LATIN LAWYER

THE GUIDE TO CORPORATE COMPLIANCE

SECOND EDITION

Editors
Andrew M Levine, Reynaldo Manzanarez Radilla,
Valeria Plastino and Fabio Selhorst

The Guide to Corporate Compliance

Second Edition

Editors

Andrew M Levine, Reynaldo Manzanarez Radilla, Valeria Plastino and Fabio Selhorst

Reproduced with permission from Law Business Research Ltd
This article was first published in July 2021
For further information please contact Natalie.Clarke@lbresearch.com

Publisher
Clare Bolton

Deputy Publisher
Rosie Creswell

Senior Account Manager
Monica Fuertes

Senior Content Coordinator
Pawel Frydrych

Head of Production
Adam Myers

Production Editor
Simon Tyrie

Subeditor
Martin Roach

Chief Executive Officer
Nick Brailey

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34-35 Farringdon Street, London, EC4A 4HL, UK

www.latinlawyer.com

ISBN 978-1-83862-750-8

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Acknowledgements

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

Alvarez & Marsal LLP

Andrew Jánszky

Anheuser-Busch InBev

Barbosa Müssnich Aragão

Beccar Varela

Buckley LLP

Camargo Corrêa Infra

Carey y Cía

Debevoise & Plimpton LLP

Demarest Advogados

FerradaNehme

Hapvida

Hogan Lovells

Incode Technologies Inc

Kestener, Granja & Vieira Advogados

Lumen Technologies

Maeda, Ayres & Sarubbi Advogados

Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados

Philippi Prietocarrizosa Ferrero DU & Uría

QIL+4 Abogados

Quinn Emanuel Urquhart & Sullivan LLP

Skadden, Arps, Slate, Meagher & Flom LLP

Sullivan & Cromwell LLP

TozziniFreire Advogados

Villarreal-VGF

Vinson & Elkins LLP

Von Wobeser y Sierra, SC

Publisher's Note

Latin Lawyer and LACCA are delighted to publish the second edition of *The Guide to Corporate Compliance*.

Edited by Andrew M Levine, a litigation partner at Debevoise & Plimpton LLP, Reynaldo Manzanarez Radilla, a corporate attorney and compliance professional at Incode Technologies Inc, Valeria Plastino, vice president, general counsel and regional compliance officer at Lumen Technologies, and Fabio Selhorst, general counsel, chief integrity officer and chief communications officer at Hapvida, this new guide brings together the knowledge and experience of leading practitioners from a variety of disciplines and provides guidance that will benefit all practitioners.

We are delighted to have worked with so many leading individuals to produce *The Guide to Corporate Compliance*. If you find it useful, you may also like the other books in the Latin Lawyer series, including *The Guide to Infrastructure and Energy Investment* and *The Guide to Corporate Crisis Management*, as well as our jurisdictional references and our new tool providing overviews of regulators in Latin America.

My thanks to the editors for their vision and energy in pursuing this project and to my colleagues in production for achieving such a polished work.

Contents

Part 4

Legislative and Regulatory Pressure Points

CHAPTER 21

Demonstrating Compliance with Data Privacy Legislation

Devika Kornbacher, Palmina M Fava, Jessica Heim and Gabriel Silva[1]

The data protection phenomenon that originated in Europe has swept across Latin America in recent years. While Chile was the first country to enact a law on data protection in 1999, several other countries followed this trend, including Argentina (2000), Uruguay (2008), Mexico (2010), Costa Rica (2011), Peru (2011), Colombia (2012), Brazil (2018) and Panama (2019).[2] These recently enacted privacy laws in Latin America follow the European Union's General Data Protection Regulation (GDPR) model. Costa Rica, for instance, is engaged in a comprehensive reform of its data privacy laws based on the GDPR model. On 28 January 2021, Costa Rica proposed a reform of the existing data protection laws,[3] aiming to restructure the existing data protection agency (PRODHAB) and to adopt Convention 108 of the European Union on Protection of Personal Data.[4]

Although Chile was the first country to regulate data privacy in Latin America, its legal framework soon became obsolete and in need of reforms due, in large part, to the lack of an official data privacy authority and the imposition

1 Devika Kornbacher, Palmina M Fava, Jessica Heim and Gabriel Silva are partners at Vinson & Elkins LLP. The authors would like to thank associates Chris James and Briana Falcon and law clerk Gabriela Astolphi of Vinson & Elkins LLP for their assistance in the preperation of this chapter.

