall inform data controllers and data processors of their duties and responsibilities and shall share best practices in order to ensure the free flow of personal data.
- Be consulted on proposals for any legislative or administrative measures which relate to the processing of personal data.
- Provide relevant regulations, guidelines, and policies relating to transfers of personal data provided for under the Proposed Bill, or any other legislation.
- Make regulations for the licensing and certification of data protection compliance officers and organizations.
- Muster the resources necessary for the effective performance of its functions and the exercise of its powers.
- Prepare and publish its reports annually, outlining its activities which shall be submitted to the President.[97]

10.4. Application to Digital Advertising

The regulatory authority for digital advertising in Nigeria is Advertising Practitioners Council of Nigeria (APCON), NITDA and NCC. The Data Protection Commission in the Proposed Bill will also regulate digital advertising upon being signed into the law.

[97] Section 9 of the Proposed Bill

11. SANCTIONS

11.1. Overview

Advertising in Nigeria is regulated by a combination of federal laws, state laws, subsidiary legislation, and guidelines. Violations of the relevant laws which protect privacy of users using cookies and other technologies attract the following penalties. There are, however, legal restrictions which either legislation or regulatory requirements have imposed on service providers when advertising their products to consumers. Any breach of such provisions would attract sanctions which may be in the form of fines or a ban from advertising the product whether temporarily or permanently.

11.2. Liability

The NDPR provides that any person who is found to be in breach of the data privacy rights of any data subject must be liable, in addition to any other criminal liability, to the following[98]:

i. Payment of a net of 2% of annual gross revenue of the preceding year or payment of the sum of NGN 10 million (approx. €23,000), whichever is higher, where the data controller is dealing with more than 10,000 data subjects.

ii. Payment of a net of 1% of the annual gross revenue of the preceding year or payment of the sum of NGN 2 million (approx. €4,600) whichever is higher, where the data controller is dealing with fewer than 10,000 data subjects.

Thus, the penalties are determined based on the number of users or data subjects whose data are being processed by the data controller, irrespective of the actual number of users who are affected by the breach.

In the same vein, the NCC Consumer Code of Practice also prescribes administrative penalties to operators which fail to adopt a policy with regards to the collection, use, and protection of consumer information. In determining the penalties, the NCC must take cognizance of the following considerations, among others[99]:

- The severity of the contravention and the need to impose such net or the amount thereof to serve as a deterrent to both the person who committed such contravention and other persons.
- Non-discriminatory and transparency in the imposition of sanctions, generally including but not limited to sanctions on different persons for similar contraventions committed in identical circumstances.
- The prevalence of the contravention in the industry generally and the likelihood of repetition by the person who committed the contravention or other persons.

---

[98] Article 2.10 of the NDPR

[99] Section 15 of the NCC (Enforcement Process, etc.) Regulations, 2019

- The duration of the contravention.
- The circumstances of the contravention and in particular, but not limited to, a consideration of whether the contravention was deliberately, recklessly, or negligently committed.

Criminal Penalties

There is an obligation on service providers to protect individuals' rights to privacy under the Constitution and take appropriate measures to safeguard the confidentiality of the data retained, processed, or retrieved for the purpose of law enforcement.[100] A breach of this provision is punishable upon conviction to imprisonment for a term of not more than three years or a fine of not more than NGN 7 million (approx. €16,100), or to both fine and imprisonment.

The CRA created different categories of penalties for offences. However, of particular interest is the provision that any person who contravenes the provision of section 20 (b)-(i) of the CRA (which include intentionally or negligently disclosing credit information in contravention of the provision of the law) must be liable on conviction to a net not less than NGN 10 million (approx. €23,000).[101]

- **Scope of liability for publishers and advertisers for processing activities of ad-tech companies:**

  The APCON mandates prior submission of exposure drafts of all advertisements required to be published online and on other social media platforms for approval by the ASP in compliance with Article 21 and 80(a) of the Nigerian Code of Advertising upon the payment of the sum of NGN25,000 (approximately USD70) per application, failure to do so results in liability in the form of fines as determined by APCON.

- **Scope of liability for ad-tech companies for collection activities of publishers and advertisers:**

  Where the ad-tech company is a network operator, the NCC Consumer Code of Practice prescribes administrative penalties to operators which fail to adopt a policy with regards to the collection, use, and protection of consumer information.

- **Scope of liability for ad-tech companies for other ad-tech companies they enable to process data (either because they make the decision of publishers or advertisers or agency dictates it).**

  There is no express provision under the laws stipulating any form of liability for ad-tech companies for other ad-tech companies they enable to process data. However, Under the NCC Consumer Code of Practice, an ad-tech company that is a licensee may collect and maintain information on individual consumers reasonably required for its business purposes. However, the collection and maintenance of information on individual consumers shall not be transferred to a third party except as permitted by any

[100] Section 38(5) and (6) of the CRA

[101] Section 21(2) of the CRA

terms and conditions agreed with the consumer, as permitted by any permission or approval of the General Principles Commission, or as otherwise permitted or required by other applicable laws or regulations.

11.3. Enforcement and Market Practice

- **How are claims raised under the law?**

  Claims are raised by filing an originating application with the accompanying documents in court. In the case of a cybercrime, the action is instituted by a charge brought before the Federal High Court. Further, the NDPR, 2019 also sets up an administrative redress panel to investigate and determine any disputes arising from the Regulation.

- **Who enforces them?**

  The enforcing body would depend on where the claim is raised. If it raised with the court, then the court would enforce. In the instance that a claim is made with the administrative redress panel of the NDPR, then the panel would be responsible for its enforcement.

- **What is their practice? (Quietly working with companies to fix, publicly coming out with large investigations? Fact specific?)**

  Generally, court proceedings are open and accessible to the public. However, the administrative redress panel may employ any means they find expedient in the resolution of the claim, be it working with the companies to fix or public hearings.

- **What up to date guidance has there been on how to handle requirements in the ad ecosystem? Have the regulators been educated on how the ecosystem operates? Have compliance regimes been discussed with them? Has their feedback been solicited?**

  As far as regulators' education and feedback goes, the APCON, the regulatory agency setup by statute as well as other APCON recognized agencies such as The Advertisers Association of Nigeria (ADVAN), Association of Advertising Agencies of Nigeria (AAAN), Outdoor Advertising Agency of Nigeria (OAAN) etc., are in the practice of organizing training seminars and workshops to educate advertisers, content publishers, media owners, agencies, regulators etc. in the public and private sector organization.

  The APCON also conduct stakeholders' forum, where stakeholders in the advertising industry are allowed to air their views about key issues of concerns and then proffer solutions.

11.4 Remedies

Given that privacy rights are guaranteed and protected under Section 37 of the Constitution, an action can be commenced against the provider of digital services using cookies through the Fundamental Rights (Enforcement Procedure) Rules, 2009, where the same is in breach of the user's privacy rights. The NDPR, 2019 also guarantees and protects data privacy rights and the remedies available include:

1. In the case of a Data Controller dealing with more than 10,000 Data Subjects, payment of the fine of 2% of Annual Gross Revenue of the preceding year or payment of the sum of 10 million naira whichever is greater.
2. In the case of a Data Controller dealing with less than 10,000 Data Subjects, payment of the fine of 1% of the Annual Gross Revenue of the preceding year or payment of the sum of 2 million naira whichever is greater.

11.5. Private Right of Action

An individual whose right to privacy has a right of action for infringement of this right as is guaranteed and enshrined in the 1999 constitution of the Federal Republic of Nigeria.

11.6. Digital Advertising Liability Issues

The Advertising Practitioners (Registration, Etc.) Act which provides the statutory framework for the regulation of advertising practitioners and creates APCON makes no express provision for liability issues in digital advertising. However, the liability issues examined in paragraph 11.2 of the NDPR and NCC consumer code of Practice would be applicable where the issues arise as a result of breach of data privacy rights or the collection, use, and protection of consumer information.

11.7. Application to Digital Advertising

The principal law governing advertising in Nigeria is the APCON Act. The APCON Act, which was promulgated about 31 years ago, provides the statutory framework for the regulation of advertisements and advertising practitioners. The APCON Act further established the APCON as the apex regulatory body for advertising in Nigeria with powers to monitor and ensure ethical advertising practices in the country. The APCON Act empowered APCON to establish the Advertising Standards Panel **(ASP)** charged with the duty of ensuring that advertorial contents conform with the prevailing Laws of the Federation, as well as the codes of ethics of the advertising profession.[102]

Digital advertising essentially involves the delivery of advertorial contents to Internet/online users via web, e-mail, ad-supported software, and Internet-enabled smartphones.

However, the disruption in the digital advertising landscape in Nigeria has lowered the barrier for participation—taking advertising out of the exclusive reserve of licensed advertising agencies and creating a levelled field for anyone who has an internet-enabled device to disseminate advertising content to the public. This may result in an aggressive market where consumers are bombarded with false, suspicious, embellished, offensive, and many times unsolicited content.

[102] Section 23 of the Act

In 2013, APCON approved and issued the 5th Nigerian Code of Advertising Practice & Sales Promotion (the "Code"). The Code requires all advertising contents be vetted by the ASP prior to being exposed to the public. This rule however made no distinction between online or offline advertising contents.

It must also be noted that the APCON vetting process, is only open and applicable to advertising practitioners[103], suggesting that non-practitioners (who make up a critical mass of online advertisers) are exempt from this regulation.

For instance, if an individual advertises hair product for women (Brazilian hair) on an online platform (such as Instagram or Twitter) and such an individual (not being a "regulated person" does not seek approval from APCON or other regulator, Apparently, the APCON Act did not specifically describe who an advertising practitioner should be. This is a massive loophole because any individual can decide to advertise any product and with the current standing of the law, APCON will not be legally bound to carry out enforcement actions against such individual.

12. NOTIFICATION | CERTIFICATION | REGISTRATION

12.1. Overview

The NDPR does not mandate registration or notification of processing activities of businesses with NITDA. It does however specify that data controllers submit a data protection audit to NITDA if they process the data of more than 1,000 data subjects (in six months) or more than 2,000 data subjects (in 12 months).

12.2. Requirements and Brief Description

Any person or institution who operates system or a network, whether public or private, must immediately inform the Nigeria Computer Emergency Response Team (ngCERT) of any stacks, intrusions, and other disruptions liable to hinder the functioning of another computer system or network, so that ngCERT can take necessary measures to tackle the issues.[104]

Any person or institution who fails to report any such incident to ngCERT within seven days of its occurrence, commits an offence and shall be liable to denial of internet services. Such persons or institutions shall, in addition, pay a mandatory sum of NGN 2 million (approx. €4,430) into the National Cyber Security Fund.[105]

---

[103] Article 6.2 and 7.1, APCON Vetting Guidelines

[104] Section 21(1) of the Cybercrimes Act

[105] Section 21(3) of the Cybercrimes Actt

A data subject has the right to be notified of a data breach affecting him or her within 48 hours after notification to the Commission.[106]

12.3. Application to Digital Advertising

The Advertising Standards Panel (ASP), a statutory committee of the Advertising Practitioners Council of Nigeria (APCON) in 2019, directed that all communication material, regardless of the medium, digital or otherwise, must first be submitted and duly vetted by the APCON before such content is exposed to the public.

13. DATA PROTECTION OFFICER

13.1. Overview

The Data Protection Officer function overlooks data protection compliance in an organization. The DPO maintains records of processing of personal data, takes lead in developing data protection and related policy and procedures. The DPO becomes a bridge between related disciplines, such as data protection, IT, audit, compliance, legal and security, analyzing how the results of data protection schemes may impact the organization.

13.2. Data Protection Officer (DPO) – Compulsory Appointment (Yes/No)

Yes. Both data controller and processor are required to appoint a DPO. A data controller or processor can also outsource to a verifiably competent firm or person.

13.3. Requirements

There are no specific requirements by law in this regard. However, DPOs are usually expected to have verifiable competence usually in the form of certification or training in data protection, security, and privacy. The data controller or processor must ensure continuous capacity building for its DPO, and its personnel involved in any form of data processing.

13.4. Application to Digital Advertising

Given that digital advertisement transcends beyond jurisdictional boundaries and as such, it is difficult to regulate, there is a lack of legislation in Nigeria as regards it. Consequently, there is no provision as to the necessity of a DPO in digital advertising.

[106] Section 17(3) of the Bill

14. SELF-REGULATION

14.1. Overview

Are there any industry self-regulatory schemes in place in the jurisdiction?

In Nigeria, there are no industry self-regulatory schemes in place. All monitoring of adherence to legal, ethical, or safety standards are done by the APCON and any other government designated bodies.

Are there any signal-based programs used in the territory to assist with digital advertising compliance?

There are no signal-based programs used in the territory to assist with digital advertising compliance in Nigeria.

14.2. Application to Digital Advertising

Given that digital advertising and ad-tech remains largely unregulated, there is no system of industry self-regulation in Nigeria.

iab.

Singapore

Cross-Jurisdiction
Privacy Project

1. THE LAW

1.1. Overview & Key Acts, Regulations, and Directives

The Personal Data Protection Act 2012 (No. 26 of 2012) ('PDPA') is the principal data protection legislation in Singapore. It governs the collection, use, and disclosure of individuals' personal data by organizations in a \manner that recognizes both the right of individuals to protect their personal data, and the need of organizations to collect, use, and disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances. The PDPA is administered and enforced by Singapore's national data protection authority, the Personal Data Protection Commission ('PDPC').

In recent years, there has been a general push by the PDPC towards a culture of accountability on the part of organizations in relation to the protection of personal data. For example, the PDPC implemented the Data Protection Trustmark Certification in 2019, which is a voluntary enterprise-wide certification program for organizations to demonstrate accountable data protection practices and compliance with the PDPA.

Development of the PDPA

Prior to the enactment of the PDPA, Singapore did not have an overarching law governing the protection of personal data. Rather, the processing of personal data in Singapore was regulated to a certain extent by a patchwork of laws including, common law, sector-specific legislation and various self-regulatory or co-regulatory codes. These existing sector-specific data protection frameworks continue to operate alongside the PDPA at present.

The PDPA was passed by the Parliament on October 15, 2012, and was implemented in three phases. The first phase, which came into effect on January 2, 2013, included provisions relating to the scope and interpretation of the PDPA; the establishment of the PDPC; the establishment of the Data Protection Advisory Committee; the establishment of the national Do-Not-Call ('DNC') Registry, and other general provisions of the PDPA. The second phase saw the provisions relating to organizations' DNC obligations come into force on January 2, 2014. The third and final phase saw the provisions relating to the protection of personal data come into force on July 2, 2014.

Recent Amendments to the PDPA

The PDPA had recently undergone its first comprehensive revision since its enactment in 2012 under the Personal Data Protection (Amendment) Act 2020 ('Amendment Act'), which was passed in the Parliament of Singapore ('the Parliament') on November 2, 2020. Most provisions of the Amendment Act (except for those noted below) came into force on February 1, 2021. The remaining amendments will come into force on a date appointed by notification in the Government Gazette ('the Gazette') which is likely to be in early 2022.

The Act seeks to amend the PDPA for the following main purposes:

- Strengthen the accountability of organizations in respect of the handling and processing of personal data.
- Enhance the legal framework for the collection, use, and disclosure of personal data.
- Provide individuals with greater autonomy over their personal data.
- Enhance the enforcement powers of the PDPC.

Several significant changes have been made under the Amendment Act. These include:

- An enhanced consent framework, which allows for the collection, use and disclosure of personal data under a number of new bases (new deemed consent and exceptions to consent provisions).
- Mandatory data breach notification and new offences aimed at strengthening accountability for protection of personal data.
- A new data portability obligation (not yet in force).
- Enhanced enforcement powers for the PDPA, including an increase in the maximum financial penalty which may be imposed for contraventions, of up to 10% of an organization's annual turnover in Singapore, or SGD 1 million (approx. €617,600), whichever is higher (the increased financial penalty is not yet in force).

Significant amendments under the Amendment Act are considered in greater detail below.

PDPA Regulations

In addition to the PDPA, the following subsidiary legislation has been promulgated. An asterisk is included with respect to those that may be relevant to digital advertising:

- Personal Data Protection Regulations 2021 ('the PDP Regulations')*.
- Personal Data Protection (Appeal) Regulations 2015.
- Personal Data Protection (Composition of Offences) Regulations 2021.
- Personal Data Protection (Do Not Call Registry) Regulations 2013.
- Personal Data Protection (Enforcement) Regulations 2021.
- Personal Data Protection (Notification of Data Breaches) Regulations 2021.
- Personal Data Protection (Exemption from Section 43) Order 2013 ('the Exemption Order').
- Personal Data Protection (Prescribed Healthcare Bodies) Notification 2015.
- Personal Data Protection (Prescribed Law Enforcement Agencies) Notification 2014.

- Personal Data Protection (Prescribed Law Enforcement Agency) Notification 2020.
- Personal Data Protection (Statutory Bodies) Notification 2013.

Other Laws and Regulations

The PDPA sets a baseline standard for personal data protection across the private sector and will operate alongside (and not override) existing laws and regulations. The PDPA provides that the data protection framework under the PDPA does not affect any right or obligation under the law, and that in the event of any inconsistency, the provisions of other written laws will prevail. For example, the banking secrecy provisions under Banking Act (Cap. 19) that govern customer information obtained by banks would prevail over the PDPA in the event of any inconsistency.

Apart from the PDPA, other laws and regulations that might govern digital advertising include:

- The Consumer Protection (Fair Trading) Act (Cap. 52A) ('CPFTA'), which was enacted to protect consumers against unfair practices and to give them additional rights in respect of goods that do not conform to contract.
- The Spam Control Act (Cap. 311A) ('SCA'), which was enacted to control email and mobile spam in Singapore.

In addition, the Advertising Standards Authority of Singapore ('ASAS') published a Code of Advertising Practice ('SCAP') and Guidelines on Interactive Marketing Communication and Social Media ('Interactive Marketing Guidelines'). For avoidance of doubt, the ASAS is a non-profit organization and is not part of the Singapore government. In addition, the SCAP and the Interactive Marketing Guidelines do not have legal force, but rather, are intended for industry self-regulation.

We also note that there are also sector-specific laws and regulations that would concern advertisements (including digital advertisements) within those sectors. For example, advertisements of therapeutic and medicinal products are governed by and subject to the restrictions under the Health Products (Advertisement of Therapeutic Products) Regulations and the Medicines (Medical Advertisements) Regulations, respectively.

1.2. Guidelines

The PDPC issued several advisory guidelines that provide clarity on the interpretation of the PDPA. Notably, these include (a) the Advisory Guidelines on Key Concepts in the Personal Data Protection Act ('the Key Concept Guidelines'); and (b) the Advisory Guidelines on the Personal Data Protection Act for Selected Topics ('the Selected Topics Guidelines'). These guidelines have recently been amended to address the requirements of the Amendment Act.

The PDPC also issued several guides that address practical topics relating to the PDPA and data protection

management and compliance generally. Of particular relevance in the context of online activities is the Guide to Notification.

All advisory guidelines and guides are accessible via the PDPC's website.

1.3. Case Law

Since 2016, the PDPC has released a series of enforcement decisions that help illustrate how the PDPA is applied. These enforcement decisions are generally accessible via the PDPC's website. To date, there have been no cases specifically relating to digital advertising.

As of December 30, 2020, the PDPC issued a total of 173 published grounds of decisions or summaries of grounds of decisions, with a significant majority of these cases relating to breaches of the obligation to implement reasonable security arrangements to protect personal data (referred to below as the Protection Obligation). The most common types of data breaches involve inadvertent disclosure of personal data, poor technical security arrangements, poor physical security arrangements, errors in mass email and/or post, and insufficient data protection policies. The following is an overview of two significant enforcement decisions.

To date, the highest financial penalties that the PDPC has imposed on organizations are SGD 250,000 (approx. €166,260) and SGD 750,000 (approx. €498,790) respectively on SingHealth Services Pte Ltd and Integrated Health Information Systems Pte Ltd, for breaching their data protection obligations under the PDPA. (See *Re Singapore Health Services Pte Ltd and another [2019] SGPDPC 3*). This unprecedented data breach which arose from a cyber-attack on SingHealth's patient database system caused the personal data of some 1.5 million patients to be compromised.

In the case of *Re Bud Cosmetics Pte Ltd* [2019] SGPDPC 1, the PDPC found that the organization had breached the Protection Obligation, as well as obligations relating to implementing policies and practices and overseas transfers of personal data (referred to below as the Accountability Obligation and Transfer Limitation Obligation respectively). In that case, the organization had collected customer information for membership registration and maintained databases online, so that it could send its customers e-newsletters with information about its products, as part of its marketing strategy. The PDPC found that a list of the organization's customers who had signed-up as the organization's members, and which contained the names, dates of birth, contact numbers, email addresses, and residential addresses of approximately 2,300 persons, was publicly accessible online. The organization had stored the member list on a third-party server based in Australia, which had been hacked. Following its investigation, the PDPC found as follows:

- In respect of the Accountability Obligation, the PDPC found that the organization's privacy policy failed to set out any procedures or practices as to how it and its employees should handle and protect personal data in their possession or control and was in breach section 12(a) of the PDPA.

- In respect of the Protection Obligation, the PDPC found that the organization did not consider the adequacy of the security of its website or information technology (IT) system, and therefore was in breach of section 24 of the PDPA.
- Finally, in respect of the Transfer Limitation Obligation, the PDPC also found that as the organization had chosen to engage IT vendors with servers located outside Singapore, it was required to ensure that the recipient of the personal data outside Singapore is bound by legally enforceable obligations to provide a standard of protection that is at least comparable to that under the PDPA. As the organization failed to do so, the PDPC found the organization in breach of the Transfer Limitation Obligation.

For its various breaches, the PDPC imposed a financial penalty of S$11,000 on the organization and issued directions for the organization to conduct a security audit, implement an IT security policy, and conduct employee training on data protection.

Apart from the PDPC's enforcement decisions, the PDPA has also been considered in legal proceedings before the Singapore courts. In *IP Investment Management Pte Ltd and others v Alex Bellingham* [2019] SGDC 207, the Court had to decide on a claim pursuant to the right of private action available to individuals under section 32 of the PDPA. The Court found that there had been a breach of certain Data Protection Provisions and that the third plaintiff had suffered loss and damage through the defendant's misuse of his personal information. Accordingly, the Court granted an injunction restraining the defendant from using, disclosing, or communicating any personal data of the third plaintiff, and ordered the defendant to undertake the destruction of all personal data of the third plaintiff.

1.4. Application to Digital Advertising

The PDPA is the key law to consider with respect to personal data processing for digital advertising purposes.

For example, if cookies that collect personal data are used in digital advertising, or if personal data is otherwise collected and used for the purposes of digital advertising, then the organization collecting and using that personal data would likely have to obtain consent from the individuals in respect of the collection and use of such personal data. Importantly, under the PDPA, organizations are not allowed to, as a condition of providing a product or service, require an individual to consent to the collection, use or disclosure of personal data about the individual beyond what is reasonable to provide the product or service to that individual.

In general, where digital advertising involves the collection, use and/or disclosure of personal data, the organization collecting the personal data in Singapore is required to notify the individual of its purposes and obtain the individual's consent unless it is a data intermediary. Such notice may be provided, for example, through the publisher's website privacy policy for the benefit of other parties in the digital advertising "chain" (even if the publisher is a data intermediary or not involved in the collection of the personal data). In certain situations, as explained below, parties may use other bases for collecting, using, and disclosing personal data such as deemed

consent by notification, legitimate interests, and business improvement purposes (subject to meeting the relevant requirements and conditions).

Guidelines Published by ASAS

Apart from the relevant laws and regulations, the guidelines laid out by ASAS would provide some guidance on best practices in digital advertising. For example, under the ASAS' Interactive Marketing Guidelines, all marketing communication should be identified as such and distinguished from editorial or personal opinions and should not be made to appear like them. Additionally, when marketing communication is individually addressed to a consumer, the subject descriptor and context should not be misleading, and the commercial nature of the communication should not be concealed.

2. SCOPE OF APPLICATION

2.1. Who Do the Laws/Regulations Apply to and What Types of Processing Activities are Covered/Exempted?

The PDPA generally applies to and regulates the collection, use, disclosure, and processing of personal data by organizations. The term "organization" is defined in the PDPA to include any individual, company, association, or body of persons, corporate or unincorporated, whether or not established or having an office in Singapore. In this regard, related organizations, such as the parent or subsidiary of a company, are each separately required to comply with the PDPA.

The PDPA exempts certain categories of organizations from complying with its provisions relating to data protection (referred to below as the Data Protection Provisions). At present, these include:

- Individuals acting in a personal or domestic capacity.
- Employees acting in the course of their employment with an organization.
- Public agencies.

In addition, 'data intermediaries' are partially exempted from the application of the PDPA if they are processing personal data on behalf of and for the purposes of another organization pursuant to a contract which is evidenced or made in writing. In relation to such personal data, data intermediaries only have the following obligations under the PDPA:

- Protection of personal data in their possession or under their control, by making reasonable security arrangements to prevent the unauthorized access, collection, use, disclosure, copying, modification, disposal, or similar risks.
- Ceasing to retain documents containing personal data, or removing the means by which the personal data

can be associated with particular individuals (e.g., destruction or anonymization of personal data) as soon as it is reasonable to assume that the purpose for which the personal data was collected is no longer served by its retention, and retention is no longer necessary for legal or business purposes

- Notification of data breaches relating to personal data processed by a data intermediary on behalf of another organization or a public agency.

2.2. Jurisdictional Reach

The PDPA has extra-territorial jurisdictional reach and applies to organizations outside of Singapore if they collect, use, disclose, or otherwise process personal data in Singapore. In particular, the PDPA applies to organizations irrespective of their place of establishment and even if they have any no physical presence in Singapore if they collect, use, disclose, or otherwise process data within Singapore. For example, organizations located overseas which collect data in Singapore from individuals via online channels or platforms will be subject to the PDPA.

Organizations that collect personal data overseas and subsequently transfer such personal data into Singapore will be subject to the Data Protection Provisions in respect of the activities involving the personal data in Singapore.

If an organization in Singapore collects personal data from outside Singapore, for use or disclosure for its own purposes in Singapore, the organization is required to comply with all Data Protection Provisions from the time it seeks to collect the personal data or from the time it brings the personal data into Singapore, as the case may be.

Hence, the data subject need not be physically located within the jurisdiction when the data is collected and processed.

We also note that where appropriate, the PDPC will work with data protection regulators in foreign jurisdictions. For example, in the case of *Re Advance Home Tutors* [2019] SGPDPC 35, given that the developer was based in the Philippines, the PDPC indicated that it intended to refer this case to the Philippines National Privacy Commission.

Additionally, in the case of *Re Orchard Turn Developments Pte. Ltd*. [2017] SGPDPC 12, given that the third-party vendor was located in Hong Kong Special Administrative Region of the People's Republic of China, the PDPC indicated that it would pursue available options for assistance in this aspect of the investigations with the relevant foreign data protection authority.

