ISSN 1680-8754

SERIES

PRODUCTION DEVELOPMENT 223

Corporate governance and data protection in Latin America and the Caribbean

Héctor J. Lehuedé

UNITED NATIONS
ECLAC
70 ECLAC FOR SUSTAINABLE DEVELOPMENT WITH EQUALITY

SERIES

PRODUCTION DEVELOPMENT	223

Corporate governance and data protection in Latin America and the Caribbean

Héctor J. Lehuedé

UNITED NATIONS

ECLAC

This document has been prepared by Héctor J. Lehuedé, Consultant at the Division of Production, Productivity and Management of the Economic Commission for Latin America and the Caribbean (ECLAC).

The author would like to convey thanks for their collaboration to Valeria Jordan, Nunzia Saporito, Georgina Nuñez (coordinator), Wilson Peres, Edwin Rojas and David Delmoral of ECLAC; Alissa Amico of the European consultancy Govern; Mona Chammas, of the European law firm Govern&Law; Erick Iriarte, of the Peruvian law firm Iriarte & Asociados; Claudio Magliona of the Chilean law firm Magliona Abogados; Nuria Lopez Cabaleiro Suarez, Camila Rioja and Renato Opice Blum of the Brazilian law firm Opice Blum; Daniella Correa, Javier Moya and Daniel Peña Valenzuela of the Colombian law firm Peña Mancero Abogados; Claudia Fonseca Martinez of the Federal Telecommunications Commission of Mexico; María José Viega Rodríguez of the Uruguayan law firm Viega & Asociados; and Ximena Cisternas and Gonzalo Smith of Falabella S.A.

United Nations publication
ISSN: 1680-8754 (electronic version)
ISSN: 1020-5179 (print version)
LC/TS.2019/38
Distribution: L

Printed at United Nations, Santiago
S.19-00395

This publication should be cited as: H. Lehuedé, "Corporate governance and data protection in Latin America and the Caribbean", *Production Development series*, No. 223 (LC/TS.2019/38), Santiago, Economic Commission for Latin America and the Caribbean (ECLAC), 2019.

Contents

Abstract 5

Introduction 7

I. International Data Protection Frameworks 11
A. The EU Framework: the GDPR 12
1. Main aspects 12
2. Accountability and governance 14
B. The U.S. Framework 15
C. Other 16
1. The OECD Privacy Guidelines 16
2. The APEC Privacy Framework 17

II. Corporate governance implications 19
A. Companies at the center of regulations 19
B. The responsibility of the board 20
1. Information 22
2. Protection 23
3. Reporting 24
4. Supervision 25
C. Board skills and committees 26
1. Board composition 26
2. Specialized committees 27
D. The role of regulation 28

III. Data protection in the region 31
A. Overview 31

1. Ibero-American Data Protection Network Standards....34
2. Economic Commission for Latin America and the Caribbean's eLAC....34
B. Regional legal and regulatory framework....35
1. Argentina....35
2. Brazil....37
3. Chile....39
4. Colombia....41
5. Mexico....43
6. Peru....45
7. Uruguay....47
IV. Comparison and analysis....49
A. Corporate governance aspects....51
1. DPOs....51
2. DPIAs....53
3. Accountability....54
B. Cross border data transfer....55
C. Summary and conclusions....57
Bibliography....59
Production Development Series: issues published....63

Tables

Table 1 Selection of data protection measures of national frameworks....50
Table 2 Selection of data protection measures related to corporate governance....51
Table 3 Authorization for international transfers of personal data....56

Abstract

This paper describes and discusses the relation between cybersecurity and corporate governance with a special interest on data protection in Latin America and the Caribbean. The motivation for the work resides in the growing role that data protection and privacy laws and regulations in developed countries reserve for corporate governance. These laws increasingly assign responsibilities to boards of directors and management with the expectation to incentivize firms to take data protection seriously in the face of cybersecurity and privacy risks. The paper presents these new rules and explores their current and potential use in the region, focusing on the rules and practices on data protection by Argentina, Brazil, Chile, Colombia, Mexico, Peru, and Uruguay. The paper was commissioned by the United Nations' Economic Commission for Latin America and the Caribbean, ECLAC.

Introduction

> "I believe the future of communication will increasingly shift to private, encrypted services where people can be confident what they say to each other stays secure and their messages and content won't stick around forever. This is the future I hope we will help bring about."

This excerpt comes from a letter addressed in March of 2019 by Mark Zuckerberg, the founder and CEO of Facebook, to users or the platform.[1] These words provide an important reminder that privacy and data protection have become increasingly important concerns globally. Such a statement might have never been made just a couple of years ago by the CEO of a company whose business model is premised on offering free connectivity in exchange of the ability to share their user's data with advertisers.