2 https://www.eff.org/deeplinks/2020/09/look-back-and-ahead-data-protection-latin-america-and-spain.

3 https://www.giromartinez.com/news/costa-rica-comprehensive-reform-on-data-privacy/.

4 https://www.larepublica.net/noticia/iniciativa-busca-incluir-la-proteccion-de-datos-como-un-derecho-autonomo-en-la-constitucion.

of low fines.[5] In this sense, inspired by the GDPR model, in 2017, Bill No. 11144-07 was introduced to the Chilean National Congress aiming to modernise the existing legal framework and to create a new data protection agency, which would allow for the enforcement of the data protection legislation. The approval process in Chile has been slow, but on 15 December 2020, the Chilean government categorised the bills as 'urgent', aiming to accelerate the process. The bill is expected to be approved and to become law in 2021.

Colombian data privacy laws are widely viewed as the most modern data protection laws in Latin America and enforcement has been noted favourably. For instance, on 26 November 2020, the Colombian data protection authority mandated that a videoconference service provider implement measures to secure the personal data of its users in Colombia, in accordance with the existing data protection law.[6] Also, throughout 2020, several fines were imposed on companies for violation of the data protection rules. Colombian authorities are considering several measures to enhance local laws, including through Draft Bill No. 339 of 2020 that addresses cyber crimes and the financial Superintendency draft resolution that seeks to introduce new report protocols for cybersecurity incidents and to implement traffic protocols for data exchanges.[7]

Similarly, Mexico, Brazil and Argentina have undertaken measures to enhance data privacy protections. In 2010, Mexico adopted the Federal Law on the Protection of Personal Data in Possession of Individuals. Since then, the executive branch has issued several other regulations and guidelines establishing further parameters for the existing data protection law. In 2017, the General Law for the Protection of Personal Data in Possession of Obligated Subjects entered into force, regulating, among other aspects, data protection in connection with the use of data held by public entities, including law enforcement agencies.[8] The Mexican data protection laws and regulations apply to all personal data information when it is processed (1) in a facility located in a Mexican territory; (2) anywhere in the world, if the information is processed on behalf of a Mexican data controller; (3) regardless of its location, if the Mexican legislation is applicable due to Mexico being part of an international convention; and (4) by using means located in Mexico.

---

5 https://www.dataguidance.com/notes/chile-data-protection-overview.

6 www.sic.gov.co/slider/superindustria-ordena-la-plataforma-zoom-reforzar-medidas-de-seguridad-para-proteger-los-datos-personales-de-los-colombianos.

7 https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/colombia.

8 http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf.

As with other data protection laws throughout Latin America and the world, the Mexican, Brazilian and Argentinian laws and regulations broadly define personal data as any information pertaining to an identified or identifiable individual and impose stiff penalties for violations. For example, violation of privacy laws in Mexico may result in fines and imprisonment, including sanctions in the range of 100 to 320,000 times the Mexico City minimum wage (currently €138.9 per month). The law also provides for imprisonment (varying from three months to five years) depending on the seriousness of the violation.[9] Violation of privacy laws in Brazil may result in warnings and fines in the range of up to 2 per cent of the annual global turnover for the breaching entity, but limited to a total amount of 50 million reais per infraction.[10] And in Argentina, violations of privacy laws could result in both monetary fines and imprisonment.

Inspired by the GDPR, in 2018, Brazil enacted its long-awaited data protection law, the LGPD. The LGPD attempted to unify over 40 different statutes that previously governed the use of personal data in Brazil. But the LGPD only became effective in September 2020. The LGDP anticipated the creation of a federal agency (the Brazilian National Data Protection Authority (ANPD)), which was officially created in October 2020 after the Brazilian Senate appointed the first officers to serve as the decision-making body of this entity.[11] On 28 January 2021, the newly formed ANPD published its regulatory strategy for 2021 to 2023 and its work plan for 2021 to 2022. According to such strategies and plans, the agency aims to promote the strengthening of the culture of protection of personal data; establish an effective regulatory environment for the protection of personal data; and improve the conditions for legal compliance.[12] In the work plan for 2021 to 2022, the agency established priority measures and time frames for implementation, with the most critical steps being the creation of the internal regulation and strategy plan for the ANDP, protection of data related to small to medium sized companies and startups, and the evolution of administrative rules regarding application of sanctions.[13]

---

9 https://iapp.org/resources/article/dla-piper-data-protection-laws-of-the-world/.