2.3. Application to Digital Advertising

Scenario 1 (*The baseline*): A user residing in Singapore (determined by IP address or geo identifier) goes onto a website hosted in Singapore (the publisher) and is served an ad from a Singapore advertiser. The ad is placed on the publisher's website by an ad server connected via a DSP/SSP. The ad server collected data relating to the user's

interaction with the website and provides relevant data to the DSP/SSP and the advertiser, who each use it for their own purposes.

In this scenario, the PDPA would likely apply in respect of the Singaporean advertiser's collection, use and disclosure of personal data. (In general, this would be the case for websites hosted in Singapore or which otherwise target the Singapore market. Note that the specific requirements for hosting or targeting the Singapore market are not specified in legislation but is in line with PDPC's general approach in such matters.)

To recap, the PDPA would apply to all organizations in respect of their data activities conducted in Singapore, unless the organization is otherwise exempted under the PDPA. In this case, it is unlikely that a Singaporean advertiser would be exempted under the PDPA.

Therefore, the collection, use and disclosure of personal data by the Singaporean advertiser will be subject to the PDPA, including the requirement to obtain consent or deemed consent for the conduct of such data activities, unless one or more of the exceptions to the requirement to obtain consent apply.

Thus, in respect of a user residing in Singapore, who visits a Singapore domain and is served an ad by a Singaporean advertiser, any collection, use or disclosure of personal data in connection with this would require consent or deemed consent from the individual, unless one or more of the exceptions to the requirement to obtain consent apply. The Singaporean advertiser would also have to inform the individual of the purposes for the use of such personal data (e.g., serving ads and building a user profile).

As may be seen from PDPC's Selected Topics Guidelines (para. 6.10), if a publisher is not itself collecting personal data, it would not be required to obtain consent. In such a scenario, unless the publisher acts as a data intermediary in relation to the collection of personal data, the party serving the ad and monitoring user interaction would also be subject to the PDPA (e.g., the ad server). Other parties further down the digital advertising ecosystem may or may not be subject to the PDPA depending on whether they are located in Singapore and/or are using/processing the personal data in Singapore.

Scenario 2 (*User outside Singapore*): A Logged-on/signed-in user, known by the publisher to be a Singapore resident, goes onto a Singapore domain but the user's IP address or geo identifier indicates the user is outside Singapore. A Singapore advertiser serves an ad and uses the user data to build a user profile.

The answer would likely be the same as Scenario 1.

Even though the individual is now outside of Singapore, the personal data collected (if any) would likely be seen as having been done in Singapore. As such, the PDPA would continue to apply to the collection, use and disclosure of such personal data, notwithstanding that the individual is outside of Singapore.

- **Q1: Does the answer change if this is a signed-out user, with no way of knowing where they are domiciled?**

  No, the answer would not change if the collection, use or disclosure of personal data is done in Singapore.

Scenario 3 (*Publisher domain outside Singapore*): A user residing in Singapore (determined by IP address or geo identifier) goes onto a website hosted outside of Singapore. The publisher, ad server and all other parties in the digital advertising ecosystem save for the advertiser are located outside Singapore.

The parties located outside Singapore would not be subject to the PDPA as the website is not hosted in Singapore and does not target the Singapore market. However, given that the Singapore advertiser would be carrying out advertising activities from within Singapore, it would have to abide by the PDPA (if it will be collecting and using personal data for its advertising purposes).

Scenario 4 (*Advertiser outside Singapore*): A user residing in Singapore (determined by IP address or geo identifier) goes onto a Singapore domain and is served an ad by an advertiser based outside Singapore. The advertiser uses the user data to build a user profile.

PDPA will not likely apply to the advertiser. The PDPA generally imposes obligations in respect of the collection, use or disclosure of personal data within Singapore. In this case, given that the advertiser is based outside Singapore, the advertiser would not likely be subject to the PDPA.

As indicated in the scenario 1 above, the specific party collecting the personal data in Singapore would be subject to the PDPA, including the obligations relating to cross-border transfers. This may be the publisher (possibly as a data intermediary) or the specific ad server.

3. DEFINITIONS

3.1. Collect

- **When a publisher allows an ad tech company's pixel on its page, who is deemed to "collect" personal information and incur legal obligations (e.g., controller/co-controller obligations under GDPR or "business" obligations under CCPA) – the publisher, the ad tech company, or both?**

Although "collection" is not defined in the PDPA, the PDPC has stated in its Key Concept Guidelines that "collection" refers to any act or set of acts through which an organization obtains control over or possession of personal data. Such collection may take place actively or passively.

In particular, with respect to control, the PDPC stated in Re AIG Asia Pacific Insurance Pte. Ltd. [2018] SGPDPC 8 that "[w]hile there is no definition of "control" in the PDPA, the meaning of control in the context of data protection is generally understood to cover the ability, right or authority to determine (i) the purposes for; and/or (ii) the manner in which, personal data is processed, collected, used or disclosed."

Given that the ad tech company's pixel acquires data on the webpage (assuming that such data constitutes personal data under the PDPA), and the company determines the means through which and purposes for which the personal data is collected (e.g., to gain information on individuals users' activities), the ad tech company is likely to be deemed to "collect" and have control over such personal data under the PDPA. Accordingly, it would be liable under the Data Protection Provisions of the PDPA.

If the publisher merely allows for the ad tech company's pixel and does not obtain possession or control of the data, then it is unlikely to be deemed to "collect" such personal data under the PDPA and is unlikely to be liable under the PDPA (as suggested in PDPC's Selected Topics Guidelines, para. 6.10). In practice, it is arguable that the publisher may be viewed as facilitating the collection of personal data via the pixel and/or determining or co-determining the purposes of collection (for marketing purposes). Hence, as a practical matter, the publisher may be treated as the party to obtain consent (for itself and other parties in the digital advertising ecosystem).

If the publisher and/or ad tech company is found to merely process (e.g., transmission through the pixel) the personal data on behalf of and for the purposes of another party, it may be deemed to be a data intermediary under the PDPA and subject to a reduced set of obligations and the other party would be required to comply with the relevant obligations in the PDPA.

3.2. Data Processing (i.e., collecting, capturing, retaining, recording, organizing, structuring, storing, altering, retrieving, consulting, using, disclosing, transmitting, disseminating, making available, aligning, combining, restricting, erasing, destroying, or otherwise processing)

The key terms to consider in this respect are "processing," "collection," "use," and "disclosure."

The term "processing" is defined in the PDPA as the carrying out of any operation or set of operations in relation to the personal data, and includes any of the following:

a) Recording
b) Holding
c) Organization, adaptation, or alteration
d) Retrieval
e) Combination
f) Transmission
g) Erasure or destruction

The PDPA does not define the terms "collection," "use," and "disclosure." These terms would apply as they are commonly understood to cover the common types of activities undertaken by organizations in respect of personal data that may fall under collection, use, or disclosure respectively. Notwithstanding the foregoing, in

its Key Concepts Guidelines, the PDPC has stated that the terms "collection," "use," and "disclosure" may be understood to have the following meanings:

a) Collection refers to any act or set of acts through which an organization obtains control over or possession of personal data.
b) Use refers to any act or set of acts by which an organization employs personal data. A particular use of personal data may occasionally involve collection or disclosure that is necessarily part of the use.
c) Disclosure refers to any act or set of acts by which an organization discloses, transfers, or otherwise makes available personal data that is under its control or in its possession to any other organization. Accordingly, when a controller organization provides personal data to its service provider (being a separate entity), it would constitute disclosure for the purposes of the PDPA.

Collection, use, and disclosure may take place actively or passively. Both forms of collection, use, and disclosure will be subject to the same obligations under the PDPA.

3.3. Personal Information

'Personal data' under the PDPA refers to all 'data, whether true or not, about an individual who can be identified from that data, or from that data and other information to which the organization has or is likely to have access.' This applies regardless of whether such data is in electronic or another form, and regardless of the degree of sensitivity.

However, the PDPA expressly excludes the following categories of personal data from its application:

- 'Business contact information,' which is defined as 'an individual's name, position name or title, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes.'
- Personal data that is contained in a record that has been in existence for at least 100 years.
- Personal data about a deceased individual who has been dead for more than ten years.

The PDPC's Key Concepts Guidelines provides some guidance on when data is considered to be personal data. In brief, there are four considerations:

- The purpose of the information (i.e. whether it is to identify an individual or relates to an individual, or has another purpose and is incidental to the individual).
- Whether the individual can be identified if the information is combined with other information (a practicability threshold is applied in determining whether an organization is likely to have access to such other information).
- The number of elements in the data set.

- The nature of the data (e.g., whether it is an assigned identifier such as a passport number or data of a biological nature).

For information such as the individual's IDFA (on the understanding that the IDFA only identifies the device and not the specific individual), the state where the device is located, the age range of the individual and his interests, each of these data points, on its own, may not be able to identify an individual.

Type of Information Collected	Does this Category Independently Constitute Personal Information? (Yes/No)	Remarks / Qualifying Notes (if any)
IP Address	No, but note comments	Per PDPC's Selected Topics Guidelines, para. 6.3, though note that there is the possibility that the set of data collected may identify a particular individual, if sufficient data is collected which may relate to the individual's characteristics, interests, background, etc.
Mobile Advertising IDs (IDFA, AAID)	No, but note comments	As these enable collection of information relating to a specific individual, there is the possibility that the set of data collected may identify a particular individual, if sufficient data is collected which may relate to the individual's characteristics, interests, background, etc.
Consumer identifiers such as: • User device ID • Publisher persistent ID/Cross-publisher cookie ID • Household ID	No, but note comments	As user device ID and publisher IDs enable collection of information relating to a specific individual, there is the possibility that the set of data collected may identify a particular individual, if sufficient data is collected which may relate to the individual's characteristics, interests, background, etc.

Hashed identifiers such as: • Hashed email • Hashed IP address	No, but note comments	As these enable collection of information relating to a specific individual, there is the possibility that the set of data collected may identify a particular individual, if sufficient data is collected which may relate to the individual's characteristics, interests, background, etc.
User Agent such as: • Character string identifying the application • Operating system • Browser information, vendor, and/or version of the requesting user agent	No	
Device Information such as: • Type, version, system settings, etc.	No	
Website Information such as: • Name • URL, etc.	No	
Advertisement Information such as: • Placement • Title • Creative ID, etc.	No	
Timestamps	No	
Metrics such as: • Counts • Amounts of time	No	

Event Data such as: (e.g., full URL including query string, referral URL)	No	
Precise geolocation (latitude, longitude)	Generally, no	This may be a concern depending on the exact precision and the frequency of collection, e.g., as to whether an individual's specific movements may be tracked.
General geolocation (city, state, country)	No	

- **Are pseudonymous digital identifiers by themselves personal information (e.g., IDFA, cookie IDs, proprietary IDs, IP addresses, etc.)? Please provide context to the above chart.**

To recap, personal data is defined as data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which the organization has or is likely to have access.

There are certain types of data, by their nature or use, are more likely to identify an individual. This includes data that has been assigned exclusively to an individual for the purposes of identifying the individual (e.g., NRIC or passport number of an individual), or data of a biological nature (e.g., DNA, facial image, fingerprint, iris prints).

A general principle which may be derived from PDPC's guidelines is that unique data may constitute personal data if it may be used to identify an individual. In this regard, at present, persistent digital identifiers would not, on their own, be likely to identify an individual and hence, would not constitute personal data. However, as this position has not been confirmed in any PDPC cases, it remains open for PDPC to take a stricter approach (i.e., treat persistent digital identifiers as personal data).

Not all data that relates to an individual may identify the individual. For example, a residential address, on its own, relates to a particular place and there could be several individuals residing there. Hence, whether a residential address or a persistent digital identifier constitutes personal data would depend on whether that data is associated with a particular identifiable individual such that the individual can be identified through the data.

Personal data also includes data that alone cannot identify a particular individual but can identify an individual if it is combined with a unique identifier or other information. For example, a mailing list of email addresses may not be personal data on its own, but if the list contains customer IDs that can be linked to records in the Customer Relationship Management (CRM) system, then the list may be considered personal data. Thus, whether a persistent digital identifier is personal data depends on availability of other information the organization has or is likely to have access to, that would allow the data points to form a dataset that identifies an individual.

As a general principle, the more data points associated with a unique persistent identifier an organization collects, the more likely that the data may be personal data. For example, if an organization profiles the websites visited by a particular IP address, the items purchased by the same IP address and other online activities associated to the IP address for a long period of time, and is able to ascertain that the particular IP address is associated with a unique person with a specific surfing profile, the organization may be found to have collected personal data.

One example of a persistent digital identifier that may be considered personal data in this respect is an IP address. According to the PDPC's Selected Topics Guidelines (para. 6.10), an IP address, or any other network identifier, may not be personal data when viewed in isolation, because it simply identifies a particular device, but not a specific individual.

However, in certain cases, IP addresses have the potential of identifying unique individuals through their activities, especially when combined with other information about individuals. Depending on how a device is used, the information collected through the Internet, and the presence of other available information affects the possibility of identifying an individual from his device's IP address. Ultimately, if IP addresses can identify individuals, they are likely to be personal data in such context.

Another example of such persistent digital identifiers that may be considered personal data is an internet cookie. Cookies are text files created on a client computer when its web browser loads a website or web application. The PDPA applies to the collection, use, or disclosure of personal data using cookies, if such cookies are able to identify individuals.

- **If the answer to the above question is "no," if a Company possesses a persistent digital identifier in Database 1 and has that same identifier in Database 2 with directly identifying information, does that render the pseudonymous information in Database 1 as personal information?**

Yes, in such a scenario, the information in Database 1 would be considered personal information (i.e., would not be regarded as pseudonymous vis-à-vis the Company).

A persistent digital identifier may be personal data if it is combined with other information such that it can be associated with, or made to relate to, an identifiable individual. Thus, an organization should consider the availability of other information it has or is likely to have access to. As long as any combination of data contains a unique

identifier of an individual, that combination of data will constitute personal data of the individual.

A general rule of thumb is that the more data points associated to a persistent digital identifier an organization collects, the more likely that the data may be considered personal data. As such, where an organization employs the use of persistent digital identifiers (e.g., a cookie ID or Mobile Ad ID) and collects additional data alongside it, the more likely the persistent digital identifiers would be considered personal data.

Furthermore, the exact type of additional data collected alongside the persistent digital identifier is also a factor. To illustrate, if the organization collects directly identifying data (e.g., name, email address) alongside the persistent digital identifier, there is a greater likelihood that the persistent digital identifier would be personal data. In contrast, if the organization only collects technical data (e.g., IP addresses) alongside the persistent digital identifier, the likelihood of the persistent digital identifier being considered personal data is lower.

In other words, both the volume of data collected along with the exact type of additional data collected would both be factors in the final analysis.

- **Is a Company's possession of a pseudonymous identifier plus other non-directly identifying data (e.g., age, gender, precise or imprecise geolocation, user agent string, timestamps) considered "personal information"?**

  In general, a pseudonymous identifier coupled with non-directly identifying data would not be considered personal information.

- **Is a Company's possession of a pseudonymous identifier "personal information" if it can hire a service provider or otherwise engage in a transaction with a third party where the identifier could be matched to the person, but the Company chooses not to hire such service provider or undertake such transaction. Is the mere fact that this service is potentially available to match to the person sufficient to render that pseudonymous identifier as "personal information"?**

  PDPC's Selected Topics Guidelines explains at some length on when data can be said to be anonymized (including using techniques such as pseudonymization), taking into account the risk of re-identification. Paragraph 3.33 of these Guidelines specifically notes that one of the risk management approaches that may be adopted is to put in place controls to limit data users' access to "other information" (from the definition of "personal data" in the PDPA) that could reidentify the data. A similar approach could be used in the case of pseudonymous identifiers. Please see section [3.6] for more information concerning PDPC's approach to anonymization.

- **What level of geolocation is personal information (precise vs. approximate)? Does it need to be associated with an identifier to be considered PI?**

  Geolocation may be personal data if an individual can be identified from that data, or from that data and other information to which the organization has or is likely to have access. Ultimately, whether such geolocation data constitutes personal data will be dependent on the exact factual scenario at hand.

  As a starting position, geolocation data, in and of itself, is unlikely to be sufficient to identify individuals. However, once the geolocation data is combined with other information, especially identifying data, the data will naturally become less ambiguous/ague, and likelihood of such geolocation data being personal data will increase.

  The precise geolocation data of an individual alone (without any other accompanying data) could theoretically be personal data, especially if the location is so unique and distinctive that only one or very few individuals could realistically be present there/enter the premises.

  In comparison, the approximate geolocation data of an individual alone (without any other accompanying data) is unlikely to be personal data.

- **Is a household identifier personal information? (Consider: If a company has a residential IP address (household level ID) and multiple unique device IDs (e.g., MAIDs for every mobile device in the house) associated with that IP address, would that affect whether the household identifier is considered personal information?)**

  It is possible for a household identifier to be personal information. PDPC's Key Concepts Guidelines provides the example that since several individuals might be residing in the same residential address, residential address constitutes personal data only if it is associated with a particular identifiable individual such that the individual can be identified through the data, or through that data together with other information that an organization has access to. Hence the answer would depend on factors such as the actual number of IDs and the extent of data collected.

- **Is a hashed identifier personal information? (Consider: there are commercially available services that will take batches of emails encrypted using standard hashes and return (often a high percentage) of clear emails from them. Does that affect whether they are considered personal information, if all a company has to do is pay for the commercial service?)**

  It is possible that a hashed identifier is personal information. As is the case with other types of data, much would depend on the exact facts at hand. However, on balance, it is likely that a hashed identifier

would not be personal data unless the hashing can be reversed and/or there is other information which may be combined to identify the individual.

- **Is probabilistic information considered personal information?**
  It is possible that probabilistic information is personal information.

Ultimately, if the information in question can identify any individual, whether on its own or together with other information that an organization has access to, then it would be considered personal data.

3.4. Sensitive Data

Even though there is no special category for sensitive personal data in the PDPA, the PDPC takes the view that personal data of a more sensitive nature should be safeguarded by a higher level of protection. The types of personal data that would typically be more sensitive in nature include an individual's national identification numbers (e.g. National Registration Identity Card and passport numbers); personal data of a financial nature (e.g. bank account details, Central Depository account details, securities holdings, transaction and payment summaries); insurance information (e.g. names of the policyholder's dependents or beneficiaries, sum insured under the insurance policy, the premium amount and type of coverage); an individual's personal history involving drug use and infidelity; sensitive medical conditions; and personal data of minors. (See *Re Aviva Ltd [2017] SGPDPC 14*).

3.5. Pseudonymous Information

There is no specific reference to pseudonymization in the PDPA. However, in its Selected Topics Guidelines, the PDPC has described pseudonymization as an anonymization technique involving 'replacing personal identifiers with other references,' and has also stated that the anonymization of personal data may be carried out to render the anonymized data suitable for more uses than its original state (i.e., the original personal data) would permit under data protection regimes, since anonymized data would not allow the identification of an individual.

Additionally, in its Guide to Basic Data Anonymization Techniques, the PDPC set out recommended best practices for pseudonymization, and recognized the distinction between irreversible pseudonymization (i.e., where the original values are properly disposed and the pseudonymization was done in a non-repeatable fashion) and reversible pseudonymization (i.e. where the original values are securely kept but can be retrieved and linked back to the pseudonym).

- **Is pseudonymous information considered personal information?**

Personal data is defined as data, whether true or not, about an individual who can be identified (a) from that data, or (b) from that data and other information to which the organization has or is likely to have access.

Whilst there is no specific reference to pseudonymization in the PDPA, according to Selected Topics Guidelines, pseudonymization is an example of an anonymization technique which anonymizes data. The Selected Topics Guidelines also states that data which has been anonymized is not personal data.

However, the Selected Topics Guidelines highlights that data would not be considered anonymized if there is a strong possibility that an individual could be re-identified, taking into consideration both:

a) The data itself, or the data combined with other information to which the organization has or is likely to have access.

b) The measures and safeguards (or lack thereof) implemented by the organization to mitigate the risk of identification.

- **Are persistent digital identifiers pseudonymous information (e.g., IDFA, cookie IDs, proprietary IDs, IP addresses, etc.)?**

  As stated above, pseudonymous information is not defined in the PDPA. Whether or not persistent digital identifiers constitute pseudonymous information would depend on the exact factual matrix at hand.

- **Does the law subject pseudonymous information to fewer obligations than "regular" personal information?**

  Yes, unless the pseudonymous information has a serious possibility for the re-identification of individuals.

  Pseudonymous information that does not enable the identification of any individual is not personal data and would not be subject to the PDPA. Pseudonymous information, however, which has a serious possibility of re-identification of individuals would be considered personal data, and organizations would be subject to the Data Protection Provisions in this regard.

3.6. Anonymized/De-identified Information

- **Is there a difference between anonymized or de-identified data?**

  There is no definition of de-identification provided by PDPA. In the Selected Topics Guidelines, the PDPC acknowledges some jurisdictions use 'anonymization' and 'de-identification' interchangeably to refer to the process of converting personal data into data that can no longer be used to identify an individual, whether alone or in combination with other available information, whilst others use 'anonymization' to refer to de-identification that is irreversible.

  The PDPC's view, as stated in the Selected Topics Guidelines, is that the term 'anonymization' refers to the process of converting personal data into data that cannot be used to identify any particular individual and can be reversible or irreversible.

  Some anonymization techniques suggested by the PDPC in the Selected Topics Guidelines include:

  (a) Aggregation: displaying values as totals, so that none of the individual values which could identify an individual is shown. For example, given a dataset with the ages of eight individuals (i.e., 33, 35, 34, 37, 42, 45, 37, 40), displaying the sum of the individual ages of the total number of individuals in a group (i.e., 303), rather than the age of each individual represented discretely.

(b) Replacement: replacing values or a subset of the values with a computed average or a number derived from the values. For example, replacing the individuals with ages of 15, 18, and 20 with an age value of 17 to blur the distinction, if exact age is not required for the desired purposes.

(c) Masking: removing certain details while preserving the look and feel of the data. For example, representing a full string of NRIC numbers as '#####567A' instead of 'S1234567A.'

Additionally, the PDPC would consider an organization to have anonymized data if there is no serious possibility that a data user or recipient would be able to identify any individuals from the data.

Whilst there is the risk of re-identification presented when using or disclosing anonymized data, this risk may be managed in certain measures. Apart from using the best anonymization technique to prevent de-anonymization, to further manage the risk of re-identification, an organization may also consider putting in place other appropriate controls, such as:

(a) Limiting the number of data recipients to whom the information is disclosed and the number of persons that can access the information.
(b) Imposing restrictions on the data recipient on the use and subsequent disclosure of the data.
(c) Requiring the data recipient to implement processes to govern the proper use of the anonymized data in line with the restrictions.
(d) Requiring the data recipient to implement processes and measures for the destruction of data as soon as the data no longer serves any business or legal purpose.

- **What common data categories are passed between publishers, advertisers, and ad tech companies that fall into this category when no persistent identifier is present (e.g., browser type, device type, operating system, app name, publisher site)?**

Based on our understanding from publicly available sources, some common data categories passed between publishers, advertisers, and ad tech companies that may fall into this category of "anonymized" data where no identifier is present include:

- Referring sites
- Overall journey on-site, including mouse cursor movement
- Events such as scrolling, and clicks
    - Search queries
    - Time of session
    - Behavior on site:
        - Contextual and thematic preferences to certain topics and pages.

- Various interactions with the page's content (downloads, etc.).
- Transitions to another place through links and ads.

- Demographics
- Consumer's gear (browser specs, ad-block on or off, etc.)
- Interaction with advertisement

3.7. Data Controller

The PDPA does not use the term 'data controller.' Instead, it uses the more general term of 'organizations' when prescribing the obligations that organizations are required to comply with under the PDPA. The term 'organization' broadly covers natural persons, corporate bodies (such as companies) and unincorporated bodies of persons (such as associations), regardless of whether they are formed or recognized under the law of Singapore or are a resident or have an office or place of business in Singapore.

3.8. Joint Controller/Co-Controller

There is no express concept of a joint controller or co-controller under the PDPA. However, we highlight that all organizations would be required to comply with the Data Protection Provisions in the conduct of their data activities, unless otherwise exempted under the PDPA.

3.9. Data Processor/Service Provider (i.e., an entity that is qualified as a processor or service provider under the law because it meets certain requirements and processes data pursuant to a permissible purpose on behalf of a controller/business)

The term 'data processor' is not used in the PDPA, but an equivalent term 'data intermediary' is used. 'Data intermediary' refers to an organization which processes personal data on behalf of another organization but does not include an employee of that other organization. Please refer to section 8 below for the definition of 'data intermediary.' See also section 2.2 above for more information on the obligations of data intermediaries.

3.10. Third Party (i.e., a third party that receives data from a business for non-business purposes and does not necessarily have specific requirements under the law as to such data, such as a third-party under the CCPA)

The term 'third party" is not used in the PDPA. Rather, a third party would also be an organization under the PDPA, including any individual, company, association, or body of persons, corporate or unincorporated, and would be subject to the provisions of the PDPA as an organization in relation to its collection, use, disclosure and/or processing of personal information.

4. DATA CONTROLLER RIGHTS AND RESPONSIBILITIES

4.1. Overview

The PDPA puts in place the following obligations on organizations with respect to their data activities:

- Consent Obligation: An organization must obtain an individual's consent before collecting, using, or disclosing his/her personal data for a purpose (sections 13 to 17 of the PDPA).
- Purpose Limitation Obligation: An organization may only collect, use, or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances (section 18 of the PDPA).
- Notification Obligation: An organization must notify the individual of the purpose(s) for which it intends to collect, use, or disclose his/her personal data on or before such collection, use, or disclosure, and may only collect, use, and disclose personal data for such purposes (sections 18 and 20 of the PDPA).
- Access and Correction Obligation: An organization must, upon request, allow an individual to access and/or correct his/her personal data in its possession or under its control. In addition, the organization is obliged to provide the individual with information about the ways in which personal data may have been used or disclosed during the past year (sections 21 and 22 of the PDPA).
- Accuracy Obligation: An organization must make a reasonable effort to ensure that personal data collected by it is accurate and complete, if it is likely to use such personal data to make a decision that affects the individual concerned or disclose such personal data to another organization (section 23 of the PDPA).
- Protection Obligation: An organization must protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal, or similar risks (section 24 of the PDPA).
- Retention Limitation Obligation: An organization must cease to retain documents containing personal data or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that the retention of such personal data no longer serves the purpose for which it was collected and is no longer necessary for legal or business purposes (section 25 of the PDPA).
- Transfer Limitation Obligation: An organization must not transfer personal data to a country or territory outside Singapore except in accordance with requirements prescribed under the PDPA to ensure that the transferred personal data will be accorded a standard of protection that is comparable to that under the PDPA (section 26 of the PDPA).

