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.

Mexico

Cross-Jurisdiction
Privacy Project

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.