10 https://iapp.org/resources/article/dla-piper-data-protection-laws-of-the-world/.

11 https://www12.senado.leg.br/noticias/materias/2020/10/20/senado-confirma-primeira-diretoria-da-autoridade-nacional-de-protecao-de-dados.

12 https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-planejamento-estrategico-para-2021-2023?mkt_.tok=eyJpIjoiT1RjMk56ZzBNbU00WlRKaSIsInQiOiI4WE5KXC9kUmRPVnlLWWJXUGhEUWxcL1RVWDI3K2xPaHpNXC9ub1p1b2F0V2tmb2xwU3B5NnNBeVA5azJWbVwvSzZaMGNDVzRMNE9GcnJMVkducWJWZDZDbFhVeTFqdm4xS2hFQWZVS2tIT01maEZHcFk2ZnZJYVwvNzRhdlVCaGx0YzlVIn0%3D.

13 https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313.

The LGPD applies to any personal data processing operation, carried out by a natural person or by a legal person under public or private law, regardless of the means by which such information is processed or the country where the information is stored, provided that: the information is processed within a Brazilian territory; the processing activity has the purpose of offering or supplying goods or services or the processing of data is related to individuals located in Brazil; or the personal data has been collected in Brazil.[14] Notably, data that is anonymised is not considered personal data, unless the anonymisation process may be reversed by reasonable means.[15]

Pursuant to principles articulated in the Argentinean Constitution, Argentina has a comprehensive data protection legal framework established by Law 25.326/2000, as further regulated by Decree 1558/2001. Since 2017, the Access to Public Information Agency has served as the data protection oversight authority in Argentina, responsible for enforcing the data protection law. Law 25.326/2000 applies throughout Argentina and to any processing of personal data carried out online.[16]

Introduction to GDPR

On 26 May 2018, the GDPR went into effect. The GDPR applies to an organisation established in the EU that processes personal data, whether or not that processing occurs in the EU, and to an organisation established outside the EU that markets goods or services to the EU or monitors the behaviour of individuals in the EU. Several companies based in Latin America trigger this second prong of the GDPR. Compliance with the GDPR, and the derogations of the various EU Member States, requires implementing various technical, administrative and organisational measures.

Conducting a data inventory

Most entities will need to conduct a thorough review of data held, collected, or processed by the entity as a first step in complying with the GDPR. Through a review of this kind, often called data mapping or data inventory, an entity will gain insight into what personal data is collected and used, where such data is stored, processing activities, and retention practices. This information will allow

14 http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

15 http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

16 https://www.linklaters.com/en/insights/data-protected/data-protected---argentina#:~:text=No%20person%20can%20be%20compelled,be%20identified%20from%20that%20information.

the covered organisation to undertake (and later document) other compliance obligations, including creating a record of data processing activities as required under Article 30 of the GDPR and demonstrating a lawful basis for processing for each activity as required by Article 6 of the GDPR.

Identifying lawful bases for processing

Processing is only lawful under the GDPR to the extent that one of the bases listed in Article 6 applies to the processing activity. These bases include consent from the data subject (which can be withdrawn); performance of a contract; compliance with a legal obligation; demonstrated need for a task of public interest or official authority; and the existence of legitimate interests (where not overridden by the interest or fundamental rights or freedoms of the data subject). Although Article 6 states that processing is lawful where 'at least one' of the bases applies, the Article 29 Working Party's guidance provides that '[a]s a general rule, a processing activity for one specific purpose cannot be based on multiple lawful bases'.

Companies should identify and document a lawful basis of processing for each of the activities identified in the data inventory and must furnish both the purpose of processing and its lawful basis when and where data is collected.