- Accountability Obligation: An organization must appoint a person to be responsible for ensuring that it complies with the PDPA, typically referred to as a data protection officer ('DPO') and develop and implement policies and practices that are necessary to meet its obligations under the PDPA, including a process to receive complaints. In addition, the organization is required to communicate to its staff information about such policies and practices and make information available upon request to individuals about such policies and practices (sections 11 and 12 of the PDPA).
- Data Breach Notification Obligation: An organization must assess data breaches that have occurred affecting personal data in their possession or under their control, and are required to notify the PDPC, as well as affected individuals, of the occurrence of certain data breaches (sections 26A to 26E of the PDPA).
- Data Portability Obligation: Upon an organization's receipt of a data porting request from an individual, the porting organization must transmit the applicable data specified in the data porting request to the receiving organization in accordance with any prescribed requirements, such as requirements relating to technical, user experience, and consumer protection matters (sections 26F to 26J of the PDPA; note that these sections are not yet in force as of July 1, 2021).

4.2. Accountability

4.2.1. Overview

Organizations are subject to the Accountability Obligation. Under the Accountability Obligation, an organization must develop and implement policies and practices that are necessary for it to meet its key obligations under the PDPA, and to make information about such policies and practices publicly available, such as via an online personal data protection policy and/or privacy policy. Every organization must also appoint one or more individuals to be responsible for ensuring that the organization complies with the PDPA (i.e., a Data Protection Officer, or "**DPO**").

4.2.2. Application to Digital Advertising

The Accountability Obligation is of general application and applies to all organizations, including organizations that engage in digital advertising activities in Singapore. Thus, under the Accountability Obligation, digital advertisers would be required to, amongst other obligations, develop and implement data protection policies and practices and ensure that it communicates such policies and practices to its staff.

Specifically, as digital advertising often involves the use of new technologies, organizations may wish to consider conducting Data Protection Impact Assessments in appropriate circumstances and implementing a Data Protection Management Program to ensure that they carry out their data activities in an accountable manner, and to increase compliance with the Accountability Obligation.

4.3. Notice

4.3.1. Overview

Organizations are subject to the Notification Obligation. An organization must notify the individual of the purpose(s) for which it intends to collect, use, or disclose his personal data on or before such collection, use, or disclosure. In addition, the organization is also obliged to provide the individual with information about the ways in which the personal data may have been used or disclosed during the past year.

There is no obligation imposed on an organization to notify or register with the PDPC before collecting, using, or disclosing any personal data in Singapore.

- **Who must receive notice? When must notice be provided? What must be in the notice in the digital advertising context?**

Under the Notification Obligation, individuals whose personal data will be collected, used, or disclosed must be notified of the purposes of such collection, use or disclosure. The notification would generally have to take place before the collection of such data, or before the use or disclosure of such data.

For example, notification may take place when an individual visits a website, which will collect some of their personal data. In practice, such notification is typically done via a website privacy policy (or similar document) linked in the website. Under the PDPA, where an organization needs to collect, use, and/or disclose personal data on a periodic basis, it must inform the individual before the first collection of the data.

Under section 20(3) PDPA, organizations are not required to inform individuals of the purposes for which their personal data will be collected, used, or disclosed if:

a) The individual is deemed to have consented to the collection, use or disclosure of his or her personal data under section 15 or 15A of the PDPA.
b) The organization is, in accordance with section 17 PDPA, collecting, using, or disclosing the personal data without the consent of the individual under one of the exceptions set out in the PDPA. See section 4.4.1 below.

- **Is specific notice required for sensitive information?**

No, there are no specific notice requirements in respect of sensitive information.

In its Guide to Notification, the PDPC clarified that the PDPA does not prescribe how organizations should inform individuals of the purposes of collection, use, or disclosure of their personal data, or what must be included as part of the notification. Organizations will need to determine the most appropriate form of notification to meet their business needs.

On this note, given that personal data of a more sensitive nature should be safeguarded by a higher level of

protection, we highlight that the PDPC stated in its Guide to Notification that organizations may wish to highlight its collection, usage, or disclosure of sensitive personal data, which may be of particular concern to individuals and to provide just-in-time notifications before data processing takes places in respect of such sensitive personal data.

- **Are there any specific requirements for providing notice related to processing children's personal information?**

No, there are no specific requirements under the PDPA to provide notice related to the processing of the personal data of minors.

However, given that there is generally greater sensitivity surrounding the treatment of minors, the PDPC has stated in its Selected Topics Guidelines that it may be prudent for organizations to consider putting in place relevant precautions if they are (or expect to be) collecting, using, or disclosing personal data about minors. For example, organizations that provide services targeted at minors could state terms and conditions in language that is readily understandable by minors, or use pictures and other visual aids to make such terms and conditions easier to understand. Other sound practices could include placing additional safeguards against unauthorized disclosure of, or unauthorized access to, personal data of minors, or anonymizing personal data of minors before disclosure, where feasible.

- **Are there any requirements compelling vendors (acting on behalf of another party in the ecosystem) directly collecting personal information or those receiving it from others personal information to provide additional notices? Who is responsible for those notices? Publishers? The vendors?**

In this instance, it is likely that the vendor would be considered a data intermediary under the PDPA. Organizations that process personal data on behalf of other organizations as data intermediaries, pursuant to a contract which is evidenced or made in writing, would only be required to comply with the Protection Obligation and the Retention Limitation Obligation. Thus, should a data intermediary collect personal data from an organization (i.e., the data controller) to process such personal data pursuant to a contract in writing, it would be the data controller who would be responsible for notifying the individuals whose personal data would be collected, used, or disclosed.

4.3.2. Application to Digital Advertising

- **Do third parties need to be named? For example, if a publisher gives privacy policy notice that it may share personal information with third parties for advertising purpose, does it have to specify which third parties? Do specific digital advertising activities or purposes need to be disclosed as well (e.g., TCF purposes)?**

No, there is no specific requirement in the PDPA for third parties to be named. While the PDPA requires purposes to be disclosed, it does not specify the level of detail required. PDPC's Key Concepts Guidelines states that organizations should state its purposes at an appropriate level of detail for the individuals to determine the reasons and manner in which the organization will be collecting, using, or disclosing his personal data. However,

an organization does not need to specify every activity it will undertake in relation to the collection, use, or disclosure of the personal data, including activities that are integral to the proper functioning of the overall business operations related to its purposes.

In general, there are no specific requirements in respect of the collection of personal data for digital advertising purposes in PDPA and related guidelines. However, in the PDPC's Guide to Data Sharing (revised February 1, 2018), it provided examples of dynamic approaches in the context of a mobile application platform. This includes just-in-time notifications and data protection dashboards.

- **From an industry perspective it's common to distinguish data use for ad targeting vs. profile building vs. measuring ad campaigns. Does the Notification Obligation require separate disclosure of those things? Or is it enough to say something general like "advertising and related purposes."**

Based on the general principles noted above, notification should be provided for all major uses of the personal data, i.e., for ad targeting, profile building, and measuring ad campaigns. To the extent that the data will be used in an aggregated manner or pursuant to specific exceptions (such as the exception for business improvement purposes in the PDPA), it is not necessary to give notification (although, as a good practice, including this in the privacy policy may pre-empt queries or complaints relating to such uses).

No, neither the PDPA nor any of the PDPC's published guidelines specifically cover data protection legal issues that arise within the digital marketing sector. Ultimately, the touchstone, under the PDPA is whether personal data is collected, used, or disclosed by the organization. If so, the organization will be required to adhere to the Data Protection Provisions in respect of such personal data.

4.4. Consent and Exceptions to Consent

4.4.1. Overview

- **For what types of personal information or purposes of processing is consent required?**

The Consent Obligation under the PDPA prohibits organizations from collecting, using, or disclosing an individual's personal data unless:

- The individual gives his consent for the collection, use or disclosure of his personal data.
- The individual is deemed to have given his consent for the collection, use or disclosure of his personal data.
- Collection, use, or disclosure without consent is required or authorized under the PDPA or any other written law.

For example, consent for the collection, use or disclosure of personal data would not be required if the collection, use, or disclosure is necessary to respond to an emergency that threatens the life, health, or safety of the individual

or another individual. We also note that when the amendments introduced under the Amendment Act include new exceptions to the Consent Obligation, such as the Legitimate Interests Exception, and the Business Improvement Exception (please refer to 4.4.1).

In this regard, we note that section 14(2)(a) of the PDPA provides that, an organization shall not, as a condition of providing a product or service, require an individual to consent to the collection, use, or disclosure of personal data beyond what is reasonable to provide the product or service to the individual. Additionally, section 14(2)9b) of the PDPA provides that organizations should not obtain or attempt to obtain consent for collecting, using, or disclosing personal data by providing false or misleading information with respect to the collection, use, or disclosure of the personal data, or using deceptive or misleading practices.

The Data Protection Provisions under the PDPA impose obligations on organizations in respect of all personal data, except for the personal data excluded under section 4 of the PDPA (e.g., personal data about an individual that is contained in a record that has been in existence for at least 100 years). Personal data is defined under the PDPA as data, whether true or not, about an individual who can be identified (a) from that data, or (b) from that data and other information to which the organization has or is likely to have access.

- **How is valid consent manifested – express consent, opt-in, implied consent, or opt-out?**

The PDPA does not prescribe how consent may be obtained, as long as valid consent is obtained. Under the PDPC's Key Concepts Guidelines, the PDPC has stated that consent may be obtained in several different ways.

In general, organizations are recommended to obtain consent from an individual through a positive action of the individual. An opt out approach may be possible where the organization has, or will have, an ongoing or long-term relationship with the individual. In other circumstances, if an organization intends to adopt the opt out approach in seeking consent, it runs the risk that it may not be in compliance with the Consent Obligation.

Whilst consent may be given verbally, as good practice, an organization should obtain consent that is in writing or recorded in a manner that is accessible for future reference.

Additionally, the PDPA sets out several situations which constitute deemed consent, even if an individual does not expressly give his consent. Under the present section 15(1) of the PDPA, an individual is deemed to consent to the collection, use, or disclosure of personal data if he or she, voluntarily provides the personal data to the organization for that purpose, and it is reasonable that the individual would voluntarily provide that data. Further, under section 15A of the PDPA, an individual is deemed to consent to the collection, use, or disclosure of his personal data where an organization notifies him of its purposes for such collection, use, or disclosure and provides a reasonable period for the individual to opt-out. However, an organization that wishes to rely on this type of deemed consent is required to conduct an assessment of the impact of the collection on the individual and mitigate any significant risks to the individual's personal data.

In relation to personal data collected via a website, deemed consent may apply in two contexts:

- Where an individual visits a website and provides personal data (or allows the collection of personal data) for a purpose related to the operation of the website, deemed consent may apply. This may include purposes set out in the website's privacy policy.

Where an organization notifies the individual (possibly via the website privacy policy or a specific notice) that personal data will be collected and gives the individual an opportunity to "opt out," deemed consent may also apply.

- **Is specific notice required as part of the consent?**

Prior to obtaining consent from an individual, an organization must notify the individual of the purposes for which his personal data will be collected, used, or disclosed. If an organization fails to inform the individual of the purposes for which his personal data will be collected, used, and disclosed, any consent given by the individual would likely not amount to valid consent under the PDPA.

- **Does the consent obligation require granularity (i.e., consent for distinct processing activities) similar to GDPR? Or is the consent obligation more generalized (e.g., requiring consumers to opt-in to "online behavioral advertising" more broadly, without having to consent to each constituent processing activity/party)? Is consent different for different uses or types of data (e.g., sensitive data, profiling, automated decision making, etc.) Please provide details.**

The PDPA does not specify the level of detail to which consent must be obtained.

Under the Consent and Notification Obligations of the PDPA, an individual only gives valid consent if the individual has been notified of the purposes for which his personal data will be collected, used, or disclosed and the individual has provided his consent for those purposes. This is a general obligation—the Notification Obligation does not specify the level of granularity for the notification of purpose for the collection, use, or disclosure of personal data.

The PDPC has stated in its Key Concepts Guidelines that an organization should state its purposes at an appropriate level of detail for the individual to determine the reasons and manner in which the organization will be collecting, using, or disclosing his personal data. However, an organization need not specify every activity it will undertake in relation to collecting, using, or disclosing personal data when notifying individuals of its purposes. For example, if an organization wishes to obtain consent to collect or use personal data for the purpose of providing a service to an individual, the organization does not need to seek consent for: (a) every activity it will undertake to provide that service; and (b) internal corporate governance processes such as allowing auditors to access personal data as part of an audit.

In considering how specific to be when stating its purposes, organizations may consider the following:

a) Whether the purpose is stated clearly and concisely.

b) Whether the purpose is required for the provision of products or services (as distinct from optional purposes).

c) If the personal data will be disclosed to other organizations, how the organizations should be made known to the individuals.

d) Whether stating the purpose to a greater degree of specificity would be a help or hindrance to the individual understanding the purpose(s) for which his personal data would be collected, used, or disclosed.

e) What degree of specificity would be appropriate in light of the organization's business processes.

Additionally, the PDPC stated in its Guide to Notification that organizations should tailor the notification to the intended audience. In their notifications, organizations should provide information on:

a) The types of personal data that will be collected, used, or disclosed.

b) How such personal data will be collected.

c) Purposes of the collection, use or disclosure of personal data.

d) Whether and why the personal data collected is necessary to provide the product or service to individuals.

e) Any third parties whom the personal data may be disclosed to.

- **Can personal information be processed for secondary purposes (i.e., differing purposes from which it was collected)?**

No personal information cannot be processed for secondary purposes unless consent has been obtained for that purpose.

Under the Purpose Obligation, organizations may collect, use, or disclose personal data about an individual only for purposes (a) that a reasonable person would consider appropriate in the circumstances, and (b) that the individual has been informed of under the Notification Obligation.

Under the Notification Obligation, section 20(1)(b) of the PDPA requires organizations to notify individuals of any other purpose of the use or disclosure of the personal data of which the individual has not been informed of at the point of collection of personal data. Additionally, under the Consent Obligation, an individual must provide his consent for the purposes for which he has been notified under the Notification Obligation.

Thus, to use personal data for purposes which were not notified to the individual, the organization will have to notify the individual of the additional purposes for the use of that individual's personal data, and the individual will have to consent to the use of his/her personal data for those additional purposes.

- **Are there any rules compelling downstream recipients/processors of personal information to provide additional notices?**

No, there are no requirements under the PDPA for data intermediaries to provide additional notices.

In general, under the Notification Obligation, notification must be obtained at the point of collection of personal data. Thus, once the individual has consented to the collection, use, and disclosure of his personal data, further notice and consent would not be necessary if the individual has already provided his consent to the data controller.

- **Are there any issues concerning the timing of consent?**

An organization must obtain the consent of the individual before collecting, using, or disclosing his personal data for a purpose. If the purpose for which the personal data will be used was not notified to the individual before the collection of personal data, the individual must be informed of this purpose, before the use or disclosure of the personal data for that purpose and must provide his consent for such use or disclosure, as the case may be.

- **Are there distinct consent requirements for sensitive personal information?**

No, the PDPA does not make a distinction between sensitive personal data and non-sensitive personal data. However, the PDPC has stated in its enforcement decisions that personal data of a sensitive nature should be safeguarded by a higher level of protection.

We note that the PDPC has issued its Advisory Guidelines on the PDPA for NRIC and other National Identification Numbers. Under this set of guidelines, the PDPC has taken the position that for the following types of personal data, namely, the Singapore National Registration Identity Card numbers, Birth Certificate numbers, Foreign Identification Numbers, and Work Permit numbers, organizations will only be allowed to collect, use, or disclose such personal data if (a) the collection, use, or disclosure is required by the law; or (b) it is necessary to establish or verify an individual's identity to a high degree of accuracy.

- **Are there distinct consent requirements for profiling consumers? If a business gets consent to use personal data for "advertising and marketing" purposes, is a separate (or more specific?) consent required to build an advertising profile for advertising?**

No, there are no distinct consent requirements under the PDPA in respect of the profiling of consumers. However, before collecting and using an individual's data for the purpose of profiling, an organization will have to obtain consent from the individual for the collection and use of his/her personal data for that purpose.

For the purpose of profiling consumers, we note that the organization might be able to rely on the new business

improvement exception to the Consent Obligation (inserted into the PDPA by the Amendment Act). The business improvement exception to the Consent Obligation enables organizations to use personal data without an individual's consent for any of the following business improvement purposes:

a) Improving, enhancing or developing new goods or services.

b) Improving, enhancing, or developing new methods or processes for business operations in relation to the organizations' goods and services.

c) Learning or understanding behavior and preferences of individuals (including groups of individuals segmented by profile).

d) Identifying goods or services that may be suitable for individuals (including groups of individuals segmented by profile) or personalizing or customizing any such goods or services for individuals.

To rely on the business improvement exception, organizations will need to ensure the following:

a) The business improvement purpose cannot reasonably be achieved without using the personal data in an individually identifiable form.

b) The organization's use of personal data for the business improvement purpose is one that a reasonable person would consider appropriate in the circumstances.

- **Are there distinct consent requirements for automated decision making?**

No, there are no distinct consent requirements under the PDPA in respect of automated decision making. However, before collecting and using an individual's data for the purpose of automated decision making, an organization will have to obtain consent from the individual for the collection and use of his/her personal data for that purpose.

For the purpose of automated decision making, similar to the profiling of customers, the organization might be able to rely on the business improvement exception to the Consent Obligation. The business improvement exception to the Consent Obligation enables organizations to use, without consent, personal data that they had collected in accordance with the Data Protection Provisions of the PDPA for any of the following business improvement purposes:

a) Improving, enhancing, or developing new goods or services.

b) Improving, enhancing, or developing new methods or processes for business operations in relation to the organizations' goods and services.

c) Learning or understanding behavior and preferences of individuals (including groups of individuals segmented by profile).

d) Identifying goods or services that may be suitable for individuals (including groups of individuals segmented by profile) or personalizing or customizing any such goods or services for individuals.

To rely on the business improvement exception, organizations will need to ensure the following:

a) The business improvement purpose cannot reasonably be achieved without using the personal data in an individually identifiable form.

b) The organization's use of personal data for the business improvement purpose is one that a reasonable person would consider appropriate in the circumstances.

- **Are there any age restrictions related to consent? Are there distinct consent requirements around processing children's personal information?**

While there are no age-specific restrictions or requirements under the PDPA, under the common law in Singapore, the age of majority is 21 years. However, the age of contractual capacity is 18 years (see section 35(1) of the Civil Law Act (Cap. 43). As a general rule, contracts are not enforceable against minors (i.e., persons under the age of 18), except for contracts for necessaries, or contracts for training or education, subject to further exceptions.

In respect of data protection issues, the PDPC has stated in its Selected Topics Guidelines that it will adopt the practical rule of thumb, that a minor who is at least 13 years of age would typically have sufficient understanding to be able to consent on his own behalf. As a general guide, where the minor is under the age of 13 years, organizations may wish to obtain consent for the collection, use, and disclosure of the minor's personal data from an individual that can legally give consent on behalf of the minor, such as the minor's parent or guardian.

However, where an organization has reason to believe or it can be shown that a minor does not have sufficient understanding of the nature and consequences of giving consent, the organization should obtain consent from an individual, such as the minor's parent or guardian, who is legally able to provide consent on the minor's behalf.

Overall, an organization should take appropriate steps to ensure that the minor can effectively give consent on his own behalf, in light of the circumstances of the particular case including the impact on the minor in giving consent.

- **Can consent, however manifested, be revoked?**

Yes, an individual has the right to withdraw his consent on giving reasonable notice to an organization.

Section 16 of the PDPA provides that individuals may at any time withdraw any consent given or deemed to have been given under the PDPA in respect of the collection, use, or disclosure of their personal data for any purpose by an organization.

4.4.2. Application to Digital Advertising

To date, there is no sector-specific legislation on digital advertising. However, based on the PDPC's Advisory Guidelines on Requiring Consent for Marketing Purposes, it is recommended for organizations to obtain express consent from the individual to collect, use, and disclose their personal data for marketing purposes. Ultimately, the

touchstone would be whether the digital marketing activities involve the collection, use, and disclosure of personal data. If so, the organization would be required to inform the individual of the purposes for the collection, use, and disclosure of personal data, and to obtain consent of the same.

Digital advertisers may wish to ensure that their digital advertising activities comply with their obligations under the PDPA. For example, if Internet cookies are used which collects data that can identify an individual (see section 3.3 for a more in-depth consideration of when this may occur), digital advertisers should ensure that they notify the individuals of the purposes for which such personal data may be used, and to obtain consent from the individuals for the collection, use, or disclosure of their personal data for those purposes.

4.5. Appropriate Purposes

4.5.1. Overview

Consent

Under the Consent Obligation, an organization is required to obtain individuals' consent to collect, use, or disclose their personal data unless such collection, use, or disclosure is required or authorized under the PDPA or any other written law. Some examples of when such collection, use, or disclosure is authorized under the PDPA is when such collection, use, or disclosure of personal data:

- Is done in response to an emergency that threatens the life, health, or safety of the individual.
- Is used to manage or terminate an employment relationship (provided that the employee is notified).
- Is publicly available.

An organization is further required to state the purposes for which it is collecting, using, or disclosing the data. Where the supply of a product or service is conditional upon consent given by an individual, such consent must not extend beyond what is reasonable to provide that product or service.

Individuals can be deemed to have given consent when they voluntarily provide their personal data for a purpose, and it is reasonable that they would voluntarily provide such data. For such deemed consent to apply, the onus is on the organization to ensure that individuals were aware of the purpose for which their personal data was collected, used, or disclosed. Two new forms of deemed consent have also be introduced under the Amendment Act – deemed consent by contractual necessity (addressed below) and deemed consent by notification. For deemed consent by notification to apply, an organization must:

- Conduct an assessment to determine that the proposed collection, use, or disclosure of the personal data is not likely to have an adverse effect on the individual (including identifying any likely adverse effect on the individual, as well as identifying and implementing reasonable measures to eliminate, reduce the likelihood or mitigate the adverse effect).

- Take reasonable steps to bring the following information to the attention of the individual:
    1. The organization's intention to collect, use, or disclose the personal data.
    2. The purpose for which the personal data will be collected, used, or disclosed.
    3. A reasonable period within which, and a reasonable manner by which, the individual may notify the organization that the individual does not consent to the organization's proposed collection, use, or disclosure of the personal data.

If the individual does not notify the organization before the expiry of the reasonable period mentioned in point 3 above that the individual does not consent to the proposed collection, use, or disclosure of the personal data by the organization, the individual is then deemed to consent.

Individuals can withdraw consent at any time by giving reasonable notice. On receipt of notice, the organization must inform the individual of the consequences of such a withdrawal. Withdrawal of consent applies prospectively and will only affect an organization's continued or future use of the personal data concerned. Organizations are generally required to inform agents and data intermediaries to whom the personal data has already been disclosed of the withdrawal.

An organization collecting personal data from a third-party source is required to notify the source of the purposes for which it will be collecting, using, and disclosing the personal data. Moreover, the organization should exercise the appropriate due diligence to check and ensure that the third-party source can validly give consent for the collection, use, and disclosure of personal data on behalf of the individuals or that the source had obtained consent for the disclosure of the personal data.

Contract with the Data Subject

Where an organization enters into a contract with an individual, the individual may be deemed to have given his consent for the collection, use, or disclosure of personal data (as the case may be).

Additionally, consent may be deemed by contractual necessity where an individual provides his personal data to one organization for the purpose of a contract and it is reasonably necessary for the organization to disclose the personal data to another organization for the necessary conclusion or performance of the contract between the individual and the first organization.

Legal Obligations

An organization is able to collect, use, and disclose personal data where it is required or permitted under law. For example, the disclosure of personal data is permitted to any officer of a prescribed law enforcement agency, upon production of written authorization signed by the head or director of that law enforcement agency or a person of a similar rank, certifying that the personal data is necessary for the purposes of the functions or duties of the officer.

Interests of the Data Subject

An organization is able to collect, use, and disclose personal data without consent where it is in the interests of the individual in question. Under the PDPA, the collection, use, or disclosure of personal data is permitted without the consent of the individual where (non-exhaustively):

- The disclosure is necessary for any purpose which is clearly in the interest of the individual, if consent for its disclosure cannot be obtained in a timely way.
- The disclosure is necessary to respond to an emergency that threatens the life, health, or safety of the individual or another individual.

Public Interest

Whilst there is no exception for public interest per se, an organization can collect, use, and disclose personal data where it is in the national interest.

Under the PDPA, amongst others, the collection, use, or disclosure of personal data is permitted without the consent of the individual where the collection, use, or disclosure is necessary in the national interest, and where the collection, use or disclosure is necessary for any investigation or proceedings, if it is reasonable to expect that seeking the consent of the individual would compromise the availability or the accuracy of the personal data.

Legitimate Interests of the Data Controller

The Amendment Act introduced a new basis for the collection, use, or disclosure of personal data without consent, which is on the basis of legitimate interests of the organization. Under this new exception, organizations may collect, use, and disclose personal data about an individual if it is in the legitimate interests of the organization or another person, and those legitimate interests outweigh any adverse effect on the individual. In this regard, the organization is required to conduct an assessment to identify any adverse effect that the proposed collection, use, or disclosure is likely to have on the individual, and identify and implement reasonable measures to eliminate, reduce the likelihood of or mitigate the adverse effect on the individual. While it may be possible that this exception applies in the context of digital advertising, the necessary assessment of the organization's interests versus any adverse effect on individuals should be done to confirm if this exception could be applied. In practice, while it is arguable that digital advertising could fall under this new exception (with the required assessment outlined above), we have not found a specific instance that digital advertising was determined to be in the legitimate interests of an organization.

Business Improvement and Research

Another new exception that has been introduced into the PDPA by the Amendment Act is the business improvement exception. Organizations may use, without consent, personal data that they collected in accordance with the Data Protection Provisions of the PDPA for business improvement purposes, which includes operational efficiency and service improvements, and developing or enhancing products or services, amongst others. This exception can be

relied upon only for purposes that a reasonable person may consider appropriate in the circumstances and where the purpose cannot be achieved without the use of the personal data.

The PDPA's research exception has also been amended under the Amendment Act. This exception enables organizations to conduct broader research and development that may not have any immediate application to their products, services, business operations, or market using personal data they have collected.

4.5.2. Application to Digital Advertising

- **Does the law or legal guidance require a specific legal basis for specific digital advertising activities? Clarify for each activity (suggest using TCF/IAB CCPA "purposes") ("profiling" must be addressed here).**

No, the PDPA does not require a specific legal basis for specific digital advertising activities.

Unlike IAB CCPA, where we understand that creating personalized ad profiles and creating personalized content profiles are not permitted when California consumers exercise their right to opt-out, the PDPA does not regulate business purposes. Rather, as stated above, in general the touchstone under the PDPA is whether the specific digital advertising activities involve the collection, use, or disclosure of personal data. Thus, if an individual does not consent to the collection, use, or disclosure for profiling of his personal data the organization cannot profile the individual unless otherwise authorized or permitted under law, including under the business improvement exception of the PDPA.