Understanding the rights of data subjects

In addition to requiring a lawful basis (e.g., consent or performance of a contract) for each processing activity, the GDPR provides the following rights to data subjects:

- Right to be informed. Data subjects have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.
- Right of access. Data subjects have the right to access and receive a copy of their personal data and other supplementary information.
- Right to rectification. Data subjects have the right to have inaccurate personal data rectified or completed if it is incomplete.
- Right to erasure. Data subjects have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.
- Right to restrict processing. Data subjects have the right to request the restriction or suppression of their personal data.
- Right to data portability. Data subjects have the right to obtain and reuse their personal data for their own purposes across services.

- Right to object. Data subjects have the right to object in relation to all or a portion of the personal data held by an entity. Data subjects also may object to a particular purpose for which their data is processed.
- Rights related to automated decision-making. Data subjects have the right not to be subject to a decision which produces legal effects or significantly impacts the data subject based solely on automated processing, including profiling.

Prohibitions on special categories of data

According to Article 9 of the GDPR, any data 'revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership', as well as 'genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation', is prohibited unless it meets one of the exceptions set out in Article 9. The most notable and widely applicable Article 9 exception is 'explicit consent' to the processing for one or more specified purposes given by the data subject. The Working Party guidance suggests that 'explicit consent' is a more stringent requirement than ordinary Article 6 consent. Specifically, the Working Party has suggested that a written statement, signed by the data subject where appropriate, is one means of demonstrating this requirement. This specific consent exception does not apply where European Union or Member State law prohibits such processing of special categories of data.

Identifying key stakeholders and appointing a data protection officer

Businesses with identified invested stakeholders are more likely to achieve successful compliance. A successful privacy team will be cross-discipline, including parties with technological expertise, as well as those with insight into current and planned business activities. In addition, Article 37 requires a business to appoint a data protection officer (DPO) under the GDPR when:

- it is a public authority or body;
- it conducts regular and systematic monitoring of data subjects on a large scale;
- the business' core activities consist of processing on a large scale of special categories of data or of personal data relating to criminal cases; or
- it is required to do so by Member State law.

A DPO will guide the organisation's GDPR compliance efforts, while serving as a point of contact for data subjects and working with data protection authorities as necessary. DPOs should remain available to company leadership and the privacy team, while maintaining sufficient independence. If an organisation

appoints a DPO even when not required by the GDPR, all the requirements of the GDPR related to DPOs remain applicable. Therefore, appointing a 'data protection officer' versus a 'data privacy officer' should be considered carefully. If an organisation decides that a DPO should not be appointed, that decision should be documented for later reference.

Contracting with Data Processors

Article 29 explicitly prevents processors from processing personal data except on the controller's instructions. Article 28 provides details on documenting these instructions by written agreement.

In particular, Article 28 dictates that controllers 'use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of [the GDPR] and ensure the protection of the rights of the data subject'. Contracts under Article 28 should include: the subject matter, duration, nature and purposes of the processing; the controller's documented instructions for processing; the categories of personal data to be processed, as well as the categories of impacted data subjects; the controller's obligations and processor's promises to assist with the controller's compliance efforts; and the processor's obligation to implement technical and organisational security measures, maintain confidentiality, delete or return personal data at the conclusion of the relationship, submit to audits, and bind subprocessors to requirements under the GDPR.

Choosing a data transfer mechanism

The GDPR also regulates the processing of data within the European Economic Area (EEA), as well as transfers of personal data outside of the EEA. Under the GDPR, there are three scenarios in which an entity legitimately can transfer personal data to a receiver outside the EEA: the receiver is located within an area covered by an adequacy decision; appropriate safeguards have been established to protect individuals' rights to their personal data; or an exception, such as explicit consent, covers the transfer.

Adequacy decisions are made by the European Commission (the Commission) and establish that a given country has adequate data protection and privacy measures. The countries with current adequacy decisions are Andorra, Argentina, Canada (for commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay, and the United Kingdom (pending approval). In 2016, the Commission issued a partial adequacy decision for the United States, ruling that only personal data transfers that are covered by the EU–US Privacy Shield (the Privacy Shield) provide sufficient protection.

On 16 July 2020, however, the Court of Justice of the European Union (CJEU) announced its decision in case C-311/18, better known as *Schrems II,* upholding the use of standard contractual clauses but striking down the Privacy Shield. This is the second time in five years that a safe harbour programme between the European Union and United States has been found inadequate by the CJEU.

For transfers that do not fall within the scope of an existing adequacy decision, 'appropriate safeguards' must be established. While the GDPR lists several kinds of appropriate safeguards, one of the most common is the SCCs. SCCs are template clauses that are preapproved by the Commission which companies can use in their contracts to ensure sufficient data protection and GDPR compliance.

Other compliance obligations

The GDPR's requirements are numerous and multifaceted. Companies beginning to work toward compliance should seek the advice of counsel. For additional information on the specific compliance and documentation requirements contained in the GDPR, please reference the table below.

Requirement/definition	Reference
Lawful bases for processing	Article 6
Access	Article 15
Disclosure of purpose of collection, source, use and third-party sharing	Articles 13, 14, 15
Erasure (deletion)	Article 17
Portability	Article 20
Opt out/object	Article 21(2)–(3) (for direct marketing purposes)
Data protection agreements	Article 28
Data protection impact assessments	Article 35
Personal data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier.
Data subject	A natural person whose personal data is processed by a controller or processor.

Jurisdictional differences in privacy regimes

Data protection regimes can vary dramatically from nation to nation, and even from state to state within the United States. What qualifies as sensitive personal information in one nation, requiring more stringent consent and processing

requirements, may receive less protection in another nation. Some nations require specific data protection programme elements that can be more onerous on a company, such as the GDPR's 'privacy by design' control environment requirements, registration of processing databases with national supervisory authorities, or the appointment of a specific data protection officer to oversee privacy issues.

Companies may find it beneficial to target investment in or shift operations to jurisdictions with fewer data protection requirements. Depending on the type of data on which the company relies, and its degree of global integration, there are significant potential compliance cost savings even among countries in Latin America that have recently heightened their data oversight. But in an increasingly global economy that relies on cross-border marketing, internet traffic and business partners, those benefits may be limited. Before starting to forum shop, companies must consider not only where their data will be stored or processed, but from whom the data will be collected and where it will be transferred. Data privacy laws often reach beyond national borders when their residents' data is at issue.

For example, if a company collects personal information from citizens and residents in the European Union, even if it hosts its website or processes the data in Panama, the data is still subject to the GDPR requirements. Segregating data into separate databases with more stringent protections based on the country of origin is possible, but requires additional administrative overhead. If a company intends to establish operations in Brazil or Ecuador that would rely on international data transfers from other countries, it will be required (either by contract or law) to follow the data protection rules of the origin country. And some countries prohibit the transfer of data internationally unless the destination country has data protection laws that are at least as robust as their own. As discussed in the previous section, the EU's GDPR mandates strict international transfer standards. The privacy regimes of Argentina, Brazil and Colombia also incorporate this type of comparative protection. So by setting up shop in a jurisdiction with few data protection laws, a company may restrict the ability to efficiently interact with companies or even internal divisions of the same company in other parts of the world.

Even if a company's aim is not to engage in regulatory arbitrage, but more simply to evaluate opportunities for international expansion, it is critical to understand the differences in data protection laws among neighbouring countries. These differences may require significant modifications to data processing policies, procedures and security that could result in major capital expenses for the company, or even subject it to liability for noncompliance. Below are some examples of factors that are treated differently under the laws of various jurisdictions discussed elsewhere in this chapter.

Definition of sensitive personal information

Most privacy regimes recognise that certain types of personal information are more intimate or sensitive, requiring enhanced protection or consent procedures when companies collect and use the data. This usually does not include directory-type information (names, addresses, phone numbers, emails) or transactional data (purchase history, etc.), which would qualify as personally identifiable information subject to some protections, but not sensitive information requiring enhanced protection.

In many Latin American countries, enhanced protections are provided for information more intimately linked to an individual's personal, physical or moral characteristics, such as: racial and ethnic origin; religious, political or philosophical beliefs and affiliations; membership in labour unions; and information related to an individual's health and sex life. Many jurisdictions, including Colombia, Costa Rica, Mexico, Brazil, the European Union and some US states offer enhanced protections for biometric data (fingerprints, retina scans, facial recognition, etc.). Genetic information is also afforded specific protections in Costa Rica, the United States, Mexico, Brazil and EU Member States. Notably, though, Argentina and Chile do not require special treatment of these categories.