- **If yes, what are the legal bases (e.g., consent, legitimate interest)? Are there any requirements related to lawful basis (need a valid legal basis to process)/fairness (scope of processing is fair)/transparency (transparent about the processing activity to the consumer and the lawful basis)?**

The PDPA is primarily a consent-based regime in respect of personal data protection. As long as an organization is in compliance with the Data Protection Provisions, including the Consent Obligation, Purpose Limitation Obligation, and Notification Obligation, the organization will be able to collect, use, and disclose personal data.

Thus, if an individual has been notified of the purposes for which his personal data would be collected, used, or disclosed, and gives consent for the collection, use, or disclosure of his personal data for such purposes, the organization would be able to collect, use, and disclose personal data for that purpose.

- **Does the law address processing for secondary purposes/differing purposes from which it was collected?**

Yes, it does.

Ultimately, under the Consent Obligation, consent must be given by the individual for the purposes for which his personal data will be collected, used, or disclosed. If the collection, use, or disclosure of personal data is for

purposes for which the individual had not been informed of before the collection of the personal data, section 20(1)(b) requires that the organization inform the individual about the additional purpose of the use or disclosure of personal data.

4.6. Safeguards

4.6.1. Overview

Generally, section 24 of the PDPA requires an organization to make reasonable security arrangements to protect personal data in its possession or under its control in order to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal, or similar risks. As stated in the PDPC's Key Concepts Guidelines, each organization should consider adopting security arrangements that are reasonable and appropriate under the circumstances. It might be useful for organizations to undertake a risk assessment exercise to ascertain whether their information security arrangements are adequate. There are various good practices recommended by PDPA that are elaborated under the respective sections in this guide.

4.6.2. Application to Digital Advertising

As stated above, the obligations set out under the PDPA in respect of personal data protection are of general application, and does not include any sector-specific provisions, including in respect of digital advertising. Additionally, there have not been any guidelines published by the PDPC that apply to the digital advertising industry.

To comply with the Protection Obligation, organizations should consider adopting security arrangements that are reasonable and appropriate in the circumstances.

In this regard, the PDPC has stated in its Key Concepts Guidelines that organizations may implement the following security arrangements:

- Ensuring computer networks are secure.
- Adopting appropriate access controls (e.g., considering stronger authentication measures where appropriate).
- Encrypting personal data to prevent unauthorized access.
- Activating self-locking mechanisms for the computer screen if the computer is left unattended for a certain period.
- Installing appropriate computer security software and using suitable computer security settings.
- Disposing of personal data in IT devices that are to be recycled, sold, or disposed.
- Using the right level of email security settings when sending and/or receiving highly confidential emails.
- Updating computer security and IT equipment regularly.

- Ensuring that IT service providers can provide the requisite standard of IT security.

5. DATA SUBJECT RIGHTS/EXEMPTIONS

5.1. Overview

In general, individuals are accorded certain rights under the PDPA which enable them to better control the collection, use, and disclosure of their personal data. One of these, which has been discussed in the context of the Consent Obligation, is the ability to withdraw consent.

5.2. Access

Organizations are subject to the Access Obligation. An organization must allow an individual to access his personal data in its possession or under its control upon request.

The organization has a duty to respond to applicants' requests to access their personal data as accurately and completely as necessary and reasonably possible, subject to the exceptions in the Fifth Schedule of the PDPA. On receipt of individuals' requests, the organization is obliged to provide the individuals, as soon as reasonably possible, with:

- Personal data about them that is in the possession or under the control of the organization.
- Information about the ways in which that personal data has been or may have been used or disclosed by the organization within a year before the date of the request.

An organization should provide a copy of each applicant's personal data in documentary form or any other form requested by the individual as is acceptable by the organization. If it is impracticable, the organization may allow the individual a reasonable opportunity to examine the personal data.

Under the Access Obligation, organizations may charge applicants a reasonable fee to respond to access requests. In doing so, an organization must provide the applicant with a written estimate of the fee. If the organization wishes to charge a fee that is higher than the written estimate, it will need to notify the applicant in writing of the higher fee. An organization does not have to respond to an applicant's access request unless the applicant agrees to pay the fee. In contrast, an organization is not entitled to impose a fee for correction requests.

There are certain exceptions whereby organizations can withhold access to an individual's personal data. For example, when such access will reveal personal data about another individual or will be contrary to the national interest; if the burden or expense of providing access would be unreasonable to the organization or disproportionate to the individual's interest; or if the request is otherwise frivolous or vexatious. In addition to the Fifth and Sixth Schedule to the PDPA, more specific rules concerning the Access and Correction Obligations may be found in Part II of the PDP Regulations.

Additionally, once the changes in the Amendment Bill come into effect, an organization which refuses to provide access to personal data requested by an individual under the Access Obligation must preserve a complete and accurate copy of the personal data concerned for not less than the prescribed period.

An organization must respond to an access request as soon as reasonably possible from the time the access request is received. If an organization is unable to respond to an access request within 30 days after receiving the request, the organization must inform the individual in writing within 30 days of the time by which it will be able to respond to the request.

5.3. Rectify

Correction Obligation

Organizations are subject to the Correction Obligation. An organization must allow an individual to correct his personal data in its possession or under its control upon request.

Individuals have the right to request an organization to correct any inaccurate data that is in the organization's control, subject to the exceptions in the Sixth Schedule of the PDPA. Unlike access requests, there is no prescribed duty to respond to a correction request, however, an organization must be satisfied on reasonable grounds that a correction should not be made. If no correction is made, the organization shall annotate the personal data in its possession or under its control with the correction that was requested but not made. Furthermore, organizations are required to send the corrected or updated personal data to specific organizations to which the data was disclosed within a year before the correction was made, unless those organizations do not need the corrected data for any legal or business purpose.

Upon receipt of an access or correction request, if the organization cannot comply within 30 days, it must inform the individual in writing of the time by which it will respond to the request.

Accuracy Obligation

Organizations are subject to the Accuracy Obligation. In particular, an organization must make a reasonable effort to ensure that personal data collected by it is accurate and complete, if it is likely to use such personal data to make a decision that affects the individual concerned or disclose such personal data to another organization.

This would generally require organizations to make a reasonable effort to ensure that:

- The personal data collected (whether directly from the individual concerned or through another organization) is accurately recorded.
- The personal data collected is complete.
- Appropriate steps have been taken to ensure the accuracy and correctness of the personal data.

- They have considered whether it is necessary to update the personal data.

Minors: As stated in the PDPC's Selected Topics Guidelines, when establishing measures to comply with the Accuracy Obligation under the Data Protection Provisions, organizations should also consider taking extra steps to verify the accuracy of personal data about a minor, especially where such inaccuracy may have severe consequences for the minor.

5.4. Deletion/Erasure

Individuals have no right in Singapore to request for an organization to destroy or delete the personal data in the organization's possession or control.

Although an individual may withdraw consent for the collection, use, or disclosure of his personal data, the PDPA does not require an organization to delete or destroy the individual's personal data upon request. With regard to personal data that is already in an organization's possession, the PDPC's Key Concepts Guidelines clarifies that the withdrawal of consent would only apply to an organization's continued use or future disclosure of the personal data concerned.

Upon receipt of a notice of withdrawal of consent, the organization must cease to collect, use, or disclose the individual's personal data, and inform its data intermediaries and agents about the withdrawal and ensure that they cease collecting, using, or disclosing the personal data for the various purposes.

However, under the Retention Limitation Obligation, organizations are required to cease retention of documents containing personal data, when it is reasonable to assume that (a) the purpose for which such personal data was collected is no longer served by the retention of personal data, and (b) such retention is no longer necessary for legal or business purposes. Thus, whilst organizations are not required to accede to an individual's request for the deletion of that individual's personal data, organizations must cease to retain such individual's personal data when it has no legal or business purpose for the retention of that personal data.

Further, if any organization fails to comply with any of the above requirements and thereby contravenes the PDPA, the PDPA may direct the organization to delete or destroy personal data that was collected, used, or retained in contravention of the PDPA. Hence, individuals may obtain this as a remedy by making a complaint to the PDPC.

5.5. Restriction on Processing

There is no separate right on restriction on processing under the PDPA, so long as the Consent Obligation is adhered to, including that the individual's valid consent is given for that purpose, and the purpose is one that a reasonable person would consider appropriate in the circumstances. We also highlight that consent would not need to be obtained if an exception to the Consent Obligation applies.

5.6. Data Portability

At present, individuals do not have a right to data portability. However, once these amendments under the Amendment Act come into force (expected in early 2022), individuals would have the right to request for their personal data to be ported across organizations. Individuals may make a data porting request to an organization, and upon receiving the data porting request, the porting organization must (unless an exception applies) transmit the applicable data specified in the data porting request to the receiving organization in accordance with any prescribed requirements, such as requirements relating to technical, user experience, and consumer protection matters.

5.7. Right to Object

While there is no separate right to object, under the PDPA, individuals have the right to give and withdraw consent at any time by giving reasonable notice.

With regard to the withdrawal of consent, individuals should be aware that the withdrawal of certain types of consent may affect the ability of the organization to continue providing them with the requested services.

Section 16 of the PDPA provides that individuals may at any time withdraw any consent given or deemed to have been given under the PDPA in respect of the collection, use, or disclosure of their personal data for any purpose by an organization. In general, organizations must allow an individual who has previously given (or is deemed to have given) his consent to the organization for collection, use, or disclosure of his personal data for a purpose to withdraw such consent by giving reasonable notice. However, the organization may continue the collection, use, or disclosure of personal data if one of the exceptions to the requirement to obtain consent applies.

The PDPC has stated in its Key Concepts Guidelines that it would consider a period of at least ten (10) business days from the day the organization receives the withdrawal notice to be reasonable notice. Should an organization require more time to give effect to a withdrawal notice, it is good practice for the organization to inform the individual of the time frame by which the withdrawal of consent will take effect.

Typically, where the withdrawal notice for marketing contains a general withdrawal message, i.e., it is not clear as to the channel of receiving marketing messages for which consent is withdrawn, the PDPC will consider any withdrawal of consent for marketing sent via a particular channel to only apply to all messages relating to the withdrawal sent via that channel.

5.8. Right Against Automated Decision-Making

The PDPA does not expressly provide for automated decision-making. Individuals have no right under the PDPA to "opt-out" from automated decision-making.

5.9. Responding to Consumer Rights Requests

There are several different requests an individual may make under the PDPA, which are:

- Notice of Withdrawal of Consent
- Request for Access to Personal Data
- Request for Correction of Personal Data

Notice of Withdrawal of Consent

In respect of an individual's notice for the withdrawal of consent, there is no prescribed format for such a notice under the PDPA. However, once an organization has received from an individual a notice to withdraw consent, the organization is required under the PDPA to inform the individual concerned of the likely consequences of withdrawing his consent.

Once reasonable notice of withdrawal of consent has been given, the organization must cease to collect, use, or disclose the individual's personal data, and inform its data intermediaries and agents about the withdrawal and ensure that they cease collecting, using, or disclosing the personal data for the various purposes. Apart from its data intermediaries and agents, an organization is not required to inform other organizations to which it has disclosed an individual's personal data of the individual's withdrawal of consent.

Although an individual may withdraw consent for the collection, use, or disclosure of his personal data, the Key Concepts Guidelines clarifies that the PDPA does not require an organization to delete or destroy the individual's personal data upon request. Organizations may retain personal data in their documents and records in accordance with the Data Protection Provisions. Typically, where the withdrawal notice for marketing contains a general withdrawal message, i.e., it is not clear as to the channel of receiving marketing messages for which consent is withdrawn, the Commission will consider any withdrawal of consent for marketing sent via a particular channel to only apply to all messages relating to the withdrawal sent via that channel.

Although a time limit is not expressly provided for in the PDPA, the PDPC has stated in its Key Concepts Guidelines that it is good practice for the organization to inform the individual of the time frame by which the withdrawal of consent will take effect if the organization will require more than ten business days to give effect to a withdrawal notice.

Request for Access to Personal Data

In respect of access requests, when an access request has been made to an organization, the organization is obliged under the Access Obligation to provide the individual access to the complete set of personal data requested by the individual which is in the organization's possession or under its control, unless the access request is calls within one of the exceptions under the Fifth Schedule of the PDPA (e.g., if the burden or expense of providing access would be unreasonable to the organization or disproportionate to the individual's interests or if

the request is otherwise frivolous or vexatious).

Under regulation 3 of the PDP Regulations, an access request must be able to identify:

a) The applicant making the request.

b) The personal data and use and disclosure information requested by the applicant.

The PDP Regulations also require that a request must be sent to the organization's DPO, or in such other manner as is acceptable to the organization.

Practically, as set out in the Key Concepts Guidelines, when responding to an access request, the organization should consider the purpose of the applicant's access request, to determine the appropriate manner and form in which access to the personal data should be provided. Generally, the organization's actual response would depend on the specific request, and organizations are reminded that in meeting their responsibilities under the PDPA, they are to consider what a reasonable person would consider appropriate in the circumstances.

Before responding to an access request, the Key Concepts Guidelines clarifies that organizations should exercise due diligence and adopt appropriate measures to verify an individual's identity. While the PDPA does not prescribe the manner in which organizations are to obtain verification from the individual making an access request, organizations are encouraged to have documentary evidence to demonstrate that it is in compliance with the PDPA, and to minimize any potential disputes. Organizations may implement policies setting out the standard operating procedures on conducting verification when processing access requests.

An organization must respond to an access request as soon as reasonably possible from the time the access request is received. Under regulation 5 of the PDP Regulations, an organization is required to respond to the access request as soon as reasonably possible. If an organization is unable to respond to an access request within 30 days after receiving the request, the organization shall inform the individual in writing within 30 days of the time by which it will be able to respond to the request.

Additionally, regulation 7 of the PDP Regulations allows an organization to charge an individual a reasonable fee to process an access request by the individual. The Key Concepts Guidelines clarifies that the purpose of the fee is to allow organizations to recover the incremental costs of responding to the access request. If an organization wishes to charge an individual a fee to process an access request, the organization must give the individual a written estimate of the fee. If the organization wishes to charge a fee higher than the original written estimate, it must inform the individual in writing of the increased fee. The organization may refuse to process or provide access to the individual's personal data until the individual agrees to pay the relevant fee.

An organization is to provide a reply to the individual even if the organization is not providing access to the requested personal data or other requested information. In such a situation, and where appropriate, organizations

should, as good practice, inform the individual of the relevant reason(s), so that the individual is aware of and understands the organization's reason(s) for its decision.

Correction Request

In respect of correction requests, this would be similar to access requests in most ways.

A correction request would need to (a) identify the applicant making the request, and (b) identify the correct request by the applicant. Additionally, the request must be sent to the organization's DPO, or in such other manner as is acceptable to the organization.

Organizations are required to respond to a correction request as soon as practicable, but if it is unable to comply with that requirement within 30 days after receiving a request, the organization must within that time inform the applicant in writing of the time by which it will respond to the request.

Importantly, under a correction request, unlike in the case of an access request, organizations are not allowed to charge any fee to respond to a correction request.

5.10. Record Keeping Concerning Rights Requests

In respect of access requests, the Amendment Act introduced a requirement under the new Section 22A of the PDPA, which states that if an organization refuses to give an individual access to his or her personal data on request, the organization must preserve a complete and accurate copy of the personal data for a prescribed period after rejecting the access request.

In respect of correction requests, if the organization is satisfied upon reasonable grounds that a correction should not be made, section 22(5) of the PDPA requires the organization to annotate (i.e., make a note to) the personal data in its possession or under its control indicating the correction that was requested but not made. As good practice, the PDPC has suggested in its Key Concepts Guidelines that the organization may also wish to annotate the reasons and explain to the individual why it has decided that the correction should not be made.

5.11. Is Providing Consumers with These Rights Required by Law or Mere Suggestions?

Any "rights" that are derived from the PDPA, or its subsidiary legislation (e.g., PDP Regulations) are required under law. However, guidelines issued by the PDPC, on the other hand, are not legally binding.

5.12. Application to Digital Advertising

To date, there is no sector-specific legislation on digital advertising. The Data Protection Provisions under the PDPA apply to the organizations in the digital advertising industry as it would to all other organizations generally, unless one of the exceptions under the PDPA applies. Hence all parties involved in the digital advertising "chain" which are in Singapore, or which have collected personal data in circumstances that amounts to data processing in Singapore

(specifically, through the ad and related monitoring tools on the publisher's website in Singapore), must provide the rights of access, correction, and data portability (when the relevant provisions come into force). More significantly, the parties must also cease to use personal data when the individual has withdrawn consent.

6. DATA CONTROLLER AND PROCESSOR AGREEMENTS

6.1. Overview

The PDPA draws a distinction between an 'organization' and a 'data intermediary' in relation to the processing of personal data. The relevant definitions as set out in section 2(1) of the PDPA are as follows:

An 'organization' is defined as any individual, company, association, or body of persons, corporate or unincorporated, whether or not:

- Formed or recognized under the law of Singapore.
- Resident, or having an office or a place of business, in Singapore.

A 'data intermediary' is defined as an organization which processes personal data on behalf of another organization but does not include an employee of that other organization.

'Processing' is defined as the carrying out of any operations or set of operations in relation to the personal data, and includes any of the following:

- Recording
- Holding
- Organization, adaptation, or alteration
- Retrieval
- Combination
- Transmission
- Erasure or destruction

If an organization is not a data intermediary, it is subject to the full set of data protection obligations under the PDPA. In contrast, as elaborated on in section 2.1 above, other than the Protection Obligation, the Retention Limitation Obligation, and the duty to notify the organization/public agency of a data breach, no other data protection obligations are imposed on a data intermediary, whereby it is processing personal data for or on behalf of an organization pursuant to a contract in writing. Therefore, to avoid both parties having to answer to the data

protection obligations to the full extent, the contract should state clearly the relationship and the rights and obligations of both parties.

Even if an organization engages a data intermediary to process personal data on its behalf and for its purposes, section 4(3) of the PDPA provides that it shall have the same obligations as if the personal data were processed by the organization itself. Therefore, effectively the organization will be required to comply with the Data Protection Provisions under the PDPA in respect of such personal data, as if it had processed such personal data itself.

Moreover, data intermediaries are typically subject to contractual obligations which necessitate compliance with the other obligations of the PDPA. According to the Key Concepts Guidelines, it is expected that organizations engaging data intermediaries would generally have imposed obligations that ensure protection in the relevant areas in the processing contract.

The PDPC on July 20, 2016 issued a non-legally binding Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data and provided sample data protection clauses that an organization purchasing services relating to the processing of personal data may include in the service agreements with the data intermediaries.

If the organization fails to put in place data protection clauses in such service agreements, the organization runs the risk of breaching its Protection Obligation by failing to take necessary actions and precautionary measures to protect such personal data.

6.2. Data Controller Outsourcing of Processing

The roles, responsibilities, and considerations for the organization (Data Controller) are encompassed within the PDPC's Guide to Managing Data Intermediaries – which is classified into (A) Governance and Risk Assessment, (B) Policies and Practices, (C) Service Management and (D) Exit Management. Nonetheless, we highlight that the guide issued by PDPC is not legally binding. Rather, the guide sets out best practices gleaned from previous data protection enforcement cases and includes measures that could be implemented to prevent similar issues from occurring.

We set out below a brief overview of the different sections of the Guide to Managing Data Intermediaries.

(A) Governance and Risk Assessment

The decision to outsource data processing activities to data intermediaries, along with the scope of these activities and the sensitivity of the processed personal data, must be determined by the senior management of the organization. In determining such decisions, the senior management must take into account the risks involved and set out relevant measures to mitigate such risks. They could also identify requirements that can be stated clearly in the contract with the data intermediary. More information on conducting such personal data risk assess-

ments and the possible mitigation approaches can be found in the PDPC's Guide to Data Protection Impact Assessments (DPIA). This is elaborated further in section 8.1.

(B) Policies and Practices

As stated in section 6.1, it is important to reiterate that the primary approach for the organization to appropriately and comprehensively protect the personal data processed by the data intermediary is through contract. It is essential for the scope of the outsourced data processing activities to be clearly defined and mutually agreed upon. Beyond that, the organization must consider and look into details like schedules to the contract and any further administrative instructions given to the data intermediary outside of the contract. These could be generated in collaboration with the data intermediary, given that it could possess the requisite technical or operational expertise and experience. Nonetheless, the responsibility falls on the organization.

(C) Service Management

Other than communicating and contracting the data protection policies, an accountable and responsible organization would also set up monitoring and reporting structures to manage the data intermediary. This would depend on the nature and extent of the outsourcing arrangement – which could include the establishment of regular Management meetings with the data intermediary personnel to ensure constant communication, proactive monitoring practices like the reviewing of document database logs and system logs, periodic audits, and on-site inspections, or even simulations and table-top exercises.

(D) Exit Management

Organizations should establish exit management plans to conclude their engagements with data intermediaries to ensure business continuity and provide the appropriate handling of personal data. This complies with the principle that an organization ceases to retain documents containing personal data when it no longer has access to those documents and the personal data they contain. Such measures for the exit management plan would include setting out clear time frames for the data intermediaries to cease retention of personal data, following the completion of the processing activities. This aligns with the Retention Limitation Obligation, which is explained in detail in section 9.1.

6.3. Data Processor Rights and Responsibilities

While the organization (i.e., the Data Controller) remains accountable for personal data that is being processed on their behalf by the data intermediary (i.e., the Data Processor), the data intermediary still possesses certain rights and responsibilities.

Generally, data intermediaries are subject mainly to the Protection Obligation under section 24 of the PDPA and the Retention Limitation Obligation under section 25 of the PDPA in respect of the personal data processed on behalf of another organization pursuant to a written contract.

For the Protection Obligation, the data intermediaries must comply with the necessary 'reasonable security

arrangements' set out to protect personal data from unauthorized access, collection, use, disclosure, or any similar risks, even though it is processing personal data on behalf of another organization. For the Retention Obligation, all data intermediaries must cease retention of documents containing personal data as soon as the retention no longer serves the purpose the personal data was collected for and is not necessary to hold the data for legal or business purposes.

Moreover, as stated in an article titled "Understanding the Role of Data Intermediaries in Data Protection and Retention," which was published in the February 2016 edition of DPO Connect (i.e., the PDPC's newsletter for Data Protection Officers), there are several points for data intermediaries to note.

Firstly, there is no 'one size fits all' solution in the protection of personal data by data intermediaries – hence, every organization should consider adopting security arrangements that are 'reasonable and appropriate' for their own unique circumstances – taking into account the nature of the data, the form in which it is collected, and the possible impact on individuals if the data is exposed.

Secondly, data intermediaries must ensure that all employees are cognizant of the importance of personal data protection – together with the policies and processes put in place to ensure that. This could possibly be enforced through employment terms and conditions.

Ultimately, the data intermediary is fully responsible under the PDPA for any activity that does not constitute processing personal data on behalf of another organization under the written contract. This would include any activity that involves collecting personal data on its own accord or using personal data for its own purposes.

In addition, the Amendment Act has introduced a new obligation for a data intermediary to notify its client organization of a data breach. Under this obligation, where a data intermediary has reason to believe that a data breach has occurred in relation to personal data that the data intermediary is processing on behalf of and for the purposes of another organization, the data intermediary must, without undue delay, notify that other organization of the data breach occurrence.

6.4. Application to Digital Advertising

To data, there is no existing legislation concerning data protection specific to digital advertising by data intermediaries. Nonetheless, it is important for the data intermediary to ensure that the individual's consent has been received to collect, secure, and disclose personal data for digital advertising.

Moreover, for data intermediaries that provide digital advertising services on behalf of an organization, they must comply with the PDPA, especially the obligations stated in section 6.3. We also emphasize the importance of including provisions in the written contract to clearly set out the data intermediaries' responsibilities and obligations, with respect to collecting, securing, and disclosing personal data for Digital Advertising purposes.

7. DATA TRANSFER & OUTSOURCING

7.1. Overview

Organizations are subject to the Transfer Limitation Obligation under section 26 of the PDPA. An organization must not transfer personal data to a country or territory outside Singapore except in accordance with the requirements prescribed under the PDPA to ensure that the transferred personal data will be accorded a standard of protection that is comparable to that under the PDPA.

To do so, the organization must generally ensure that the recipients of such personal data are bound by legally enforceable obligations to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA. These 'legally enforceable obligations' include those imposed under law, contract, or Binding Corporate Rules (BCR), or any other legally binding instrument. More specific rules may be found in Part III of the PDP Regulations.

Any organization transferring personal data out of Singapore must generally ensure that the recipients of such personal data are bound by legally enforceable obligations to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA. In addition to this requirement, a contract imposing legally enforceable obligations must specify the countries and territories to which the personal data may be transferred under the legally enforceable obligations.

In relation to transfers of personal data outside of Singapore to related organizations, the PDPC has accepted BCRs as a form of such 'legally enforceable obligations,' which:

- Require every recipient of the transferred personal data to apply a standard of protection that is at least comparable to the protection under the PDPA.
- Specify the recipients of the transferred personal data to which the BCRs apply.
- Specify the countries and territories to which the personal data may be transferred under the BCRs.
- Specify the rights and obligations provided by the BCRs.

A recipient of personal data is considered 'related' to the transferring organization if:

- The recipient, directly or indirectly, controls the transferring organization.
- The recipient is, directly or indirectly, controlled by the transferring organization.
- The recipient and the transferring organization are, directly or indirectly, under the control of a common person.

There are a few express situations whereby an organization can be taken to have satisfied the requirement of taking

appropriate steps to ensure that the recipient outside Singapore is bound by legally enforceable obligations to protect personal data in accordance with comparable standards. These include:

- Where the individual consents to the transfer of the personal data to the recipient in that country.
- Where the transfer of the personal data to the recipient is necessary for the performance of a contract between the individual and the transferring organization, or to do anything at the individual's request with a view to the individual entering into a contract with the transferring organization.
- Where the transfer of personal data to the recipient is necessary for the conclusion or performance of a contract between the transferring organization and a third party which is entered into at the individual's request, or which a reasonable person would consider to be in the individual's interest.
- Where the transfer is necessary for a use or disclosure in certain situations where the consent of the individual is not required under the PDPA, subject to the organization taking reasonable steps to ensure that the personal data will not be used or disclosed by the recipient for any other purpose.
- Where the personal data is data in transit or publicly available in Singapore.

As set out under regulation 9(5) of the PDP Regulations, data subjects are allowed to withdraw any consent given for the transfer of personal data to a country or territory outside Singapore. Moreover, the data subject is not said to have consented to the transfer of personal data if:

- Where the individual was not, before giving consent, given a reasonable summary in writing of the extent to which the personal data to be transferred will be protected to a standard comparable to the protection under the PDPA.
- The transferring organization required the individual to consent to the transfer as a condition of providing a product or service.
- The transferring organization obtained or attempted to obtain the individual's consent for the transfer by providing false or misleading information about the transfer, or by using other deceptive or misleading practices.