Mexico's data privacy regime includes a more expansive definition of sensitive personal information than many other jurisdictions, specifically covering pictures, videos, geolocation and the data subject's signature. It is also one of the few regimes in the region to include banking information as a sensitive category. The United States also requires additional safeguards when dealing with data provided to financial institutions or credit agencies.

Consent-conscious jurisdictions

The definition of sensitive information is commonly accompanied by restrictions on use that are predicated on specific notice to or consent from the data subject. Informed consent is often required before processing sensitive data, and almost always before selling or disclosing that information to any third parties. In some jurisdictions, though, consent is required before a company can collect or process even non-sensitive personal information. A company that has built its data protection policies on the rules of one nation may open itself up to liability by applying those policies in a jurisdiction that demands a greater degree of control for data subjects.

For example, Costa Rica's Law on the Protection of Persons Regarding the Processing of their Personal Data makes it mandatory to obtain informed and express consent from data subjects to process any personal data. That consent must

specify (among other things) the purpose for collecting the data, how the data will be processed, and all recipients and parties with access to the data. Additional consents are required before a company can transfer that data to a third party.

Similarly, Argentina's Personal Data Protection Act states that data processing is only legal with prior, express and informed consent of the data subject. But a number of exceptions apply that broadly carve out categories of personal information companies typically collect. No consent is required to process directory-type information, including name, address, date of birth or even taxpayer identification numbers. Nor is consent required when the data arises from a contractual or professional relationship with a data subject. Use of data for marketing, provision of credit services, or by third-party service providers, is also allowed without consent (though is limited by other rules). Sensitive data, however, may only be collected and processed where necessary and with consent.

Mexico requires some level of consent for all processing of personal data, but allows implicit consent (where the data subject is given notice of the use and an opportunity to opt-out) for processing personal information, generally. Heightened thresholds for consent are required for processing more sensitive data. Express consent (opt-in) is required to process financial or asset data, and express written consent is necessary to process sensitive personal information.

Again, segregating data by degree of sensitivity and place of origin is possible. It is even recommended in some circumstances – for example, more sensitive data may be protected with additional encryptions or be subject to access restrictions to reduce the potential harm of a data breach. But it may be particularly onerous to maintain different standards and protocols for different employees, customers, and business partners in different locations. And if a company's use of the data (analytics, marketing, etc.) would be diminished by segregating along jurisdictional lines, the value in collecting the data in the first place could be reduced.

Breach notification requirements

Possibly the most notorious and feared event in the world of data processing is the breach. Whether the result of hacking, phishing, insider misappropriation, or stolen device, a data breach that compromises the security of a data subject's information (sensitive or otherwise) can cause substantial harm to a company's customers. For that reason, many jurisdictions require that breaches be disclosed to data subjects, government authorities, and sometimes even the media. And while some of the world's largest companies have publicly fallen victim to significant data breaches (Yahoo, Uber, eBay, LinkedIn, Marriott, Adobe), breach notification rules can still subject a company to substantial reputational harm and business disruptions.

While there are currently no breach notification requirements in Chile or Argentina, other Latin American countries require strict and robust disclosures:

- Colombia's Statutory Law 1581[17] requires both a data controller (the entity that collects and directs use of the data) and the data processor (the entity that carries out the processing instructions) to notify the Superintendent of Industry and Commerce of a security breach, or even a known risk of a breach, within 15 days;
- Costa Rica's Executive Decree No. 37554-JP[18] requires notification to data subjects and to the national data protection authority (PRODHAB) within five business days. Companies must also complete a thorough review of the breach and its impact during that short time period, and incorporate details of the breach and remediations in their notification; and
- Mexico and Brazil require breach notifications, but only under certain circumstances where the breach is likely to materially affect the property or moral rights of the data subject (Mexico) or likely to result in a risk of harm to the data subjects (Brazil).

It is critical to remember that data protection laws are often drafted to protect the residents of that jurisdiction, wherever their data is processed. A breach that results in the disclosure of unencrypted personal information of Californians or Belgians will require notification pursuant to those jurisdictions' privacy rules, even if the hacked server was located in Chile, for example. The common rule for evaluating any jurisdictional nuance will always be to understand the source and use of the data at issue.