7.2. Application to Digital Advertising

To date, there is no existing legislation concerning data protection specific to Digital Advertising in respect of cross border data transfer. Therefore, organizations based in Singapore that transfer personal data out of Singapore, whether for digital advertising purposes or otherwise, would be required to comply with the Transfer Limitation Obligation.

The digital shift has changed how personal data is being used and being transferred for the publishing of advertisements via digital mediums, especially concerning user data collection. A prime example of such transfers

would be when a user connects to a mobile application or website. In such a case, the personal data is sent to automatic bidding platforms, which is subsequently transferred to advertising intermediaries to locate potential clients.

Additionally, cloud-based advertising services have developed rapidly, with many digital advertisers moving towards the use of cloud-services. Cloud-based advertising generally refers to cloud-based services that support the selection, transaction and delivery of advertising and ad-related data, where content and prices are determined by end-users through auction mechanisms that match bidders with advertising impressions. This is applicable to search, display, mobile, social, and video advertisements. This way, cloud-based advertising can update and optimize advertisement campaigns in real-time.

In this regard, we note that the Selected Topics Guidelines includes a chapter on cloud services. This chapter provides guidance on the responsibilities of organizations when making use of cloud services for processing personal data. For organizations utilizing and transferring data to such cloud-based advertising services, the following should be noted:

- An organization that engages a cloud service provider (CSP) as a data intermediary to provide cloud services is responsible for complying with the Transfer Limitation Obligation in respect of any overseas transfer of personal data in using the CSP's cloud services. This is regardless of whether the CSP is located locally or overseas.
- An organization must ensure that any overseas transfer of personal data, in the course of engaging a CSP, is in accordance with the PDPA – where the organization ensures that the CSP only transfers data to locations with comparable data protection regimes or has legally enforceable obligations to ensure a comparable standard of protection. These measures can be specified in the written contract between the organization and the CSP.

In the event the arrangement with a CSP is more in the nature of a controller-to-controller transfer, the transferring organization would not be responsible for the CSP to the extent it acts as a controller (while retaining responsibility to the extent it acts as a data intermediary for the organization). Nevertheless, the same requirements in respect of transfers would apply in a controller-to-controller situation.

Ultimately, organizations should review and take note of contracts with CSPs, to ensure that such contracts include appropriate provisions on the transfer of personal data, the overseas locations to which the data can be transferred to, and the security measures that will be put in place for the protection of the data (including allowing the organization the right to audit the CSP's security measures, or to require the CSP to possess industry certifications).

8. AUDIT/ACCOUNTABILITY

8.1. Overview

Data Processing Records

There is no obligation imposed on an organization to maintain any data processing records. However, all organizations should ensure that they comply with the Data Protection Provisions of the PDPA in carrying out their data activities.

Data Protection Impact Assessments

At present, there is no obligation imposed on an organization to put in place a Data Protection Impact Assessment ('DPIA'). However, once the changes introduced in the Amendment Bill come into force, certain provisions will require assessments (which may be narrower in scope than a full DPIA) to be done by an organization. For example, an organization that intends to rely on deemed consent by notification will be required to conduct an assessment to determine that the proposed collection, use, or disclosure of personal data is not likely to have an adverse effect on the individual. For such an assessment, the organization must:

- Identify any adverse effect that the proposed collection, use, or disclosure of the personal data for the purpose concerned is likely to have on the individual.
- Identify and implement reasonable measures to (i) eliminate the adverse effect; (ii) reduce the likelihood that the adverse effect will occur; or (iii) mitigate the adverse effect.
- Comply with any other prescribed requirements.

In addition, we highlight that whilst DPIAs are currently not mandatory under the PDPA, the PDPC has published a Guide to Data Protection Impact Assessments. In it, the PDPC states that the DPIA is a tool that allows organizations to 'be better positioned to assess if their handling of personal data complies with the PDPA or data protection best practices and implement appropriate technical or organizational measures to safeguard against data protection risks to individuals'.

- **Audit - What audit rights are dictated by law (e.g., must companies have audit rights over their vendors? Does it matter what the classification of those vendors are?)**

For organizations that have delegated work to vendors or data intermediaries, the organization remains liable to comply with the Data Protection Provisions of the PDPA for the personal data collected and processed. However, to date, there are no mandatory audit rights under law for companies over their vendors – instead, the audit rights over vendors must be clearly specified within the agreements between the companies and vendors.

As stated in section 6.2 of the Guide to Managing Data Intermediaries, the parties can set out monitoring and reporting structures to manage the vendors, in their carrying out of data processing activities. In setting out such

structures, the company can consider conducting audit exercises, requesting an independent audit report or having on-site inspections at the vendors' premises. Such audit remediation measures are essential in ensuring that any data protection risks are addressed efficaciously.

- **Accountability - Must companies/vendors keep certain records to prove they have met certain requirements? What are those requirements?**

Since the implementation of the PDPA, the principle of accountability has been implied in sections 11 and 12 of the PDPA. In the recent amendment to PDPA, the Amendment Act inserted an express reference to accountability – stating that organizations are accountable for personal data in their possession or under their control. This evinces the importance of the principle and highlights centrality in personal data protection.

In July 2019, the PDPC updated the Key Concepts Guidelines to include the Accountability Obligation as a Data Protection Provision (previously the Openness Obligation). The PDPC also published the Guide to Accountability Under the PDPA, which explains accountability principles in the context of personal data protection and how an organization may demonstrate accountability for personal data in its care.

The amendments to the PDPA have also introduced a framework for mandatory notification to the PDPC when a data breach takes place. Under Clause 13 of the Amendment Bill, organizations must notify the PDPC and/or the affected individuals of any data breaches that satisfy certain criteria. This amendment is merely one example of this shift towards an accountability-based approach in PDPC's approach towards personal data protection.

8.2. Application to Digital Advertising

To date, there is no existing legislation concerning data protection specific to digital advertising for audit and record keeping purposes.

9. DATA RETENTION

9.1. Overview

The Retention Limitation Obligation in section 25 of the PDPA requires an organization to dispose of its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data, and such retention is no longer necessary for legal or business purposes.

The PDPA does not prescribe a specific retention period for personal data and the duration of time whereby an organization can legitimately retain personal data is assessed on a standard of reasonableness, having regard to the purposes for which the personal data was collected and retained. Accordingly, legal, or specific

industry-standard requirements in relation to the retention of personal data may apply.

Where there is no longer a need for an organization to retain personal data, the organization should cease to do so. An organization will be deemed to have ceased to retain personal data when it no longer has access to the documents and the personal data they contain, or when the personal data is otherwise inaccessible or irretrievable to the organization. In considering whether an organization has ceased to retain personal data the PDPC will consider the following factors in relation to the personal data:

- Whether the organization has any intention to use or access the personal data.
- How much effort and resources the organization would need to expend to use or access the personal data again.
- Whether any third parties have been given access to that personal data.
- Whether the organization has made a reasonable attempt to destroy, dispose of, or delete the personal data in a permanent and complete manner.

9.2. Application to Digital Advertising

To date, there is no existing legislation concerning data protection specific to digital advertising for data retention. Nonetheless, the PDPC has published certain enforcement decisions relating to the application of the PDPA to digital advertising companies.

In *Re Social Metric Pte Ltd [2017] SGPDPC 17*, Social Metric is a digital marketing agency that provides social media marketing services by collecting personal data of its clients' customers for purposes like customer engagement and analysis of customer demographics. The agency created nine webpages on its website and listed out the personal data of the individuals that it collected from. The Commissioner found that Social Metric had breached the Retention Limitation Obligation, because it retained the personal data of its clients' customers even after the social media campaign was over, and it failed to show that it had any purpose for such retention pursuant to the Retention Limitation Obligation.

At the time of collection, organizations carrying out collection of personal data on behalf of its clients for marketing and advertising campaigns may be considered data intermediaries. However, it must be noted that when the marketing campaign ends and the organization holds on to the personal data for a period of time that is more than reasonable, the organization may not be deemed a data intermediary. Instead, it would assume the full data protection responsibilities of an 'organization' under the PDPA.

In that case, it was noted that limbs (a) and (b) of section 25 of the PDPA is conjunctive – hence if the organization still needs to retain personal data to (a) serve the purpose for which the personal data was collected for or (b) to serve any legal or business purposes, the organization is allowed to retain such personal data.

10. DATA PROTECTION AUTHORITY | REGULATORY AUTHORITY

10.1. Overview

Before the PDPA was enacted in 2012, Singapore had no overarching legislation to govern the protection of personal data. The PDPA is a general data protection law which applies to all private sector organizations and establishes the PDPC and the Data Protection Advisory Committee (DPAC).
More information on the PDPC is provided below.

10.2. Main Regulator for Data Protection

The PDPC is the regulatory authority that is responsible for administering and enforcing the PDPA. It is part of the converged telecommunications and media regulator, the Infocomm Media Development Authority ('IMDA'), which is in turn a statutory body under the purview of the Ministry of Communications and Information.

Meanwhile, the DPAC provides advice to the PDPC on matters concerning the review and administration of the personal data protection framework, with the example of key policy and enforcement issues. Sector-specific data protection obligation may be separately enforced by the relevant sectoral regulators.

10.3. Main Powers, Duties and Responsibilities

The main powers, duties, and responsibilities of the PDPC are as follows:

- To promote awareness of data protection in Singapore.
- To provide consultancy, advisory, technical, managerial, or other specialist services relating to data protection.
- To advise the Government of Singapore on all matters relating to data protection.
- To represent the Government internationally on matters relating to data protection.
- To conduct research and studies, promote educational activities relating to data protection, including organizing and conducting seminars, workshops, and symposia relating thereto, and support other organizations conducting such activities.
- To manage technical cooperation and exchange in the area of data protection with other organizations, including foreign data protection authorities and international or inter-governmental organizations, on its own behalf or on behalf of the Government.
- To administer and enforce the PDPA.
- To carry out functions conferred on the PDPC under any other written law.

- To engage in such other activities and perform such functions as the Minister may permit or assign to the PDPC by order published in the Gazette.

10.4. Application to Digital Advertising

The PDPA applies to all private sector organizations in Singapore, regardless of their scale or size. The PDPC has published several sector-specific advisory guidelines to clarify the application of the PDPA in these specific sectors. However, to date, there are no specific advisory guidelines for the domain of digital advertising or marketing in Singapore.

Nonetheless, the PDPC has issued decisions relating to digital advertisers that have been found to have contravened data protection provisions under the PDPA. These decisions usually involve organizations that provide advertising and marketing services to clients by assisting in collecting and storing personal data. For this category of enforcement decisions, the case of *Re Social Metric Pte Ltd*, as mentioned in section 9.2, involves the breach of the Retention Limitation and Protection Obligations of the PDPA, while the case of *Re O2 Advertising Pte Ltd [2019] SGPDPC 32* involves the breach of the Protection, Retention Limitation and Accountability Obligations.

Furthermore, another common type of enforcement decision which may be relevant to digital advertisers revolves around whether the organization had complied with the Consent Obligation to obtain valid consent before collecting, using, or disclosing personal data (under section 13 of the PDPA) and the Purpose Limitation Obligation (under section 18 of the PDPA) to only use and disclose personal data for relevant purposes (e.g., for marketing/advertising or otherwise). Examples are *Re Spring College International Pte Ltd [2018] SGPDPC 15* and *Re Aventis School of Management Pte Ltd [2018] SGPDPC 7*.

11. SANCTIONS

11.1. Overview

The PDPC is responsible for enforcing the PDPA. Where the PDPC is satisfied that an organization has breached the Data Protection Provisions under the PDPA, the PDPC is empowered with wide discretion to issue such remedial directions as it thinks fit. These include directions requiring the organization to:

- Stop collecting, using, or disclosing personal data in contravention of the PDPA.
- Destroy personal data collected in contravention of the PDPA.
- Provide access to or correct personal data.
- Pay a financial penalty of up to SGD 1 million (approx. €617,600).

We highlight that for the breach of any Data Protection Provision, the Amendment Bill introduces a higher financial penalty of up to 10% of an organization's annual turnover in Singapore, or SGD 1 million (approx. €617,600), whichever is higher.

In the course of its investigation, the PDPC has certain investigative powers, which include:

- By notice in writing, requiring an organization to produce any specified document or specified information.
- By giving at least two working days' advance notice of intended entry, entering into an organization's premises without a warrant.
- Obtaining a search warrant to enter an organization's premises and take possession of, or remove, any document.

Non-compliance with certain provisions under the PDPA may also constitute an offence, for which a fine or a term of imprisonment may be imposed. The quantum of the fine and the length of imprisonment (if any) vary, depending on which provisions are breached.

For instance, a person found guilty of making requests to obtain access to or correct the personal data of another without authority may be liable on conviction to a fine not exceeding SGD 5,000 (approx. €3,090) or to imprisonment for a term not exceeding 12 months, or both (section 51(2) of the PDPA).

The Amendment Bill has also introduced further enforcement powers and offences. For instance, under the new section 48F of the PDPA, an individual commits an offence if he takes any action to re-identify or cause re-identification of a person to whom anonymized information in the possession or under the control of an organization or a public agency relates, where the re-identification is not authorized by the organization or public agency, and the individual either knows that the re-identification is not authorized or is reckless as to whether the re-identification is or is not authorized. The penalty is a fine not exceeding SGD 5,000 (approx. €3,090) or to imprisonment for a term not exceeding two years, or both.

An organization or person who obstructs or impedes the PDPC or an authorized officer, or knowingly or recklessly makes a false statement to the PDPC, or knowingly misleads or attempts to mislead the PDPC in the exercise of their powers or performance of their duties under the PDPA, commits an offence for which that person would be liable upon conviction to a fine of up to SGD 10,000 (approx. €6,180) and/or to imprisonment for a term of up to 12 months (in the case of an individual), or a fine of up to SGD 100,000 (approx. €61,770) (in any other case). Additionally, once the Amendment Bill comes into effect, any person who neglects or refuses to comply with an order to appear before the PDPC, or without reasonable excuse neglects or refuses to furnish any information or produce any document specified in a written notice to produce information, will be guilty of an offence punishable by a fine not exceeding SGD 5,000 (approx. €3,090) or to imprisonment for a term not exceeding 12 months, or both.

An aggrieved individual or organization may make a written application to the PDPC to reconsider its direction or decision. Thereafter, any individual or organization aggrieved by the PDPC's reconsideration decision may lodge an appeal to the Data Protection Appeal Panel. Alternatively, an aggrieved individual or organization may appeal directly to the Data Protection Appeal Panel without first submitting a reconsideration request. A direction or

decision of the Data Protection Appeal Panel (via the Data Protection Appeal Committee) may be appealed to the High Court on a point of law or where such decision relates to the amount of a financial penalty. The decision of the High Court may be further appealed to the Court of Appeal.

An individual who suffers loss or damage directly as a result of a contravention of the provisions of the PDPA may also commence a private civil action. However, such a right of private action is only exercisable after all avenues of appeal, in respect of the relevant infringement decision issued by the PDPC, have been exhausted.

11.2. Liability

- **Scope of liability for publishers and advertisers for processing activities of ad tech companies.**

To date, there is no specific legislation that details the scope of liability for publishers and advertisers for processing activities of ad tech companies.

In relation to liability under the PDPA, ad tech companies process and analyze the data for online advertising campaigns, often on behalf of publishers and advertisers. Accordingly, in such a situation, they are likely to fall within the definition of 'data intermediary' under section 2 of the PDPA. In respect of processing of personal data on behalf of and for the purposes of another organization pursuant to a contract which is evidenced or made in writing, the data intermediary is only liable for the Protection and Retention Limitation Obligations.

However, for such publishers and advertisers engaging such ad tech companies, these organizations have the same obligation under the PDPA in respect of personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organization itself. Refer to section 6 for more details. In situations where the ad tech company is acting as a data controller (at least in some aspects of its processing of personal data), the publishers and advertisers would not be liable for non-compliance by the ad tech company.

- **Scope of liability for ad tech companies for collection activities of publishers and advertisers.**

To date, there is no legislation regarding the scope of liability for ad tech companies in relation to the collection activities of publishers and advertisers.

As stated above, in relation to liability under the PDPA, to the extent that such ad tech companies may be considered data intermediaries processing personal data on behalf of and for the purposes of another organization pursuant to a contract which is evidenced or made in writing, the data intermediary is only liable for the Protection and Retention Limitation Obligations.

However, if for any reason the ad tech company processes the personal data collected by publishers and advertisers in a manner which is not in accordance with its obligations as a data intermediary (e.g., out of the scope of the contract), it may be considered a data controller (i.e., an organization) and be liable under the full suite of the

Data Protection Provisions.

- **Scope of liability for ad tech companies for other ad tech companies they enable to process data (either b/c they make the decision of pub or advertisers or agency dictates it).**

Insofar as an ad tech company engages other organizations to process personal data on their behalf, those other organizations may be considered data intermediaries for the ad tech company. Under the PDPA, data intermediaries which that process personal data on behalf of and for the purposes of another organization pursuant to a contract which is evidenced or made in writing are only subject to the Protection Obligation and the Retention Limitation Obligation in respect of the personal data they process (section 4(2), PDPA). The rest of the data protection obligations remain with the primary organization (i.e., the ad tech company) which has possession or is in control of the personal data.

11.3. Enforcement and Market Practice

- **How are claims raised under the law?**

The PDPC takes a complaints-based approach towards the enforcement of Data Protection Provisions. Nonetheless, the PDPC is also empowered statutorily to commence investigations on its own accord.

Upon the receipt of a complaint or on its own accord, the PDPC may initiate investigations to determine whether the relevant organization has been compliant with the PDPA. Part IV of the Advisory Guidelines on Enforcement of the Data Protection Provisions sets out certain factors which the PDPC may take into account in determining whether to commence an investigation. Such factors include, among others:

- Whether the organization may have failed to comply with all or a significant part of its obligations under the PDPA.
- Whether the organization's conduct indicates a systemic failure by the organization to comply with the PDPA.
- Whether the complainant had previously approached the organization to seek a resolution of the issues in the complaint but failed to reach a resolution.
- Whether the PDPC has sought to facilitate dispute resolution between the complainant and the organization.
- Whether the PDPC has commenced a review, whether the organization has complied with its obligations under the Personal Data Protection (Enforcement) Regulations 2021 in relation to a review, the organization's conduct during the review and the outcome of the review.
- Public interest considerations.

- **Who enforces them?**

The PDPC is the authority that administers and enforces the PDPA.

Under the section 48I of the PDPA, the PDPC may, if it is satisfied that an organization is not complying with any Data Protection Provision, give the organization such directions as the PDPC thinks fit in the circumstances to ensure compliance with that provision.

The Amendment Act introduced several new provisions which extends PDPC's enforcement powers. For instance, the new section 48L of the PDPA expressly empowers the PDPC to accept statutory undertakings. Under this new section, where the PDPC has reasonable grounds to believe that an organization has not complied, is not complying or is likely not to comply with any of the data protection provisions, the organization may give, and the PDPC may accept, a written voluntary undertaking.

Furthermore, the Amendment Act also introduced a new section 48G which empowers the PDPC to establish or approve one or more dispute resolution schemes for the resolution of complaints by mediation, and to make regulations relating to the operation of such schemes. Section 48G also allows the PDPC, with or without the parties' consent, to refer the matter to mediation under a dispute resolution scheme, if it is of the view that the matter may more appropriately be resolved in this manner.

- **What is their practice (quietly working with companies to fix, publicly coming out with large investigations? Fact specific?)**

In the Guide on Active Enforcement, when a complaint is received by the PDPC, the PDPC will first assess whether it is able to assist in facilitating communication between the individual and the organization. In the occasion that the individual and organization are not able to directly resolve the issue, and both parties are agreeable, the PDPC may refer the matter for mediation by a qualified mediator, or other alternate dispute resolution methods. If the matter is resolved, the PDPC will generally not proceed with further investigations.

In taking enforcement actions, the PDPC's objective is to encourage organizations to comply with the PDPA. Decisions on investigations into breaches of the PDPA by organizations are published and communicated publicly to, among others, to encourage organizations to imbed an accountability culture towards data protection and to deter conduct or practices which may contravene organizational obligations pursuant to PDPA.

After the commencement of the investigation, there are several enforcement actions that can be taken by PDPC:

(A) Suspension or Discontinuation of Investigation

Section 50 of the PDPA states that the PDPC may suspend, discontinue, or refuse to conduct investigations if it thinks fit – including in the following situations:

- The complainant has not complied with a direction issued by the PDPC.
- The parties involved have mutually agreed to settle the matter.
- The PDPC is of the opinion that the matter may be more appropriately investigated by another regulatory authority and refers the matter to that authority.

(B) Undertaking

Under certain circumstances, the PDPC or the organization may initiate an undertaking process. The process includes a written agreement between the organization involved and the PDPC, in which the organization voluntarily commits to remedy the breaches and take steps to prevent recurrence. The organization's request to invoke the undertaking process must be made soon after the incident is known – and the discretion to accept this process lies with the PDPC. The undertaking process is intended to allow organizations with good accountability practices and an effective remediation plan to be provided with a window of opportunity to implement their remediation plans.

(C) Expedited Decision

An expedited decision may be considered by PDPC under certain circumstances, usually where there is an upfront admission to be liable for breaching relevant obligations under the PDPA by the organization. This expedited decision allows for the investigations to end in a shorter time and achieve a similar enforcement outcome of a full investigation.

Note that organizations that are considered for expedited decisions must make a written request to the PDPC when investigations commence. The organization must specify that it is prepared to accept liability for any breach of PDPA obligations. It will provide and admit to all relevant information of the incident as well as identify the areas to which it is admitting liability to.

(D) Full Investigation Process

Usually, the PDPC will encourage the use of alternate dispute resolution or other pathways to resolve any disputes or issues. However, for incidents with high impact, the PDPC will launch a full investigation process. For instance, when the personal data disclosed affects significantly or it affects a significant number of people. Once a breach is determined, the following enforcement actions may be imposed on organizations: warning, directions only, financial penalties only or directions and financial penalties.

- **What guidance is there on how to handle requirements in the ad ecosystem? Have the regulators been educated on how the ecosystem operates? Have compliance regimes been discussed with them? Has their feedback been solicited?**

The Data-Driven Marketing Association of Singapore (DMAS), a non-profit organization established in Singapore, aims to curate the best practices for marketing in Singapore and facilitate the sharing of information and ideas

on direct marketing. With regards to data protection, in line with the PDPA's DNC provisions, the DMAS has issued guidelines for its members, including the DMAS Guidelines for Using Commercial Electronic Messages coupled with several Compliance Checklists. These provides clear guidance on how to handle specific requirements in the advertisement ecosystem.

DMAS has been active in taking part in past public consultations held by PDPC – namely in the Public Consultation on Review of the PDPA 2012 – Proposed Data Portability and Data Innovation Provisions and the Public Consultation on Approaches to Managing Personal Data in the Digital Economy.

Such feedback has culminated in certain amendments in the Amendment Bill, for instance, the introduction of a Data Portability Obligation under the new Part VIB of the PDPA. Under this obligation, subject to certain conditions and exceptions, organizations are required to, at the request of an individual, transmit personal data that is in the organization's possession or under its control to another organization in accordance with any prescribed requirements.

11.4. Remedies

As mentioned in section 11.1, when the PDPC finds that an organization is in breach of any of the Data Protection Provisions in the PDPA, it may issue orders or directions to the organizations to ensure compliance. These directions, include to:

- Stop collecting, using, or disclosing personal data in contravention of the PDPA.
- Destroy personal data collected in contravention of the PDPA.
- Provide access to or correct personal data.
- Pay a financial penalty of up to SGD 1 million.

In section 30(3) of the PDPA, a District Court has the jurisdiction to enforce any direction set out by the PDPC and may, for the purpose of enforcing this direction, make any order:

- To secure compliance with the direction.
- To require any person to do anything to remedy, mitigate or eliminate any effects arising from:
    - Anything done which ought not, under the direction, to have been done.
    - Anything not done which ought, under the direction to have been done, which would not have occurred had the direction been complied with.

11.5. Private Right of Action

In section 32(1) of the PDPA, any person who suffers loss or damage directly as a result of a contravention of any provision in Part IV, V or VI of the PDPA by an organization shall have a private right of action for relief in civil pro-

ceedings in a court. Section 32(3) of the PDPA further states that the court may grant to the plaintiff in a private action any of the following: reliefs by way of injunction or declaration, damages or other reliefs as the court deems fit.

On February 19, 2019, the State Court dismissed a claim brought against the Singapore Swimming Club for defamation and breach of the PDPA. Although written grounds of judgment are not available, this case is significant as it appears to be the first time where the Singapore courts were asked to consider whether there was a breach of the PDPA, and the PDPC did not make any decision in respect of any purported contravention of the PDPA.

The recent case of *IP Investment Management Pte Ltd and Ors v. Alex Bellingham* [2019] SGDC 207 is the only reported decision to-date that considered a private action brought pursuant to section 32 of the PDPA. The main issue before the court was whether the right of private action under section 32 extended to corporate bodies. The court held that the right of private action only applies to individuals, and the right under section 32 does not extend to organizations. Although the plaintiffs argued that section 2(1) of the Interpretation Act extends 'person' to include 'any company or association of body of persons, corporate or unincorporate', the court rejected this submission.

At [85] to [86] of the decision, the court stated that the extension of section 32 to encompass organizations would allow such organizations to use the provision as a 'substitute for contractual or other arrangements' which might be expected of organizations to put in place to protection personal data in their possession, as seen in section 24 of the PDPA. The purposive interpretation taken by the court clarified that "Parliament could [not] have intended that section 32 of the PDPA should serve as a kind of crutch for organizations which have not complied with their obligations under the PDPA, for this would severely undermine the stated aim of the PDPA as legislation to 'safeguard individuals' personal data against misuse by regulating the proper management of personal data'."

11.6. Digital Advertising Liability Issues

As mentioned in section 10.4, the enforcement decisions on organizations involved in digital advertising and marketing published by PDPC often involve the following contraventions:

- Breach of Protection Obligation under section 24 of the PDPA
- Breach of Retention Limitation Obligation under section 25 of the PDPA
- Breach of Accountability Obligation under section 11(3) and 12 of the PDPA
- Breach of Consent Obligation under section 13 of the PDPA
- Breach of Purpose Limitation Obligation under section 18 of the PDPA

12. NOTIFICATION | CERTIFICATION | REGISTRATION

12.1. Overview

Section 20 of the PDPA provides that an organization must notify an individual of the purpose(s) for which it intends to collect, use, or disclose his personal data, on or before such collection, use or disclosure (i.e., the Notification Obligation).

According to the PDPC's Guide to Notification, a notification informs individuals of the purposes for which an organization is collecting, using, or disclosing their personal data. A notification may also provide other information such as the business contact information of the data protection officer or a representative of the organization who is responsible for addressing queries regarding the organization's personal data protection policies, processes for withdrawal of consent and requests for access or correction of individuals' personal data.

With respect to certification and registration, there is no requirement for the organization to certify or register with the PDPC in relation to the collection or processing of personal data. Nonetheless, there are voluntary initiatives in relation to certification. For instance, on January 9, 2019, the IMDA launched the Data Protection Trustmark (DPTM) certification scheme for the CBPR and PRP systems. The certification establishes robust data governance standard to help businesses increase their competitive advantage and build trust with their customers.

12.2. Requirements and Brief Description

In relation to the Notification Obligation, subject to certain exceptions, Section 20(1) of the PDPA requires an organization to inform the individual of: (a) the purposes for the collection, use, and disclosure of his personal data, on or before collecting the personal data; or (b) any purpose for use or disclosure of personal data which has not been informed under sub-paragraph (a), before such use or disclosure of personal data for that purpose.

12.3. Application to Digital Advertising

As far as we are aware, there is no legislation that applies specifically to ad tech companies regarding notification, certification, and registration.

Nonetheless, we note that the PDPC has issued a Guide to Notification, which provides guidance on the type of notifications that organizations may wish to consider, e.g. most effective presentation format, layout, location of the notification, and clarity of language used.

13. DATA PROTECTION OFFICER

13.1. Overview

It is mandatory for organizations to appoint a DPO, or a panel of individuals, to be responsible for ensuring that the organization complies with the PDPA. This is part of the Accountability Obligation.

The obligation to appoint a DPO is provided for by section 11(3) of the PDPA. On the whole, section 11 requires organizations to designate the appropriate individuals, who may in turn delegate certain responsibilities to other officers, so that they collectively co-operate to ensure that the organization complies with the PDPA.

As stated in the PDPC's Key Concept Guidelines, an organization's DPO plays an essential role in how the organization meets its obligations under the PDPA. The responsibilities of the DPO often include working with senior management and the organization's business units to develop and implement appropriate data protection policies and practices for the organization. In addition, the DPO would undertake a wide range of activities, which may include producing (or guiding the production of) a personal data inventory, conducting data protection impact assessments, monitoring, and reporting data protection risks, providing internal training on data protection compliance, engaging with stakeholders on data protection matters and generally acting as the primary internal expert on data protection. Depending on the organization's needs, the DPO may also work with (or have additional responsibilities relating to) the organization's data governance and cybersecurity functions. The DPO can also play a role in supporting an organization's innovation.

The rationale of appointing a DPO is to embed personal data protection into corporate governance by involving senior management, which is crucial to ensure a commitment to accountability. It is the responsibility of senior management to appoint a DPO, preferably from senior management, who can effectively direct and oversee data protection initiatives. The DPO will be supported by representatives from various organizational functions.

13.2. DPO – Compulsory Appointment (Yes/No)

Under the PDPA, organizations are required to develop and implement policies and practices that are necessary to meet its obligations under the PDPA. In particular, organizations are required to designate at least one individual, known as the DPO, to oversee the data protection responsibilities within the organization and ensure compliance with the PDPA.

DPOs may register with the PDPC on a voluntary basis to keep abreast of developments in the PDPA. It is not required under the law to inform the PDPC of the DPO's details but the PDPC strongly encourages all organizations to do so.

13.3. Requirements

All organizations, including sole proprietorships, are required to designate at least one person, a Data Protection

Officer (DPO), to be responsible for ensuring that the organization complies with the PDPA. An organization may appoint one or more individuals to be its DPO (section 11(3) of the PDPA). Once appointed, the DPO may in turn delegate certain responsibilities to other officers (section 11(4) of the PDPA).

The DPO may be a person whose scope of work solely relates to data protection or a person in the organization who takes on this role as one of his multiple responsibilities. It should be noted that legal responsibility for complying with the PDPA remains with the organization and is not transferred to the designated individual(s) (section 11(6) of the PDPA).

Organizations are free to assess and decide, according to their needs, whether the DPO function should be a dedicated responsibility or an additional function within an existing role in the organization. The DPO (or someone working with him) may also be the primary contact point for the organization's data protection matters. Section 11(5) of the PDPA requires an organization to make available the business contact information of at least one individual designated by the organization under section 11(3) while section 20(1)(c) and 20(4)(b) require an organization to make available the business contact information of a person who is able to answer questions on behalf of the organization relating to the collection, use or disclosure of personal data. The PDPC explains that these individuals and persons may be the same individual or the organization may have different persons undertaking such roles. The business contact information may be a general telephone or email address of the organization. While there is no requirement that such a person must be located in Singapore, to facilitate prompt responses to queries or complaints, the PDPC recommends, as good practice, that the business contact information of this person should be readily accessible from Singapore, operational during Singapore business hours and if telephone numbers are used, be Singapore telephone numbers.

The PDPC recommends that DPOs should be: (a) sufficiently skilled and knowledgeable; and (b) amply empowered, to discharge their duties as a DPO, although they need not be an employee of the organization. Organizations should ensure that individuals appointed as a DPO are trained and certified. The individual(s) should ideally be a member of the organization's senior management team or have a direct reporting line to the senior management to ensure the effective development and implementation of the organization's data protection policies and practices.

Organizations that have not appointed a DPO are in breach of the Accountability Obligation and may be subject to a financial penalty. The PDPC may also issue directions to that organization to appoint a DPO.

13.4. Application to Digital Advertising

At the time of writing, there is no legislation that applies specifically to ad tech companies regarding such notification, certification, and registration. Nonetheless, the provisions within the PDPA should generally apply.

To enhance the capabilities of Data Protection Officers (DPOs) in organizations, a two-day preparatory course - "Practitioner Certificate in Personal Data Protection (Singapore)" - has been developed to equip them

with practical data governance and data protection knowledge and skills and learn to utilize risk-based tools to establish a robust data protection infrastructure for their organization.

The PDPC has also developed the DPO Competency Framework and Training Roadmap to guide data protection professionals in enhancing their competencies so as to perform their job functions effectively in an organization. The framework outlines the core competencies and proficiency levels for a DPO and provides guidance on a viable career pathway from entry-level data protection executives to regional data protection senior management roles.

14. SELF-REGULATION

14.1. Overview

- **Are there any industry-self regulatory schemes in place in the jurisdiction?**

At the time of writing, all advertisements published in Singapore must adhere to the Singapore Code of Advertising Practice ("the Code"), administered by ASAS. The Code promotes high standard of ethics in advertising. The guidelines were developed in consultation with social media agencies, public agencies, multinational companies, and members of the public.

For the digital advertising industry, the Advertising Standards Authority of Singapore (ASAS), an advisory council to the Consumers Association of Singapore (CASE) issued Guidelines on Interactive Marketing Communication and Social Media ("the Guidelines") on August 29, 2016. These Guidelines, which are to be read with the Code, set the standards on advertising and marketing communication that appear on interactive and social media.

Although the Code is not legally binding, ASAS may request offending marketers to amend or withdraw any advertisement contrary to the Code. ASAS may also impose sanctions, such as withholding of advertising space and withdrawal of trading privileges from offending marketers. In extreme cases of non-compliance, ASAS may impose the additional sanction of adverse publicity.

- **Are there any signal-based programs used in the territory to assist with digital advertising compliance?**

We are not aware of any Singapore legislation that governs with such programmatic advertising platforms.

14.2. Application to Digital Advertising

Please see our comment above.

15. PENDING PRIVACY BILLS

15.1. Overview

As stated above, the Personal Data Protection (Amendment) Act was passed on November 2, 2020, and most of its

provisions came into force on February 1, 2021. There are no other pending privacy bills at present.

The PDPA is a consent-based regime, and in order to the extent that there is collection, use, or disclosure of personal data involved in the lawful processing of a digital advertising transaction (i.e., serving a behavioral ad), consent would need to be obtained from the relevant individuals.

Overview of applicable Opt-out consent laws:

- Sections 13-17 of the PDPA:
    - Section 13 of the PDPA prohibits organizations from collecting, using, or disclosing an individual's personal data unless the individual gives, or is deemed to have given, his consent for the collection, use or disclosure of his personal data.
    - Section 14(1) of the PDPA states how an individual gives consent under the PDPA. In particular, an individual has not given consent unless the individual has been notified of the purposes for which his personal data will be collected, used, or disclosed and the individual has provided his consent for those purposes. If an organization fails to inform the individual of the purposes for which his personal data will be collected, used, and disclosed, any consent given by the individual would not amount to consent under section 14(1).
    - Section 14(2) of the PDPA sets out additional obligations that organizations must comply with when obtaining consent. This subsection provides that an organization providing a product or service to an individual must not, as a condition of providing the product or service, require the individual to consent to the collection, use, or disclosure of his personal data beyond what is reasonable to provide the product or service.
    - Section 15 of the PDPA addresses two situations in which an individual may be deemed to consent even if he has not actually given consent.
    - Section 16 of the PDPA provides that individuals may at any time withdraw any consent given or deemed to have been given under the PDPA in respect of the collection, use or disclosure of their personal data for any purpose by an organization.

As noted by the PDPC, there are various means of obtaining an individual's consent to the collection, use and disclosure of his personal data for a specified purpose. For example, organizations may adopt the opt out avenue to obtain consent by deeming that an individual has given his consent through inaction on his part. In general, the PDPC notes that failure to opt out may be due to other reasons than the individual's desire to give consent. The PDPC's view is that a failure to opt out will not be regarded as consent in all situations. Rather, whether or not a

failure to opt out can be regarded as consent will depend on the actual circumstances and facts of the case. The opt out method of obtaining consent also has many variants, and depending on its implementation, could be more or less likely to constitute consent.

The PDPC recommends that organizations obtain consent from an individual through a positive action of the individual to consent to the collection, use, and disclosure of his personal data for the stated purposes. If an organization intends to adopt the opt out approach in seeking consent, the organization should consider the risks that it may not have satisfied the Notification Obligation and Consent Obligation.

Amendment Act and its Effects

Deemed Consent by Notification

Clause 7 of the Amendment Act introduces the new section 15A, which expands the consent regime by introducing deemed consent by notification. Under this provision, organizations may notify their customers of the new purpose and provide a reasonable period for them to opt out. Before doing so, organizations must conduct a risk assessment and conclude that the collection, use, or disclosure of personal data in this manner will not likely have an adverse effect on the individual.

This is useful for organizations that wish to use the personal data of existing customers for new purposes. For example, a financial institution may want to use voice data as an alternative means to authenticate and verify its customers. With these amendments, the financial institution can notify its customers of the intended use of their voice data, provide a reasonable opt-out period, and a contact number for customers' queries. It should be noted that the individual may still withdraw his deemed consent any time after the opt-out period has lapsed.

Deemed Consent for Contractual Performance:

Multiple layers of contracting and outsourcing are common in modern commercial arrangements. Section 6 expands deemed consent to cater for scenarios where personal data is passed from an organization to successive layers of contractors for the organization to fulfil the contract with its customer. Crucially, organizations relying on deemed consent for contractual necessity can only collect, use and disclose personal data where it is reasonably necessary to fulfil the contract with the individual.

Legitimate Interests Exception

Section 31 introduces the First Schedule to the PDPA, which sets out a new exception to consent for these legitimate uses of personal data. To rely on this exception, organizations must conduct an assessment to eliminate or reduce risks associated with the collection, use or disclosure of personal data, and must be satisfied that the overall benefit of doing so outweighs any residual adverse effect on an individual. To ensure transparency, organizations must disclose when they rely on this exception. One of many potential use cases is anomaly detection in payment systems to prevent fraud or money-laundering.

Business Improvement Exception

The new First and Second Schedules introduced in sections 31 and 32 make clear that organizations may use personal data for business improvement purposes including: operational efficiency and service improvements; developing or enhancing products or services; and knowing the organizations' customers. As a safeguard, this exception can be relied upon only for purposes that a reasonable person may consider appropriate in the circumstances and where the purpose cannot be achieved without the use of the personal data.

Businesses have asked for this exception to also apply to entities within a group as they may consolidate corporate or administrative functions or concentrate research and development expertise in a single unit that supports the entire group. Recognizing this commercial reality, Part 5 of the new First Schedule in clause 31 allows related corporations to collect and disclose personal data among themselves for the same purposes. The Bill provides for additional safeguards for intra-group sharing by requiring related corporations to be bound by a contract, agreement, or binding corporate rules to implement and maintain appropriate safeguards for the personal data.

Research and Development Exception

The current research exception has also been revised in section 32 to support commercial research and development that is not immediately directed at productization, in other words, going upstream. This could apply to research institutes carrying out scientific research and development, educational institutes embarking on social sciences research, and organizations conducting market research to identify and understand potential customer segments.

iab.

South Korea

Cross-Jurisdiction Privacy Project

1. THE LAW

1.1. Overview & Key Acts, Regulations, and Directives

The main laws and regulations related to data protection are the Personal Information Protection Act ("PIPA") and its implementing regulations, which regulate the collection, usage, disclosure, and other processing (collectively, processing or process) of personal information by governmental and private entities. In addition to the PIPA, there are sector-specific laws which also regulate data protection. The processing of personal information by information and communications service providers ("ICSPs"), including telecommunication service providers, was regulated by the Act on Promotion of Information Communication Network Usage and Information Protection ("Network Act"). Following recent amendments to data protection laws and regulations in South Korea that went into effect on August 5, 2020, most of the provisions related to the processing of personal information, including those specially applying to ICSPs in the Network Act, have been transferred to the PIPA.

The data protection laws in South Korea provide very prescriptive specific requirements throughout the lifecycle of the handling of personal information. The data protection laws consist of a general law and several special laws pertaining to specific industry sectors. An asterisk is included for those likely to apply to digital advertising transactions:

- PIPA (as amended in 2020)*

The processing of personal information by ICSPs and recipients of such information, which was previously governed by the Network Act (English version without 2020 Amendments available here; up-to-date version only available in Korean here), is now governed by PIPA following the deletion of the relevant provisions from Network Act and their transfer to PIPA on August 5, 2020. These provisions are now included in the PIPA as a new chapter ("the Special Provisions for ICSPs").

1.2. Guidelines

Data protection authorities, including the Personal Information Protection Commission ("PIPC"), the central administrative agency established by PIPA, have also issued various guidelines related to the protection of personal information:

- A guide to the Interpretation of Data Protection Laws and Regulations, issued by (only available to download in Korean, here).
- Guidelines for minimizing the collection of personal information issued by PIPC (including guidelines for preparing consent forms for the collection and provision to third parties of personal information) (only available to download in Korean, here).
- Guidelines for the Pseudonymization of Personal Information, issued by PIPC (only available to download in Korean here).

- Guidelines on online personal information processing issued by PIPC (only available to download in Korean here).
- Korea Communications Commission ("KCC") has issued Personal Information guidelines on online personalized advertising privacy (only available in Korean here) ("theKCC Online Processing Guidelines"); and
- Handbook on the Pseudonymization and Anonymization of Personal Information in the Financial Sector (only available to download in Korean here).

PIPC has issued the following guidance on cookies and similar technologies:

- Research paper on the scope of personal information protection in the world, in comparison with South Korea (only available to download in Korean here) ("the Research Paper").
- Guidelines for minimizing the collection of personal information (including guidelines for preparing consent forms for the collection and provision to third parties of personal information) (only available to download in Korean, here).
- Guidelines on online personal information processing issued by the PIPC (only available to download in Korean here); and
- Guidelines on the Interpretation of Data Protection Laws and Regulations (only available to download in Korean here) ("PIPC Guidelines").

Moreover, KCC has issued the following guidance:

- Personal Information guidelines on online personalized advertising privacy (only available in Korean here) ("'he KCC Online Processing Guidelines").

Although such guidelines lack binding legal effect, they may, nevertheless, serve as useful reference materials on how laws and regulations are likely to be interpreted in practice.

1.3. Case Law

As a civil law jurisdiction, South Korea's principal source of legal authority is legislation (as opposed to case law in common law jurisdictions), and in particular, codifications in the Constitution of the Republic of Korea and statutes enacted by the Government of the Republic of Korea or the National Assembly. However, several recent court decisions are important reference points for how data protection laws and regulations may be interpreted in practice.

In the Supreme Court Decision 2016Do13263, decided on April 7, 2017, the Supreme Court of Korea invalidated the consent obtained from data subjects because the defendant collected personal information under circumstances that made it difficult for data subjects to clearly understand what they had consented to, even though the consent they had provided satisfied formalities prescribed by law (i.e. the notice was provided in font size of 1mm).

Furthermore, in the Seoul High Court ("the High Court") Decision 2017Na2074963/2017Na2074970 (Consolidated), decided on May 3, 2019, the High Court ruled that the Korea Pharmaceutical Information Center's provision of sensitive personal information--(i.e. prescription data of patients to third parties)--without consent constituted a violation of PIPA. At the same time, the High Court noted that if the personal information has undergone appropriate de-identification measures which make it impossible to identify specific individuals, such as encryption, then the provision of such de-identified data to third parties without the consent of data subjects should not be considered a violation of PIPA.

1.4. Application to Digital Advertising

With respect to the processing of personal information related to digital advertising, PIPA and the Network Act appear to be the most relevant laws; the KCC Online Processing Guidelines appear to be the most relevant guidelines. Although there exists no notable case law to date on online/targeted advertising, the Seoul Central District Prosecutors' Office previously determined in November 2011 that a mobile dynamic IP address should not be viewed as personal information because multiple mobile device users may connect to the same IP address within the same access point range and a mobile dynamic IP address may constantly change across different points in time.

There is no signal-based program in South Korea which is related to compliance for digital advertising. The KCC Online Processing Guidelines provide that the following data protection principles should be followed when conducting online behavioral advertising:

1. Transparent collection/use of behavioral data: (i) advertising businesses and media publishers must implement measures to provide conspicuous notice to users of the fact that their behavioral data may be collected/used online; (ii) advertising businesses must collect only the minimum amount of behavioral data necessary to conduct online behavioral advertising; (iii) advertising businesses must obtain the consent of users before combining their behavioral data with individual identifiers for use in online behavioral advertising; (iv) advertising businesses must not knowingly (1) collect behavioral data from a user under the age of 14 or from an online service primarily used by such underage users for the purpose of conducting online behavioral advertising or (2) conduct online behavioral advertising towards such underage users; and (v) advertising businesses and media publishers which provide behavioral data they have collected to other third party advertising businesses must conspicuously disclose, on the landing page of their internet homepage or the screen where their advertisement is placed, information on (1) the recipients of behavioral data, (2) items of behavioral data provided, and (3) the recipients' purposes of use of the behavioral data.

2. Ensure the informational self-determination right of users: advertising businesses must make available to users various measures to control/use their data, including at least one of the following measures, so that users may easily decide whether to have their behavioral data provided to third parties or receive online behavioral advertisements.

- Enable users to exercise control directly through the advertisement screen.
- Enable users to exercise control through their mobile device.
- Enable users to exercise control via an association or other organization.

3. Ensure the security of behavioral data: advertising businesses must (i) implement technical and organizational security measures to safeguard behavioral data which is processed for online behavioral advertising; and (ii) only store behavioral data for the minimum duration necessary to achieve relevant purposes unless the further storage thereof is otherwise required by law.

4. Enhance awareness and bolster redress measures: advertising businesses must (i) actively notify users and advertisers on matters related to online behavioral advertising and the protection of behavioral data; and (ii) implement redress measures to respond to inquiries from users related to online behavioral advertising and requests from users related to data privacy infringement.

2. SCOPE OF APPLICATION

2.1. Who Do the Laws/Regs Apply to and What Types of Processing Activities are Covered/Exempted?

PIPA applies to the processing of personal information relating to living natural persons only. It is understood that PIPA applies to all persons (whether a public agency, juridical person, organization, or individual) in South Korea, but PIPA does not specify its territorial scope. Personal Information file means a collection of personal information in which personal information is systematically organized pursuant to certain rules for easy search or use of such personal information.

On January 9, 2020, the National Assembly passed several amendments to PIPA (only available to download in Korean here) ("the 2020 Amendments"), which entered into effect on August 5, 2020. In particular, the 2020 Amendments include, among other things, new definitions for pseudonymization and anonymization processing, as well as associated requirements, restrictions, and penalties, and measures for centralizing personal information protection services within PIPC.

2.2. Jurisdictional Reach

It is understood that PIPA applies to all persons (whether a public agency, juridical person, organization, or individual) in Korea, but PIPA does not specify its territorial scope. Meanwhile, the Network Act expressly provides that its provisions may apply to acts which take place outside South Korea if such acts affect markets or users in Korea. This reflects the KCC's position regarding the extraterritorial applicability of the Network Act as well as other Korean data protection laws and may provide insight into how PIPC may interpret the extraterritorial applicability of PIPA going forward.

2.3. Application to Digital Advertising

Scenario 1 (The baseline): A user residing in Korea (determined by IP address or geo identifier) goes onto a Korean domain and is served an ad by a Korean advertiser. The advertiser uses the user data to build a user profile.

According to PIPA, a data controller means a person who processes personal information to perform work. Thus, anyone who collects and uses the personal information of a user in Korea for the purpose of creating a profile to electronically transmit advertising information to such user may be deemed a data controller under PIPA and become subject to its provisions.

Scenario 2 (User outside Korea): A logged-on/signed-in user, known by the publisher to be a Korean resident, goes onto a Korean domain but the user's IP address or geo identifier indicates the user is outside Korea. A Korean advertiser serves an ad and uses the user data to build a user profile.

It is not certain if PIPA will apply in Scenario 2 as neither a literal reading of its provisions nor regulatory guidance clearly addresses this particular issue. That said, PIPA may apply in cases where the person who is processing the personal information of a user for business purposes is located in Korea even if such user is not.

- **Q1: Does the answer change if this is a signed-out user with no way of knowing where they are domiciled?**

Likewise, it is not certain if PIPA will apply in this case as neither a literal reading of its provisions nor regulatory guidance clearly addresses this particular issue. That said, the likelihood of PIPA applying may increase if both the advertiser and publisher are located in Korea.

Scenario 3 (Publisher domain outside Korea): A user residing in Korea (determined by IP address or geo identifier) goes onto a domain outside of Korea. A Korean advertiser serves an ad and uses the user data to build a user profile.

It is not certain if PIPA will apply in Scenario 3 as neither a literal reading of its provisions nor regulatory guidance clearly addresses this particular issue. That said, the likelihood of PIPA applying in this case should be lower vis-à-vis the above scenario where both the Advertiser and Publisher are located in Korea.

- **Q1: Does the answer change if the site hosts content aimed at Korean residents (e.g., a news aggregator with a section on Korean current affairs)?**

Likewise, it is not certain if PIPA will apply in this case as neither a literal reading of its provisions nor regulatory guidance clearly addresses this particular issue. That said, the likelihood of PIPA applying may increase if the site is targeting users in Korea.

- **Q2: Does the answer change if the advertiser is based outside of Korea?**

Likewise, it is not certain if PIPA will apply in this case as neither a literal reading of its provisions nor regulatory guidance clearly addresses this particular issue. That said, the likelihood of the PIPA applying should be much lower if both the advertiser and publisher are not located in Korea.

Scenario 4 (Advertiser outside Korea): A user residing in Korea (determined by IP address or geo identifier) goes onto a Korean domain and is served an ad by an advertiser based outside Korea. The advertiser uses the user data to build a user profile.

Likewise, it is not certain if PIPA will apply in Scenario 4 as neither a literal reading of its provisions nor regulatory guidance clearly addresses this particular issue. That said, the likelihood of the PIPA applying appears to be lower vis-à-vis the above scenario where both the advertiser and publisher are located in Korea.

- **Q: Does the answer change if the advertiser has an affiliate/group company based in Korea?**

Likewise, it is not certain if PIPA will apply in this case as neither a literal reading of its provisions nor regulatory guidance clearly addresses this particular issue. That said, it appears that, from a practical standpoint, the likelihood of the PIPA applying will be higher if the advertiser has an affiliate/group company based in Korea.

3. DEFINITIONS

3.1. Collect

The law does not provide a specific definition.

When a publisher allows an ad tech company's pixel on its page, who is deemed to "collect" personal information and incur legal obligations (e.g., controller/co-controller obligations under GDPR or "business" obligations under CCPA)--the publisher, the ad tech company, or both?

Based on relevant laws/regulations and the established position of data protection authorities, it is difficult to determine who may be deemed to be "collecting" personal information in a general sense as such determination will need to be made on a case-by-case basis after considering the circumstances of a particular case. However, under the KCC Online Processing Guidelines, "Advertisers" (e.g., ad tech companies) refer to entities that transmit

ads based on online behavioral data that they collect via online mediums including their own websites and apps or those of another company, while "media publishers" refer to those who provide the mediums and channels through which online behavioral data is collected or the online targeted ads are published. Thus, the KCC Online Processing Guidelines appear to assume that ad tech companies will be collecting behavioral data. Meanwhile, ad tech companies, which connect Advertisers and Publishers in the digital advertising marketplace, can be further delineated into DSP (Demand side Platforms), ADX (AD Exchanges), and SSP (Supply Side Platforms) etc. That said, the specific categories and subcategories of ad tech companies are becoming ever more diverse and, because the purposes for using data may be unique for each ad tech company, it is becoming increasingly difficult to uniformly define them based on whether they have collected data themselves, have received data from a third party, or have been entrusted with the processing of data (please see Section 6.1 for more information on the distinction between a third party provision/entrustment) by a third party as ad tech companies may feature a mixture of each of the foregoing aspects. In addition, apart from the KCC Online Processing Guidelines, regulatory authorities have failed to issue any further guidance regarding the processing of data in the digital marketplace.

3.2 Data Processing (i.e., collecting, capturing, retaining, recording, organizing, structuring, storing, altering, retrieving, consulting, using, disclosing, transmitting, disseminating, making available, aligning, combining, restricting, erasing, destroying, or otherwise processing)

"Processing" of personal information is defined to mean the "collection, generation, recording, storage, retention, processing, editing, search, outputting, rectification, restoration, use, provision, disclosure or destruction of personal information or any other action similar to any of the foregoing."

3.3. Personal Information

PIPA has a broad definition of personal information, which is any data relating to a living natural person that (i) identifies a particular individual by his or her full name, resident registration number, image or the like, (ii) even if it by itself does not identify a particular individual, may be easily combined with other information to identify a particular individual (in such cases, whether or not the information may be "easily combined" shall be determined by reasonably considering the time, cost, and technology used to identify the individual such as the likelihood that the other information can be procured), or (iii) is information under items (i) or (ii) above which is pseudonymized and thereby becomes incapable of identifying a particular individual without the use or combination of additional information for restoration to its original state. PIPA does not contain any provisions which clearly address the meaning of "identifiability." However, PIPC Guidelines provide that "identifiability" should mean the capability, of the person who is processing the data in question (i.e. data controller and/or data processor) and after reasonably considering the methods of processing data which may be used by such person, to identify a specific individual.