Registration requirements

One consideration that is perhaps more straightforward is whether the jurisdiction in which the company plans to process data requires registration of data processing activities with the national authority. This type of registration is not required in most US states (with some specific exceptions for data brokers and telemarketers). But it is required in numerous Latin American jurisdictions and can be a significant administrative burden. For example, Costa Rica's Law on the Protection of Persons Regarding the Processing of their Personal Data No. 8968,[19]

17 Sections 17 and 18.

18 Articles 38 and 39.

19 Article 21, with definition guidance from Article 2(j) of Executive Decree No. 37554-JP, and Article 1(j) of Decree No. 40008-JP.

requires any entity that manages a database containing personal information, and that distributes, discloses or commercialises such personal information in any manner, to register with PRODHAB. Some exceptions and exemptions exist, including for entities that manage databases for entirely internal purposes and for financial institutions governed by other specific bank secrecy regulations. But for those entities that must register, a substantial submission is required, including details about the data owner, an appointed employee responsible for the databases, a list of all processors and transfer recipients, the type of data to be stored, the purposes and foreseen uses, collection procedures, technical safeguards and risk assessments, and a certified copy of minimum security protocols that details all processes followed by the company to manage the data.

Similarly, Colombia's Statutory Law 1581, in addition to the breach notification rules described above, created the National Register of Data Bases and requires mandatory registration of databases that store and process personal data by any data controller entities that have total assets above 100,000 tax value units (approximately 3.63 billion Colombian pesos or US$1.07 million). And Argentina's Data Protection Authority (AAIP) maintains a National Registry of Personal Databases.[20] To be deemed a lawful database, all archives, registries, databases and data banks – whether public or private – must be registered. The registration does not require disclosure of the contents of the database, but rather a more general description of the database, its creation, maintenance and details of compliance with various aspects of Argentina's data protection laws. There are no registration requirements in Brazil or Mexico, and only public databases must be registered with Chile's Civil Registry and Identification Service.

In sum, substantial differences exist in the substantive and administrative application of data protection laws from nation to nation. Depending on how a company's current data compliance programme is constructed, those differences can present either an opportunity or a potential liability pitfall when considering entering a new market. And operating within a global economy will often require attention to multiple regimes at once. There is no secret safe harbour where companies can seek shelter from oversight. There is also no easy one-size-fits-all global compliance solution, and the rate of legislative change occurring in Latin America over the last several years is evidence that companies will need to continue to stay abreast of the applicable privacy rules and to adapt accordingly.

20 Sections 3 and 21 of the Personal Data Protection Act.

Data compliance programmes

While developing a programme that addresses the significant requirements governing the use, collection and treatment of individuals' personal information in our increasingly globalised world may appear to be a substantial challenge, resources exist to help meet the challenge and to avoid the liabilities that derive from failing to mitigate these risks. When embarking on developing or updating a data compliance programme, companies can be guided by the fair information practice principles (FIPPs), which underpin all data privacy laws. Those principles include awareness, consent, participation, security and enforcement. The key questions when developing or updating such a programme, as outlined above, can generally be traced back to these FIPPs, including the initial requirement of data mapping and inventory, asking what data is held, how it is used and what the lawful bases are for processing it exist; determining what data subject rights pertain to the data; and assessing whether prohibitions on special categories of data apply. Appointing a DPO who is responsible for these questions and staying abreast of the applicable regulations is crucial to the success of the programme. Moreover, having a well designed data compliance programme in place, implemented, tested and continuously updated, will not only help prevent violations of data privacy laws, including serious data security breaches, it will also help the company defend itself from potential lawsuits and regulatory investigations should incidents occur.

APPENDIX 1

About the Authors

Devika Kornbacher

Vinson & Elkins LLP

Devika Kornbacher is a partner at Vinson & Elkins LLP's Houston office. She is an intellectual property and technology lawyer who leverages her extensive technology knowledge and experience to assist clients in such fields as energy, sports, aviation, software and hardware. Devika has been designated a Certified Information Privacy Professional (CIPP/US) by the International Association of Privacy Professionals (IAPP)

Devika advises on obtaining, protecting, licensing and enforcing intellectual property rights, as well as on other technology-related legal matters that might arise in all aspects of her clients' business.

She is experienced in handling a wide array of transactions, including commercialisation agreements, licence agreements, reseller agreements, collaboration agreements, joint ventures, software development agreements and patent clearances. In addition, she counsels clients on digital media, open source software, cybersecurity and other technology-related issues.