Meanwhile, there has been recent discourse, mainly in the academic sector, about the need to regard personal information as consisting of (i) particular data attributable to an individual person (singling out), (ii) particular data linked

to particular person (linkability), and (iii) particular persons inferable from particular data (inferrability); thereby treating "single out" and "identifiability" as different concepts. Such distinction has yet to be reflected in PIPA, but the Credit Information Act does make such distinction, albeit indirectly, as it specifically differentiates between "cases where certain data subjects are distinguishable from other data subjects" and "cases where a data subject is identifiable" when defining pseudonymized processing.

Type of Information Collected	Does this Category Independently Constitute Personal Information? (Yes/No)	Qualifying Notes (if any)
IP Address	Partially no.	In general, static IP addresses used by individuals are considered to be personal information whereas static IP addresses used by companies and dynamic addresses are not considered to be personal information. However, a mobile dynamic IP address is not viewed as personal information.
Mobile Advertising IDs (IDFA, AAID)	Partially No.	In a case where the controller has both the mobile AD ID and the matching user information (e.g., name, contact information etc.), the mobile AD ID would be viewed as personal information. Otherwise, the mobile AD ID by itself would not be regarded as personal information unless the controller has other information (e.g., linked/ matched behavioral information) which could be combined therewith to identify a specific individual.
Consumer identifiers such as: • User device ID • Publisher persistent ID/Cross-publisher cookie ID • Household ID	• User device ID: No. • Publisher persistent ID/ Cross-publisher cookie ID: No. Household ID: Yes (e.g., addresses and home phone numbers, etc.)	

Hashed identifiers such as: • Hashed email • Hashed IP address	• Hashed email: Yes. • Hashed IP address: Partially No.	In general, pseudonymized information is considered to be personal information. However, if data controllers are unable to identify specific individuals from the hashed emails and hashed IP addresses, then it would be difficult to view the hashed emails and hashed IP addresses as constituting personal information from the perspective of such data controllers.
User Agent such as: • Character string identifying the application • Operating system • Browser information, vendor, and/or version of the requesting user agent	No.	
Device Information such as: • Type, version, system settings, etc.	No.	
Website Information such as: • Name • URL, etc.	No.	
Advertisement Information such as: • Placement • Title • Creative ID, etc.	No.	
Timestamps	No.	

Metrics such as: • Counts • Amounts of time	No.	
Event Data such as: (e.g., full URL including query string, referral URL)	No.	
Precise geolocation (latitude, longitude)	Yes.	Precise location which can be used to identify specific individuals or households is likely to be considered personal information
General geolocation (city, state, country)	No.	

*Please note that the middle column of the above table is asking "Does this Category Independently Constitute Personal Information?" and so our responses for each "item of information collected" in the leftmost column have been provided on this basis.

- **Are pseudonymous digital identifiers by themselves personal information (e.g., IDFA, cookie IDs, proprietary IDs, IP addresses, etc.)? Please provide context to the above chart.**

There is no law or regulation in Korea that governs behavioral advertising or behavioral data such as persistent digital identifiers in particular, nor clear official rulings or court judgements on the above question. However, the collection and processing of cookies and behavioral data, which is necessary for conducting behavioral advertising, is considered as personal information and subject to notice and consent requirements for the processing of if such information can be used to identify specific individuals. As you may find in Section 1.5 KCC Online Processing Guideline 1. (iii) which says "(iii) advertising businesses must obtain the consent of users before combining their behavioral data with individual identifiers for use in online behavioral advertising", the regulator appears to be in a position that persistent digital identifiers by themselves alone may not be personal information. However, it does not exclude the possibility of them being regarded as personal information in case a controller may, or have a capacity to, link or combine with other information which allows the identification of specific individuals, even though it did not actually combine persistent digital identifiers with such other information. Based on our experiments, the regulator appears to believe that such possibility of combinability would amount to such information to be personal information. Combinability should be determined based on reasonableness of time, technology, or cost for such combination.

For your reference, the Research Paper acknowledges that information contained or found through IP addresses, log records, or cookies, may be combined with other information to identify an individual and thus constitute personal information (pages 8, 14-16, 34, 47, 87, 124, 167, 171, 189-193, 212-217, 298, and 308 of "Research Paper" - only available in Korean).

Considering this research paper and KCC Guideline, we believe that advertising identifiers alone would not be viewed as personal data so long as they are not, or might not be, combined with other data or they cannot identify specific individuals even after combination with other data.

- **If the answer to the above question is, "no," if a Company possesses a persistent digital identifier in Database 1 and has that same identifier in Database 2 with directly identifying information, does that render the pseudonymous information in Database 1 as personal information?**

Please see above. Probably yes, it would be personal information.

- **Is a Company's possession of a pseudonymous identifier plus other non-directly identifying data (e.g., age, gender, precise or imprecise geolocation, user agent string, timestamps) considered "personal information"?**

Please see above. To answer this kind of question, we would need information of the various circumstances surrounding the processing of data and the answer might vary case by case, i.e., it may or may not.

- **Is a Company's possession of a pseudonymous identifier "personal information" if it can hire a service provider or otherwise engage in a transaction with a third party where the identifier could be matched to the person, but the Company chooses not to hire such service provider or undertake such transaction. Is the mere fact that this service is potentially available to match to the person sufficient to render that pseudonymous identifier as "personal information"?**

May not provide a simple answer. But we do not think it could make such identifier be recognized as personal information simply based on the fact that the Company have a possibility of hiring such a service provider or undertake such transaction.

- **What level of geolocation is personal data (precise vs. approximate)? Does it need to be associated with an identifier to be considered PI?**

PIPA governs the processing of the personal information of data subjects located in Korea. There is no clear guidance on the level of geolocation for it to constitute personal information. However, regulatory guidance related to the Location Information Act provides that data such as the details of relay stations appearing in mobile phone call records, GPS coordinates of mobile devices collected to determine the location of individuals (when combined with the personal details of device users), and RFID tags collected from the body parts of individuals may be deemed personal location information. The geolocation-related data in question does not need to be associated

with an identifier to be considered personal information as data comprised of only attribute values (which mean any values relating to an individual which are not uniquely assigned to such individual or an object related to such individual) may still be deemed personal information if such data can be easily combined with other information to identify a specific individual.

The Act on the Protection, Use, Etc. of Location Information ("Location Information Act") defines "personal location information" as location information which, if not by itself, can be easily combined with other information to identify the location of a specific individual. For example, geolocation coordinates (even if unable to identify the location of a specific individual by themselves) may be deemed personal location information if easily combinable with other information such as IMEI, IDFA or the name of the device holder to identify the location of such individual. Under the Location Information Act, personal location information may not be, in principle, collected, used, or provided to a third party without the consent of the data subject.

- **Is a household identifier personal data? (Consider: If a company has a residential IP address (household level ID) and multiple unique device IDs (e.g., MAIDs for every mobile device in the house) associated with that IP address, would that affect whether the household identifier is considered personal information?)**

Household identifiers such as addresses and home phone numbers will be considered personal information as they can be used to identify specific individuals. If, from the perspective of data controllers, household identifiers such as residential IP addresses can be easily combined with other unique device IDs to identify specific individuals, then such household identifiers are likely to be deemed personal information.

- **Is a hashed identifier personal data? (Consider: there are commercially available services that will take batches of emails encrypted using standard hashes and return (often a high percentage) of clear emails from them. Does that affect whether they are considered personal information, if all a company must do is pay for the commercial service?)**

Likely yes. See pseudonymized information below. In addition, encryption measures are related to mandatory safeguards which must be implemented when storing/transmitting personal information but do not affect whether particular data may be considered as personal information or not.

- **Is probabilistic information considered personal information?**

Probabilistic information will be considered personal information to the extent such data can be used on its own or be easily combined with other information to identify specific individuals. Regarding combinability with other data, the amended PIPA provides that factors such as the time, cost, and technology required for combination should be reasonably considered when assessing the obtainability of other data. Also, PIPC Guidelines further provide that such other data must be legally obtainable.

3.4. Sensitive Data

Sensitive data is defined as "personal information regarding an individual's ideology, faith, trade union or political party membership, political views, health, sexual orientation, and other personal information that may cause a material breach of privacy," and further includes genetic information, criminal records, information on an individual's physical, physiological, and behavioral characteristics generated through certain technical means for the purpose of identifying a specific individual and racial/ethnic data as stated in Article 18 of the Enforcement Decree of PIPA (English version without 2020 Amendments available here; up-to-date version only available in Korean here) ("PIPA Enforcement Decree").

3.5. Pseudonymous Information

Personal information "that is pseudonymized in accordance with subparagraph 1-2 below and thereby becomes incapable of identifying a particular individual without the use or combination of information for restoration to the original state (hereinafter referred to as 'pseudonymized information')." 1-2. The term "pseudonymization" means a procedure to process personal information so that the information cannot identify a particular individual without additional information, by deleting in part, or replacing in whole or in part, such information.

- **Is pseudonymous information considered personal information?**

As mentioned above in Section 3.5, pseudonymized information is considered personal information.

- **Are persistent digital identifiers pseudonymous information (e.g., IDFA, cookie IDs, proprietary IDs, IP addresses, etc.)?**

No, we do not believe persistent digital identifiers will be considered pseudonymized information as such data does not appear to be personal information which has been pseudonymized in accordance with the abovementioned subparagraph 1-2 (of Article 2) of the PIPA.

- **Does the law subject pseudonymous information to fewer obligations than "regular" personal information?**

Yes, PIPA subjects pseudonymized information to fewer obligations than "regular" personal information; namely, the exemption of consent requirements which apply to the processing of "regular" personal information.

3.6. Anonymized/De-identified Information

Anonymized/de-identified Information is any information which cannot be used to identify a specific individual even if the information is combined with other information, after reasonably considering factors such as time, cost, technology, is not subject to PIPA.

- **Is there a difference between anonymized or de-identified data?**

Seemingly, yes. For reference, the concept of de-identified information includes both pseudonymized information in 3.5 and anonymized information in 3.6. Previously, the Guidelines for the De-Identification of Personal Information treated de-identified information and anonymized information as similar concepts, but the recently published Guidelines for the Pseudonymization of Personal Information now refers to just pseudonymized information and anonymized information without mentioning the term de-identified information. It has not been clear even between professionals in Korea that the concept of de-identified information exists under the current version of the PIPA (effective from Aug. 5, 2020) or is it a hybrid of pseudonymized and anonymized, as there were not many de-identification cases under the Guidelines for the Pseudonymization of Personal Information. But, generally speaking, de-identified data under the Guidelines for the De-Identification of Personal Information is a concept close to that of anonymized data under the GDPR, based on the explanation set forth in such Guidelines.

- **What common data categories are passed between publishers, advertisers, and ad tech companies that fall into this category when no persistent identifier is present (e.g., browser type, device type, operating system, app name, publisher site)?**

The KCC Online Processing Guidelines refers to the data used for online behavioral advertising as "behavioral data" which is further defined thereunder as the online activity data of users (e.g., website visit history, app usage history, and purchasing/search history) which can be used to identify and analyze, among others, their interests, preferences, and characteristics. There is no law or regulation in Korea that governs online behavioral advertising, behavioral data, or persistent digital identifiers, in particular. However, the collection and processing of cookies and behavioral data, information necessary for conducting online behavioral advertising, is considered "personal information" and subject to notice and consent requirements for the processing of personal information if such information can be used to identify specific individuals. In practice, behavioral data is deemed to be personal information when processed together with user identifiers but is not deemed to be such when processed on a standalone basis.

3.7. Data Controller

The concept of data controller, or personal information controller, under PIPA is similar to the concept of data controller under the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"). As mentioned above, PIPA defines a data controller as "a public institution, corporate body, organization, individual, who, by itself or through a third party, processes, i.e., collects, generates, connects, interlocks, records, stores, retains, processes, edits, searches, outputs, corrects, restores, uses, provides, discloses, destroys, or otherwise handles personal information to administer personal information files for official or business purposes."

3.8. Joint Controller/Co-Controller

Not applicable.

3.9. Data Processor/Service Provider (i.e., an entity that is qualified as a processor or service provider under the law because it meets certain requirements and processes data pursuant to a permissible purpose on behalf of a controller/business)

Data controllers may outsource the processing of personal information to third parties, i.e., data processors.

3.10. Third Party (i.e., a third party that receives data from a business for non-business purposes and does not necessarily have specific requirements under the law as to such data, such as a third-party under the CCPA)

Not applicable.

4. DATA CONTROLLER RIGHTS AND RESPONSIBILITIES

4.1. Overview

Data controllers have various other obligations under PIPA, including handling personal information in a way which minimizes any possible infringement upon the privacy of data subjects, and, where possible, anonymizing personal information, and if anonymization is not possible, pseudonymizing the data before processing. Specifically, data controllers must maintain the security of personal information, taking into account the likelihood and risk of infringement of data subjects' privacy. This likelihood and level of risk may vary depending on various factors such as the types and methods of the handling of personal information. In particular, data controllers are required to take the technical, administrative and physical measures necessary to ensure the security of personal information. These measures include, among other things, the establishment of internal rules for adequate administration of personal information, and the keeping of access logs to prevent personal information from being lost, stolen, leaked, fabricated, or destroyed. PIPA has a prescriptive list of the minimal measures to be taken in this regard.

Data controllers must also provide notice when processing personal information. Explicit consent is generally required prior to the collection/use/provision to third parties of personal information, subject to certain exceptions. The consent for a provision to third parties must be obtained separately from the consent for the collection and use of personal information. Moreover, consent for the processing of particular identification data, i.e., RRNs, passport numbers, driver's license numbers, and alien registration numbers, and sensitive data must be obtained separately from each other, and from any other consent. Personal information must not be used beyond consented purposes unless the separate consent of data subjects has been obtained.

Only a few limited exceptions to this consent requirement are recognized under South Korean law. However,

pursuant to the 2020 Amendments, personal information may be used/provided without the data subject's consent within the scope reasonably related to the original purpose of the collection after considering whether the contemplated use/provision is related to the original purpose of the collection, such use/provision to third parties of the personal information could have been predicted in light of the circumstances surrounding the collection and customary handling practices, the use/provision will not result in any disadvantage to the data subject, and/or the data controller has implemented the necessary safeguards to ensure the security of the personal information (e.g. encryption).

4.2. Accountability

4.2.1. Overview

PIPA recognizes the accountability principle to some extent. Article 3(8) states that "the data controller shall endeavor to obtain the trust of data subjects by observing and performing such duties and responsibilities as provided for in this Act and other related statutes."

4.2.2. Application to Digital Advertising

Advertisers, online behavioral advertising businesses (e.g., ad tech companies), media publishers of online behavioral advertisements, and any other data controllers which collect and use the personal information of users for digital advertising must follow the accountability principle.

4.3. Notice

4.3.1. Overview

Notification through a privacy policy: PIPA has a prescriptive list of information that must be contained in a privacy policy, including, but not limited to, the purposes of use, retention period, information on provision to third parties, and outsourcing and disposal of personal information. Data controllers must publicly disclose their privacy policies in a manner that enables data subjects to examine the terms of these privacy policies, including any revisions made to them, at any time.

If a data controller processes personal information collected from a third party, the data controller must also immediately notify the relevant data subjects of the following matters upon a data subject's request:

- The source of collected personal information;
- The purpose of the processing of personal information; and
- The fact that the data subject has the right to request suspension of the processing of his/her personal information.

In addition, if a data controller processes (i) the sensitive data or particular identification data of 50,000 or more data subjects or (ii) the personal information of one million or more data subjects, and seeks to process any

personal information it receives from a third party (which has provided such personal information pursuant to the data subjects' consent), the data controller must also provide notice to the data subjects of the above matters. However, there is an exception to this notification obligation, whereby the data controller does not need to provide such notice if the data controller does not receive any personal information, such as contact information, through which notification can be made to the data subject.

- **Who must receive notice? When must notice be provided? What must be in the notice in the digital advertising context? (Consider also, what notice needs to be provided when pixels fire on a webpage?)**

PIPA only requires data controllers to disclose a privacy policy (on their internet homepage or through other methods) but does not prescribe exactly when such disclosure must be made. Also, PIPA and other relevant laws do not prescribe any notice requirements related to digital advertising in particular. However, the KCC Online Processing Guidelines recommend the following measures to be taken for the transparent collection/use of behavioral data (please see our explanation below in Section 1.5 for more information on the data protection principles recommended by the KCC Online Processing Guidelines to be followed when conducting online behavioral advertising).

1. Ad tech companies which engage in behavioral advertising via a third party website/app are recommended to insert, within the online behavioral advertisement or a space adjacent thereto, a conspicuous banner and, on a separate page linked to such banner, disclose detailed information related to the online behavioral advertisement such as (i) the names of businesses which are collecting/processing behavioral data, (ii) the items of behavioral data which are collected, (iii) the methods through which behavioral data are collected, (iv) the purposes for collecting behavioral data, (v) the periods of retention/usage of behavioral data and the methods of processing information thereafter (vi) the methods through which users may exercise their informational self-determination rights, and (vii) the methods for providing redress to users for damages related to online behavioral advertising.

2. Publishers which allow ad tech companies to collect behavioral data through their own websites or apps are recommended to provide conspicuous notice (through their privacy policies or otherwise) of information on (i) the names of businesses which are collecting/processing behavioral data and (ii) the methods through which behavioral data are collected.

- **Is there specific notice required for sensitive information?**

PIPA only requires separate (apart from other consent for the collection and use of personal data/transfer to 3rd parties) opt-in consent to be obtained from the data subjects to process sensitive information. No additional notice, such as the risk of processing sensitive information, is required when obtaining separate consent.

- **Are there any specific requirements for providing notice related to processing children's personal information?**

PIPA requires ICSPs to secure certain process to obtain the consent by the legal guardian (typically their parents) of children under age 14.

- **Are there any requirements compelling vendors directly collecting personal information or those receiving it from others to provide additional notices? Who is responsible for those notices? Publishers? Vendors?**

Vendors will be responsible for providing the notices if they directly collect the personal information and are deemed the data controllers (as defined above in Section 3.7) of such personal information. However, as explained above in Section 3.1, it is difficult to uniformly categorize vendors into those which collect data by themselves, receive data from other publishers, and which are entrusted with the processing of data by publishers.

4.3.2. Application to Digital Advertising

- **Do third parties need to be named? For example, if a publisher gives a privacy policy notice that it may share personal information with third parties for advertising purpose, does it have to specify which third parties?**

In order to provide personal information to third parties, data controllers are required to specifically indicate, in the consent form, the names/trade names of the third-party recipients of personal information

There are no specific requirements. The general notice requirements imposed on the data controllers are still applicable.

- **From an industry perspective, it is common to distinguish data use for ad targeting vs. profile building vs. measuring ad campaigns. Does the notice requirement require separate disclosure of those things, or is it enough to say something general like, "advertising and related purposes"?**

With respect to online behavioral advertising, the KCC Online Processing Guidelines impose certain notice obligations related to the collection and use of behavioral data on online behavioral advertising businesses (e.g., ad tech companies) and media publishers of online behavioral advertisements. Additionally, online behavioral advertising businesses are further obligated thereunder to (i) allow consumers to control the receipt of advertisements, (ii) handle complaints made by consumers, and (iii) implement security measures for the protection of behavioral data. (For more details, please see section1.5 above).

4.4. Consent and Exceptions to Consent

4.4.1. Overview

Data controllers must provide notice when processing personal information. Explicit consent is generally required prior to the collection/use/provision to third parties of personal information, subject to certain exceptions.

For your reference, PIPC Guidelines provide that data controllers should (i) provide notice, in a clear and easily understandable manner, of information on the items of personal information collected and the reasons for such collection when obtaining consent from users and (ii) obtain "explicit consent" because they are required to obtain consent in accordance with Article 22 of PIPA (which, among other things, prohibits data controllers from obtaining blanket consent for all types of processing, requires data controllers to provide notice of material information and the scope of consent, requires data controllers to differentiate between required/optional consent (e.g., for marketing/promotional purposes).

In addition, PIPC Guidelines provide that consent for the collection/use of personal information which is required by PIPA should voluntary opt-in (via written signature, oral confirmation, or an online checkbox) consent and be clearly verifiable.

- **For what types of personal information or purposes of processing is consent required?**

Under PIPA, the explicit consent is generally required prior to the collection/use/provision to third parties of personal information subject to certain exceptions. For the definition of personal information, please see section 3.3 (Personal Information).

- **How is valid consent manifested–express consent, opt-in, implied consent, or opt-out?**

The explicit consent is required prior to the collection/use/provision to third parties of personal information and the transmission of for-profit advertisements through an electronic medium.

- **Is specific notice required as part of the consent?**

Under PIPA, data controllers and ICSPs are required to provide notice of the following matters when obtaining consent from data subjects for the collection and use of personal information:

» The purpose of the collection and use of personal information.

» The items of personal information to be collected/used.

» The period for retaining and using the personal information; and

» The data subject's right to refuse his/her consent and outline any disadvantages, if any, which may follow from such refusal.

In addition, data controllers and ICSPs are required to provide notice of the following matters when obtaining consent from data subjects for the provision of personal information to third parties:

» The specific name of the third-party recipient.

» Items of personal information to be shared.

» Third party recipients' purposes of use.

» Period of retention and use by the third-party recipient; and

» The data subject's right to refuse his/her consent and outline any disadvantages, if any, which may follow from such refusal.

Please note that PIPA only requires data controllers to obtain opt-in consent when processing personal information and not in cases where other types of data (which is not personal information) is processed. Yet, the KCC Online Processing Guidelines provide that consent (similar to opt-out consent) should also be obtained in order to process behavioral data–which differs somewhat from what is explicitly prescribed by PIPA. It should be noted that PIPA is a legally binding statute whereas the KCC Online Processing Guidelines represent non-binding regulatory guidance. Thus, PIPC and other regulatory authorities are unlikely to actively investigate a data controller which has adhered faithfully to the KCC Online Processing Guidelines but public prosecutors/courts may decide differently when determining if such data controller has committed a violation of PIPA or other relevant laws.

- **Does the consent obligation require granularity (i.e., consent for distinct processing activities) similar to GDPR, or is the consent obligation more generalized (e.g., requiring consumers to opt-in to "online behavioral advertising" more broadly, without having to consent to each constituent processing activity/ party)? Is consent different for different uses or types of data (e.g., sensitive data, profiling, automated decision making, etc.) Please provide details.**

The explicit consent is generally required prior to the collection, use, and provision to third parties and data processors of personal information, subject to certain exceptions. The consent for a provision to third parties and data processors must be obtained separately from the consent for the collection and use of personal information.

To process sensitive information, the data controller must obtain the data subject's explicit consent separate from the consent to the processing of other personal information.

Under PIPC Guidelines, data controllers must provide notice of legally required information in a manner which is clearly understandable to data subjects when obtaining consent for the processing of personal information. Thus, as in the case of information on the "names of the third-party recipients of personal information," other information which is legally required to be notified, such as the "purposes for the collection/use of personal information," needs to be clearly stated with particularity as well.

When obtaining consent for the collection/use of personal information for marketing or other similar purposes, data controllers are recommended to collect/use only the minimum necessary personal information (after grouping such personal information by similar categories) to achieve such purposes.

For your reference, Naver Corp., which is the largest internet portal operator in Korea, uses wording such as the

following as one of the "purposes of use" for its collection/use of personal information when obtaining consent through its website:

"to analyze service usage records and access frequency, compile statistics on the usage of services, and to provide customized services and place advertisements based on such analysis of services and statistics."

- **Can personal information be processed for secondary purposes (i.e., differing purposes from which it was collected)?**

Personal information must not be used beyond consented purposes unless the separate consent of data subjects has been obtained. But the amended PIPA allows data controllers to use personal information within the scope reasonably related to the original purpose of the collection without the consent of the data subject as mentioned above.

In this regard, Article 14-2 of the Enforcement Decree of PIPA provides that personal information may be additionally used/provided as above without consent after considering, among other factors, (i) whether such additional use/provision is related to the original purpose of the collection, (ii) whether such additional use/provision may result in any disadvantage to the data subject, (iii) whether such additional use/provision was foreseeable in light of the circumstances surrounding the collection of such personal information or the customary practice of processing such personal information, and (iv) whether the data controller has implemented the necessary safeguards to ensure the security of the personal information (e.g., encryption). In light of the foregoing, the additional use/provision of personal information without consent for marketing purposes is unlikely to be permitted under PIPA unless the original purpose of the collection of the personal information in question was for marketing purposes.

- **Are there any rules compelling downstream recipients/processors of personal information to provide additional notices?**

There are no specific rules for that. Thus, transfer of personal data to downstream recipients/processors could be deemed as either transfer to 3rd party (i.e., Controller to controller transfer) or transfer for outsourcing of data processing (controller to processer/sub processer transfer).

- **Are there any issues concerning the timing of consent?**

The explicit consent is required prior to the collection/use/provision to third parties of personal information.

- **Are there distinct consent requirements for sensitive personal information?**

"Sensitive (personal) information" is defined as "personal information regarding an individual's ideology, faith, trade union or political party membership, political views, health, sexual orientation, and other personal information that may cause a material breach of privacy," and further includes genetic information, criminal records, information on

an individual's physical, physiological, and behavioral characteristics generated through certain technical means for the purpose of identifying a specific individual and racial/ethnic data.

To process sensitive information, the data controller must obtain the data subject's explicit consent separate from the consent to the processing of other personal information.

- **Are there distinct consent requirements for profiling consumers? If a business gets consent to use personal data for "advertising and marketing" purposes, is a separate (or more specific?) consent required to build a profile for advertising?**

No, there are not. But profiling might be viewed as collection and use of additional information from the data subjects, as it creates additional items of specific individuals. However, two things should be noted:

(i) Separate consent is required to use personal information for "advertising and marketing" purposes.

(ii) Data items to be generated through profiling may not be specified in detail. For instance, many companies simply say something similar to wordings like, "use [cookies, IP address, device identifiers, ad identifiers...] for personalized services"/"use [cookies, IP address, device identifiers, ad identifiers ...] for personalized advertising and marketing."

- **Are there distinct consent requirements for automated decision making?**

No, there are not.

- **Are there any age restrictions related to consent? Are there distinct consent requirements around processing children's personal information?**

If data controllers and ICSPs seek to process the personal information of children under the age of 14, they are required to obtain the consent of the children's legal guardians. The minimum amount of personal information that is necessary to obtain the legal guardian's consent in the first place may be collected from the child without the legal guardian's consent. Also, such legal guardians are authorized to exercise the children's rights under PIPA and the Network Act.

- **Can consent, however manifested, be revoked?**

Data controllers who are ICSPs must allow data subjects to withdraw their consent to the processing (e.g., collection/use, provision to third parties) of their personal information at any time without exception. Any other data controllers (who are not ICSPs) must respond to a data subject's request to suspend the processing of his/her personal information.

4.4.2. Application to Digital Advertising

Under the Network Act, the recipient's explicit prior consent is required for the transmission of commercial

advertising information through electronic means (e.g., mobile phone, email, etc.) This consent must be obtained in addition to the consent for the collection and use of personal information for marketing purposes. In case of RTB, it may be arguable. However, in practice this clause under the Network Act is applicable to the cases of transmitting the commercial ads through direct call, texting, email, messenger, or other similar methods.

The Location Information Act will be applicable to the collection and processing of location information. If any personal location information is collected for the purpose of location-based advertising, consent for the collection and use of personal location information under the Location Information Act and consent for the collection and use of personal information under PIPA must be obtained, respectively.

There is no law or regulation in Korea that governs behavioral advertising in particular. However, the collection and processing of cookies and behavioral data, information necessary for conducting behavioral advertising, will be subject to notice and consent requirements for the processing of personal information if such information can be used to identify specific individuals.

4.5. Appropriate Purposes

4.5.1. Overview

Unlike the GDPR, PIPA in principle requires explicit informed consent to be obtained for the processing of personal information via consent forms after providing notice of certain matters prescribed by law and separate consent must be obtained for each category of processing (e.g., collection and use, provision to third parties). Although PIPA also recognizes legitimate interest and other legal bases under the GDPR as valid grounds for processing personal information, such legal bases are only recognized in limited scope.

Article 15(1)(vi) of PIPA exceptionally provides that personal information may be collected and used without consent in cases where the collection/use is necessary to achieve a legitimate interest of the data controller and where such legitimate interest clearly overrides the rights of the data subject (provided that the collection/use is substantially relevant to the legitimate interest of the data handler and that the collection/use is only done to a reasonable extent). PIPC Guidelines provide that "the preparation/procurement of supporting materials for the collection/calculation of service fees, collection of debts, and commencement/continuation of legal action" may be examples of what may constitute a "legitimate interest."

Accordingly, the aforementioned "legitimate interest" exception is unlikely to apply in cases where the purposes for the collection/use of personal information relates to marketing. In addition, as explained above, the recent amendments to PIPA permitting the additional use/provision of personal information without consent are unlikely to apply as well unless the original purpose of the collection of the personal information in question was for marketing.

4.5.2. Application to Digital Advertising

- **Does the law or legal guidance require a specific legal basis for specific digital advertising activities? Clarify for each activity (suggest using TCF/IAB CCPA "purposes") ("profiling" must be addressed here).**

Digital advertising activities which involve "access to data stored on and/or functions installed on the mobile devices of users" may be regulated by Article 22-2 of the Network Act which requires data controllers which are ICSPs to obtain the express prior informed consent of users after providing conspicuous notice of certain legally required information when seeking to access such data/functions on the mobile devices of users in the course of providing their services.

Digital advertising activities which involve "profiling" may be regulated by Article 30 of PIPA which requires data controllers to disclose (usually via a privacy policy on the internet homepage) information concerning the installation, operation, and the right to refuse a device that automatically collects personal information such as internet access information files.

Apart from the foregoing, there is no law or legal guidance which requires a specific legal basis for specific digital advertising activities.

- **If yes, what are the legal bases (e.g., consent, legitimate interest)? Are there any requirements related to lawful basis (need a valid legal basis to process) fairness (scope of processing is fair) transparency (transparent about the processing activity to the consumer and the lawful basis)?**

Not applicable.

- **Does the law address processing for secondary purposes/differing purposes from which it was collected?**

Personal information must not be used beyond consented purposes unless the separate consent of data subjects has been obtained. But the amended PIPA allows data controllers to use personal information within the scope reasonably related to the original purpose of the collection without the consent of the data subject as mentioned above.

4.6. Safeguards

4.6.1. Overview

PIPA requires organizations to implement appropriate security measures with respect to personal information. In addition, PIPA provides lists of physical, organizational, and technological measures that organizations may utilize in the safeguarding of personal information.

4.6.2. Application to Digital Advertising

Details regarding the minimum safeguards to be implemented by ICSPs are provided in "The Standards of Technical

and Managerial Safeguards for Personal Information." (only available in Korean here[1]) which prescribe standards for various security measures for the protection of personal information such as the following.

- Establishment and implementation of internal control plan.
- Restriction of access to the personal information processing system ("PIPS").
- Prevention of falsification/alteration of access records to PIPS.
- Encryption of personal information.
- Prevention of malicious codes/programs.
- Prevention of physical access.
- Security measures when printing/copying materials containing personal information.
- Security measures which restrict the labelling of personal information.

5. DATA SUBJECT RIGHTS/EXEMPTIONS

5.1. Overview

The data controller must ensure that personal information is accurate, complete, and up to date to the extent necessary for achieving the purposes of its handling, and data subjects may exercise their rights of access, correction, suspension of use, and removal of their personal information and withdrawal of consent to the processing of their personal information. To this end, PIPA also has prescriptive procedural rules to ensure data subjects' exercise of such rights.

5.2. Access

Under PIPA, a data subject may request access to his/her personal information processed by the data controller. The right of access may be denied to the extent it may possibly cause damage to the life or body of a third party, or improperly violate the property and other interests of a third party.

The request must be made in accordance with the procedure determined by the data controller. Such procedure should meet the following requirements: (i) the methods available to the data subject in making the request need to be data subject-friendly, such as in writing, by telephone or electronic mail, or via the Internet; (ii) data subjects must be able to request access at least through the same window or in the same manner that the data controller uses to collect such personal information, unless a justifiable reason exists (e.g. difficulty in continuously operating such window), and (iii) details regarding the manner and procedure for exercising the right to request access is to be posted on the website operated by the data controller (if such website exists).

5.3. Rectify

Under PIPA, a data subject who accesses his/her personal information has the right to request rectification/erasure of his/her personal information. The data controller must rectify the personal information immediately upon receiving such a request and notify the data subject of the results, within 10 days from the date of receiving such a request.
The request must be made in accordance with the procedure determined by the data controller. Such procedure should meet the foregoing requirements set forth 5.2.

5.4. Deletion/Erasure

Please see above at section 5.3.

Exception to the right of erasure: erasure is not permitted when the collection of the said personal information is required by other laws.

5.5. Restriction on Processing

Under PIPA, a data subject has the right to request suspension of the processing of his/her personal information.

Data controllers must comply with a data subject's request to suspend processing of his/her personal information unless one of the following exceptions applies:

(i) Where special provisions exist in law or it is inevitable to observe the data controller's legal obligations.

(ii) Where access may possibly cause damage to the life or body of a third party, or unfairly infringe upon a third party's property or other interest; or

(iii) Where the data controller would not be able to perform the terms of a contract entered into with the data subject if it does not process the personal information and the data subject did not clearly indicate his/her intention to terminate the contract.

The request must be made in accordance with the procedure determined by the data controller. Such procedure should meet the foregoing requirements set forth 5.2.

For your reference, PIPA provides similar concept to the right to restrict of processing under GDPR, there are some key differences. For instance, unlike GDPR, PIPA only recognizes the right to withdraw consent with respect to data controllers who are ICSPs. Data controllers (who are not ICSPs) must respond to a data subject's request to suspend the processing of his/her personal information. PIPA does not explicitly provide for the right to object nor right to restriction on processing. A data subject may exercise this right to suspension against the data controller whether such processing is based on his/her consent, legitimate interest of the data controller, or not unless the exceptions

above. This right to suspend the processing might be similar to the rights to restriction of processing or to object under GDPR.

5.6. Data Portability

Not applicable.

5.7. Right to Object

Please see section 5.5. above.

5.8. Right Against Automated Decision-Making

Not applicable.

5.9. Responding to Consumer Rights Requests

The request must be made in accordance with the procedure determined by the data controller. Such procedure should meet the foregoing requirements set forth 5.2. The data controller must respond to the data subjects who request access, correction, suspension of use, and removal of their personal information within 10 days of receiving the request. The response should either be confirmation that the data subject's personal information has been processed (if the request was granted), or the fact that the request has been denied and the reasons for such denial and method of objecting to such denial.

5.10. Record Keeping Concerning Rights Requests

None.

5.11. Is Providing Consumers with These Rights Required by Law or Mere Suggestions?

It is required by law.

5.12. Application to Digital Advertising

As mentioned above, advertisers, online behavioral advertising businesses (e.g., ad tech companies), media publishers of online behavioral advertisements, and any other data controllers which collect and use the personal information of users for digital advertising must allow such users to exercise their rights as data subjects. And data controllers who process personal information which they have received from other data controllers must also allow such users to exercise their rights as data subjects.

In addition, the KCC Online Processing Guidelines provide that ad tech companies must provide users with the means and methods to easily choose (similar to an opt-out in this respect) whether or not to provide their behavioral data and to receive online behavioral advertisements. However, such regulatory guidance does not correspond exactly with applicable requirements under PIPA, and PIPC has yet to clearly opine on this issue. Yet, because even the KCC Online Processing Guidelines provide that behavioral data should be viewed as personal information if

capable of identifying. The right to suspend the processing mentioned in section 5.5 above could be the basis for demanding such opt-out under the KCC Online Processing Guidelines above if it is personal information.

6. DATA CONTROLLER AND PROCESSOR AGREEMENTS

6.1. Overview

Under PIPA, outsourcing the processing of personal information to a third-party data processor requires a written agreement.

6.2. Data Controller Outsourcing of Processing

Outsourcing the processing of personal information to a third-party data processor requires a written agreement that must include:

- The terms prohibiting a data processor from processing personal information for any purpose other than for the performance of outsourced tasks.
- The technical and administrative safeguards implemented for the protection of personal information; and
- Any other matters prescribed by the PIPA Enforcement Decree for the safe administration of personal information.

South Korean legislation does not provide specific requirements in relation to cookies and third parties, in terms of entering into a data transfer agreement.

6.3. Data Processor Rights and Responsibilities

As data processors are likely to be treated as data controllers, data processors will, in general, be subject to the same legal obligations as those applicable to data controllers. In the case of a violation of PIPA by a data processor, i.e., an outsourced service provider, the data processor will be deemed as an employee of the data controller and the data controller will have vicarious liability, provided, that the same shall not apply where such corporation or individual has not been negligent in taking due care and supervisory activities concerning the relevant business affairs to prevent such offense.

Regarding the vicarious liability of data controllers, the Supreme Court of Korea has previously decided that a credit card company, and the credit information company which was contracted by said credit card company to develop a fraud detection system on its behalf, shall be jointly liable for damages arising from the leakage of personal information caused by the employee of the credit information company.

In addition, the proviso to Article 74(1)(ii) of PIPA states that "provided, however, that the same shall not apply in cases where such company or individual has not been negligent in exercising due care and supervision concerning the relevant business affairs to prevent the commission of the violation" thereby providing for cases where the company or an individual with relevant responsibility may be exempted from vicarious liability stemming from violations of PIPA committed by their employees. However, it appears that the foregoing exemption is rarely recognized by courts/regulators in practice.

For your reference, with respect to the transfer of personal information to third parties, the Supreme Court of Korea has previously held that the provision of personal data to third parties should refer to cases where a data transfer (that is beyond the original purposes for the collection/use of personal information) is conducted for the benefit and business purpose of the transferee whereas the outsourcing of the processing of personal information to third parties should refer to cases where a data transfer (that is consistent with the original purposes for the collection/use of personal information) is conducted for the benefit and business purpose of the transferor.

In addition, the Supreme Court of Korea further opined that the totality of the circumstances, after reviewing factors such as the purposes and methods of obtaining personal information, whether any consideration has been given/received in exchange for the transfer of personal information, whether the recipient of personal information is actually being supervised/managed, the effect of the transfer on the data subject/user's need to protect his/her personal information, and the party who will ultimately use the personal information, should be considered when determining whether a transfer of personal information to a third party should be viewed as a provision or an outsourcing.

Accordingly, although it is not entirely clear based on the provided information, the relationship between and among ad tech companies, publishers, and advertisers may be viewed as an outsourcing if such relationship meets the aforementioned factors related to an outsourcing.

6.4. Application to Digital Advertising

Advertisers, online behavioral advertising businesses (e.g., ad tech companies), and media publishers of online behavioral advertisements which outsource the processing of the personal information of users to third parties must do so pursuant to a written agreement which contains certain information prescribed by PIPA.

7. DATA TRANSFER & OUTSOURCING

7.1. Overview

There are separate requirements for provision to third parties and outsourcing to data processors.

Specifically, a provision to third parties refers to cases where a data transfer is conducted for the benefit and

business purpose of the transferee, whereas outsourcing refers to cases where a data transfer is conducted for the benefit and business purpose of the transferor.

The prior consent of data subjects is required in order to conduct a provision to third parties, whereas in the case of an outsourcing, PIPA does not require the prior consent of data subjects.

Data controllers may not enter into data transfer agreements which violate relevant laws and regulations. In particular, PIPA requires data controllers to obtain the prior consent of data subjects when conducting a provision to a third party overseas. For ICSPs and recipients of personal information provided by ICSPs, the prior consent of data subjects will be required for all cross-border transfers, irrespective of whether such transfer constitutes a provision or outsourcing, unless an exception is applicable. However, in the case of cross-border transfers constituting an outsourcing or storage, such consent may be omitted so long as the following information is disclosed in the ICSP's privacy policy: (i) items of the personal information to be transferred, (ii) countries where the personal information is to be transferred and the date/time/methods of transfer, (iii) recipients (if the recipient is a corporation then the name of the corporation and the contact information of the person in charge of the management of personal information) to whom the personal information is to be transferred to, and (iv) the purposes of use and the periods of retention of such recipients of personal information.

7.2. Application to Digital Advertising

Advertisers, online behavioral advertising businesses (e.g., ad tech companies), and media publishers of online behavioral advertisements which outsource the processing or storage of the personal information of users to third parties located outside South Korea must do so pursuant to the consent of such users or disclosure in the privacy policy of certain information prescribed by PIPA.

In principle, PIPA requirements applying to cross-border transfers of personal information will need to be complied with when conducting Real Time Bidding as relevant laws/regulations, and guidance do not recognize any particular exceptions for Real Time Bidding. That said, regulatory authorities have yet to clearly opine on the issue of Real Time Bidding or the regulation of digital advertisements in general.

8. AUDIT/ACCOUNTABILITY

8.1. Overview

- **Audit - What audit rights are dictated by law (e.g. must companies have audit rights over their vendors? Does it matter what the classification of those vendors are?)**

Under PIPA, companies which outsource the processing of personal information to vendors are required to manage and supervise such vendors for the secure processing of personal information.

- **Accountability - Must companies/vendors keep certain records to prove they have met certain requirements? What are those requirements?**

Under PIPA, companies which outsource the processing of personal information to vendors must be able to check how personal information is being managed by such vendors and thus, it would be practically recommendable for vendors to keep records on how personal information is being managed internally.

8.2. Application to Digital Advertising

Advertisers, online behavioral advertising businesses (e.g., ad tech companies), and media publishers of online behavioral advertisements which outsource the processing of the personal information of users to third parties are required to manage and supervise such third parties for the secure processing of personal information.

9. DATA RETENTION

9.1. Overview

The basic principles applicable to data retention include:

» The principle of fair and legitimate collection of the minimum necessary personal information to the extent necessary for the explicitly stated and consented purposes; and

» The principle that such personal information must be handled only to the extent necessary for the explicitly stated and consented purposes.

If the retention of personal information is required by South Korean law or regulations beyond the retention period notified to, and consented by, data subjects, such personal information will need to be kept separate from any other personal information.

If the Special Provisions for ICSPs apply, in order to protect personal information of the users who do not use information and communications services for a period of one year, ICSPs must either destroy the inactive user's personal information immediately after the aforementioned time period or separate the inactive user's personal information from other users' personal information for separate storage and administration.

9.2. Application to Digital Advertising

Under PIPA, advertisers, online behavioral advertising businesses (e.g., ad tech companies), and media publishers of online behavioral advertisements which process the personal information of users will be required to destroy such personal information as soon as it is no longer necessary. If the continuing preservation of such personal information is required by another law or regulation, then such personal information must be separated and stored separately from other "ordinary" personal information. In addition, the personal information of inactive users (i.e., at

least 1 year of inactivity) must also be separated and stored separately from other "ordinary" personal information.

10. DATA PROTECTION AUTHORITY REGULATORY AUTHORITY

10.1. Overview

Under the amended PIPA, PIPC is assigned with the role of supervisory authority.

10.2. Main Regulator for Data Protection

The main data protection authorities are:

- PIPC
- KCC
- Korea Internet & Security Agency (KISA)
- Financial Services Commission (FSC)

10.3. Main Powers, Duties and Responsibilities

The main powers of PIPC are:

- Enforcing PIPA
- Addressing issues regarding formal interpretations
- Imposing administrative fines, penalty surcharges, corrective orders, and other administrative sanctions
- Shaping data protection policy and
- Assessing the enactment/amendment of laws and administrative measures relating to the protection of personal information

The main functions of KCC are:

- Enforcing the Network Act
- Addressing issues regarding formal interpretations and
- Imposing administrative fines, penalty surcharges, corrective orders, and other administrative sanctions

The main duty of KISA is to:

- Perform tasks delegated to it by KCC and PIPC

The main duties of FSC are:

» Enforcing the Credit Information Act

» Addressing issues regarding formal interpretations and

» Imposing administrative fines, penalty surcharges, corrective orders, and other administrative sanctions

10.4. Application to Digital Advertising

Advertisers, online behavioral advertising businesses (e.g., ad tech companies), and media publishers of online behavioral advertisements (i) which process the personal information of users will be subject to the jurisdiction of PIPC (ii) and any of the foregoing which are deemed ICSPs or which electronically transmit commercial advertising information will be subject to the jurisdiction of KCC.

11. SANCTIONS

11.1. Overview

Regulators such as PIPC, KCC, and FSC may impose various administrative sanctions such as corrective orders, administrative fines, and penalty surcharges for violations of respective laws and regulations. Public prosecutors may also investigate any violations which are also subject to criminal punishment.

Under PIPA, anyone who knowingly receives personal information which lacks proper consent (for the provision thereof to such person) may also be subject to criminal punishment. Similarly, anyone who receives personal information for a for-profit or improper purpose with knowledge that the provider thereof has used/provided such personal information in violation of PIPA may also be subject to criminal punishment.

11.2. Liability

- **Scope of liability for publishers and advertisers for processing activities of ad tech companies**

  See below.

- **Scope of liability for ad tech companies for collection activities of publishers and advertisers**

  See below.

- **Scope of liability for ad tech companies for other ad tech companies they enable to process data (either b/c they make the decision of pub or advertisers or agency dictates it)**

PIPA and the Network Act only provide that an outsourced processor of personal information shall be deemed an employee of the outsourcing data hander but do not contain any other provisions which specifically deal with liability for violations related to the outsourcing of the processing of personal information or the electronic transmission of commercial advertising information.

In this regard, please refer to our above explanation in Section 6.3 for more information regarding the vicarious liability of data controllers for violations of PIPA committed by their outsourced processors. Please also refer to our above explanation is Section 3.1 for more information regarding why it is difficult to uniformly define the data processing categories of ad tech companies in the digital marketplace.

11.3. Enforcement and Market Practice

- **How are claims raised under the law?**

Under PIPA, data subjects may seek compensation against data controllers for any damages they suffer due to violations committed by such data controllers.

A data subject who has his/her rights/interests infringed upon by a data controller or an ICSP who processes his/her personal information may report such infringement to the data protection authorities mentioned above in 10.2 and investigative authorities such as the public prosecutor.

- **Who enforces them?**

Enforcement will be done by the data protection authorities in cases where a report has been made to them and by court decision in cases where a report has been made to the investigative authorities.

- **What's their practice (quietly working with companies to fix, publicly coming out with large investigations? Fact specific?)**

In the case of minor violations, it is common practice for data protection authorities to first issue a corrective order followed by the imposition of sanctions for a failure to obey such corrective order. In the case of more serious violations, data protection authorities are likely to impose sanctions or make criminal referrals from the outset.

- **What up-to-date guidance has been shown on how to handle requirements in the ad ecosystem? Have the regulators been educated on how the ecosystem operates? Have compliance regimes been discussed with them? Has their feedback been solicited?**

To date, guidance on advertisements has been issued in the form of the KCC Online Processing Guidelines. These guidelines were finally issued following a public review period to solicit feedback from the private sector and thus, the pertinent KCC officials who were initially involved with preparations back then would have likely had a good understanding of the advertising ecosystem. However, following the recent transfer (from KCC to PIPC) of enforcement authority on August 5, 2020, it is not clear if the current officials in charge at PIPC possess the same level of understanding.

11.4. Remedies

Regulators such as PIPC, KCC, and FSC may impose various administrative sanctions such as corrective orders,

administrative fines, and penalty surcharges for violations of respective laws and regulations.

Public prosecutors may also investigate any violations which are also subject to criminal punishment. Additionally, data controllers may become civilly liable to any data subjects who suffer damages as a result of such violations.

11.5. Private Right of Action

Under PIPA, data subjects may seek compensation against data controllers for any damages they suffer due to violations committed by such data controllers. Such damages are capped by statute to three million won (approximately $3,000 USD at this time) per data subject so affected.

Specifically, under Article 39-2 of PIPA, data subjects may claim statutory damages (up to KRW 3 million without having to prove their actual damages) against data controllers who are intentionally or negligently at fault for the loss, theft, leakage, falsification, alteration, or damage of personal information. In such cases, the burden will fall upon the data controllers to prove that they have not been intentionally/negligently at fault in order to avoid liability for the claimed statutory damages.

In addition, data controllers may also be liable under Article 39(3) of PIPA for punitive damages (up to treble the amount of damages proven by data subjects) if data subjects have suffered actual damages due to the loss, theft, leakage, falsification, alteration, or damage of personal information resulting from their intentional or grossly negligent acts/omissions unless the data controllers can successfully prove otherwise.

Finally, data subjects may also seek compensation against data controllers based on general tort liability under the Civil Code for any damages (both economic and non-economic damages such as mental anguish) they suffer due to violations of PIPA by such data controllers.

In practice, courts have tended to award damages (usually ranging from KRW 100,000 to KRW 200,000 per data subject) arising from the leakage of personal information on a case-by-case basis after considering the facts of a particular situation.

11.6. Digital Advertising Liability Issues

According to the KCC Online Processing Guidelines, ad tech companies are recommended to have in place measures (e.g., make inquiries, exercise rights as data subjects, report damages) to provide redress to users who have suffered damages related to online behavioral advertising.

Advertisers, online behavioral advertising businesses (e.g., ad tech companies), and media publishers of online behavioral advertisements which process the personal information of users or which are deemed ICSPs may have sanctions imposed by the data protection authorities mentioned above in 10.2 and may also be found by a court to be civilly/criminally liable to data subjects.

12. NOTIFICATION | CERTIFICATION | REGISTRATION

12.1. Overview

There are no legal obligations for data controllers and/or data processors to notify, certify, or register in relation to their data processing activities.

12.2. Requirements and Brief Description

There are no legal obligations for data controllers and/or data processors to notify any regulatory authority of their data processing activities.

Under PIPA and the Network Act, there is a certification system called the Personal Information and Information Security Management System (ISMS-P). While the Network Act requires certain qualified ICSPs to be certified under ISMS-P, PIPA only provides that data controllers be certified under the ISMS-P on the basis of voluntary participation.

12.3. Application to Digital Advertising

There are no particular reporting or registration obligations related to digital advertising under relevant laws/regulations and regulatory guidelines in South Korea.

13. DATA PROTECTION OFFICER

13.1. Overview

PIPA requires data controllers to appoint a data protection officer ("DPO").

13.2. DPO – Compulsory Appointment (Yes/No)

Yes.

13.3. Requirements

Under PIPA, all data controllers must appoint qualified officials as DPO to take charge of all aspects of their handling of personal information. Specifically, data controllers, excluding public institutions, must appoint a person satisfying any one of the following conditions as their DPOs:

- The owner or representative director of a business or
- An executive officer, however if there are no executive officers, then the head of the department responsible for processing personal information.

The DPO is not, however, required to be based in Korea or be fluent in the Korean language.

That said, ICSPs without a business presence in Korea that, nevertheless, provide online services to users in Korea and meet certain legally prescribed thresholds (i.e., (i) annual revenue of at least KRW 1 trillion in the previous year, (ii) annual revenue of at least KRW 10 billion in the information and communications sector, (iii) daily average number of users whose personal data is stored/managed was at least 1 million for the last three months of the previous year, or (iv) anyone who has been ordered by PIPC to submit relevant materials/documents in relation to the actual/potential occurrence of a data breach involving the leakage of personal information which violates/potentially violates PIPA) will be required under the Network Act to designate a domestic representative (i.e., a natural person or legal entity having an address or business office in Korea) to carry out various tasks performed by a DPO on behalf of such ICSPs.

However, data controllers who qualify as small business owners are deemed to have appointed their owner or representative as their DPO unless they specifically appoint someone else.

In the case of public institutions, the DPO must be a public official who meets certain requirements prescribed by law.

13.4. Application to Digital Advertising

Advertisers, online behavioral advertising businesses (e.g., ad tech companies), and media publishers of online behavioral advertisements which process the personal information of users are required to appoint a DPO. In addition, any of the foregoing which are deemed ICSPs and which meet certain legally prescribed thresholds (i.e., daily average of 1 million users during the last three months of the previous year or annual revenue of at least KRW 10 billion in the information and communications sector in the previous year) will be required to appoint an executive officer as their Chief Information Security Officer and report such fact to the Ministry of Science and ICT.

14. SELF-REGULATION

14.1. Overview

- **Are there any industry-self regulatory schemes in place in the jurisdiction?**

Currently, self-regulatory organizations are permitted to operate upon designation as such by PIPC. If an organization which has been designated by PIPC as a self-regulatory organization is determined to have faithfully complied with its internal regulations then this fact will serve as a mitigating factor when PIPC is deciding punishment for a violation of PIPA by such organization. As of present, there are no self-regulatory organizations or schemes related to digital advertising in particular. However, given the expansion in authority of PIPC following the recent amendments to PIPA and the increasing interest in online behavioral advertising, there is possibility that

self-regulatory organizations or schemes related to digital advertising may yet be designated/established in the future.

- **Are there any signal-based programs used in the territory to assist with digital advertising compliance?**

In Korea, the concept of signal-based programs is somewhat unfamiliar, and it is not clear if signal-based programs are being used for digital advertising here.

14.2. Application to Digital Advertising

Not applicable.

15. PENDING PRIVACY BILLS

15.1. Overview

Recently, PIPC has publicly announced its plans to proceed with additional amendments to PIPA which, among other things, introduces a right to challenge decisions based on profiling, recognizes the right to data portability, unifies regulations applying to online/offline businesses, and permits data transfers to other jurisdictions with adequate levels of data protection.

15.2. Application to Digital Advertising

Not applicable.