Palmina M Fava

Vinson & Elkins LLP

Palmina M Fava is a partner at Vinson & Elkins LLP's New York office, who has over 20 years of experience. She represents clients in internal and government investigations, litigation, and corporate governance counselling, with a principal focus on matters involving the Foreign Corrupt Practices Act (FCPA), international anti-corruption, anti-money laundering and anti-bribery laws, accounting irregularities, bid rigging and unfair trade practices, off-label pharmaceutical marketing, misappropriation of trade secrets, fraud, cybersecurity and data privacy.

Palmina regularly represents companies in matters before the United States Department of Justice, the Securities and Exchange Commission, other federal and state agencies, and international regulatory bodies. She leads teams in investigations in Latin America, throughout Western and Eastern Europe, Asia, Africa, and the Middle East. Relying on her extensive language skills, she is capable of assisting clients in Spanish, Portuguese, Italian and English.

She also designs and implements comprehensive, practical and user-friendly corporate compliance programmes tailored to a client's particular risks and growth strategies. She provides employee and third-party training; conducts proactive reviews of a client's high-risk business areas; structures commercial arrangements to protect against compliance risks; and handles due diligence of agents, joint venture partners, and targets in mergers and acquisitions or other investment transactions.

Palmina's litigation practice focuses on commercial, business tort, and intellectual property disputes. She has served as lead litigation and trial counsel in matters involving breaches of fiduciary duty, breaches of contract, fraud, negligence, misappropriation of trade secrets and insurance coverage. She has tried and defended cases in federal and state courts, and before arbitration panels, and represented clients in appellate arguments, mediations and negotiations.

Jessica Heim

Vinson & Elkins LLP

Jessica Heim is a partner in Vinson & Elkins LLP's government investigations and white-collar criminal defence group based in San Francisco. She has been designated as a Certified Information Privacy Professional (CIPP/US) by the International Association of Privacy Professionals (IAPP). Her practice involves helping clients – specifically companies, their audit committees or individual executives – respond to issues that arise through whistle-blower hotlines or government inquiries of every sort. She also assists clients with proactive compliance measures, finding creative ways to develop and implement formal compliance programmes and processes and defending those programmes to regulators.

Gabriel Silva

Vinson & Elkins LLP

Gabriel Silva is a partner at Vinson & Elkins LLP's New York office. Gabriel's principal area of practice is corporate finance. He works with a variety of public and private companies as well as private equity investors and their portfolio companies in connection with mergers, acquisitions, dispositions and securities offerings. His practice has a global reach, spanning Latin America, the United

States, Europe, and Asia, and involves extensive experience advising a multinational client base of leading corporations and financial sponsors on complex, cross-border transactions. In particular, Gabriel has significant experience in transactions in the digital infrastructure sector, such as telecoms towers, data centres and fiber.

Vinson & Elkins, LLP
1114 Avenue of the Americas
32nd Floor
New York, New York 10036
United States
Tel: +1 212 237 0000
pfava@velaw.com
zterwilliger@velaw.com
michaelward@velaw.com
josesanchez@velaw.com
jheim@velaw.com
dkornbacher@velaw.com
gsilva@velaw.com
ncardenas@velaw.com
www.velaw.com

Published by Latin Lawyer and LACCA, edited by Andrew M Levine, a litigation partner at Debevoise & Plimpton LLP, Reynaldo Manzanarez Radilla, a corporate attorney and compliance professional, Valeria Plastino, vice president, general counsel and regional compliance officer at Lumen Technologies, and Fabio Selhorst, general counsel, chief integrity officer and chief communications officer at Hapvida, *The Guide to Corporate Compliance* is designed to assist key corporate decision-makers and their advisers in the effective handling of their compliance obligations in Latin America.

This guide delivers specialist insight to our readers – general counsel, compliance officers, government agencies and private practitioners –who must navigate the region's complex, fast-changing framework of rules and regulations.

In preparing this guide, we have been working with practitioners from a variety of disciplines and geographies, who have contributed a wealth of knowledge and experience. We are grateful for their cooperation and insight.

Visit latinlawyer.com
Follow @LatinLawyer on Twitter
Find us on LinkedIn

ISBN 978-1-83862-750-8