The last decade has witnessed a fast pace of technological disruption, prompting firms to move towards digital business models that find new ways to generate value from access to large repositories of customers' data. Digital flows are now soaring in a world that is more interconnected than ever. While flows of finance and trade slowed down after the financial crisis, cross-border flows of data keep increasing at extraordinary rates. And they are expected to continue to grow along with rising e-commerce, online searches, video streaming and the like.[2] These digital flows are changing the economics of global trade by bringing down transaction costs and offering companies

---

1 In the blog post, Zuckerberg says that people "want to know their data is stored securely in places they trust. Looking at the future of the internet and privacy, I believe one of the most important decisions we'll make is where we'll build data centers and store people's sensitive data." He also states that people "expect their private communications to be secure and to only be seen by the people they've sent them to -- not hackers, criminals, over-reaching governments, or even the people operating the services they're using." Zuckerberg, Mark, A Privacy-Focused Vision for Social Networking, Facebook Blog, March 6, 2019, available at: https://m.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/.

2 See McKinsey Global Institute (2016), Digital Globalization: The New Era of Global Flows, March 2016, available at: http://ma.mckinsey.com/practicecrm/MGI/MGI_Digital_globalization_Full_report_March_2016.pdf.

the opportunity to scale up, creating global markets that even small companies can tap into through digital platforms such as eBay, Amazon or Alibaba.

Behind this digital growth there is a wealth of data that ranges from purely commercial information, such as the number of sales of a given product on a given market at a certain point in time, to extremely personal information. Consumers, users, clients, employees and many more agree, more or less aware of the consequences of their acts, to share their personal data with counterparts as part of contracts and in exchange for goods and services. Not long ago, this information was of little or no value to most parties. That is no longer the case.

In our modern economy data are an asset that more and more companies are mining in ways that improve their ability to conduct business, allows them to predict trends and adapt quickly, better understand the markets, and often also enhance their customers' experience. As any valuable asset, companies are facing the challenge of protecting data from theft and misuse in the face of sprawling cybersecurity[3] risks.

In its 2017 Global Risk report, the World Economic Forum argues that "greater interdependence among different infrastructure networks is increasing the scope for systemic failures —whether from cyber-attacks, software glitches, natural disasters or other causes— to cascade across networks and affect society in unanticipated ways."[4] Indeed, numerous breaches of cybersecurity and customer data protection[5] in recent years have put privacy in jeopardy and made e-commerce vulnerable to theft and fraud. Some of the high-profile cases of personal data breaches involve billions of users and have caused massive damage, both for the organizations that failed to protect the data as well as to their customers, whose information became available for misuse. Some of them are:

- Yahoo. In September of 2016 and while involved in an M&A process, internet giant Yahoo disclosed it had been hacked two years earlier, in what at the time was the biggest data breach in history. The attacker obtained the names, email addresses, birth dates and telephone numbers of 500 million Yahoo users.[6] Three months later, the company admitted that in 2013 the company had already been hacked by a different

---

[3] Cybersecurity for this report is understood as "the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation." This includes strategy, policy, and standards regarding the security of and operations in cyberspace, and encompassing the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. For this and other useful definitions, see the U.S. National Initiative for Cybersecurity Careers and Studies (NICCS) Portal's cybersecurity lexicon: https://niccs.us-cert.gov/about-niccs/glossary#C.

[4] See: World Economic Forum (2017), Global Risks Report 2017, 12th Ed., January 2017, available at: www.weforum.org /reports/the-global-risks-report-2017.

[5] Cybersecurity breaches or incidents for this report are understood as "an occurrence that actually or potentially results in adverse consequences to (adverse effects on) (poses a threat to) an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences." This includes an occurrence that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. For this and other useful definitions, see NICCS's glossary, available at: https://niccs.us-cert.gov/about-niccs/glossary#I.

[6] See *Yahoo execs botched its response to 2014 breach, investigation finds*, by Michael Kan, IDG News Service, March 2, 2017, available at: www.csoonline.com/article/3176181/security/yahoo-execs-botched-its-response-to-2014-breach-investigation-finds.html.

group who had obtained the personal data of 1 billion Yahoo accounts, including this time their passwords, security questions and answers. In October of 2017, Yahoo revised its original disclosure, increasing the number of users affected to 3 billion overall.[7] The impact of these breaches is estimated to have reduced the value of the company by $350 million USD.

- Facebook. In 2014, the U.K. affiliate of U.S. political consulting firm Cambridge Analytica, hired a researcher to gather personal data of U.S. Facebook users. Using a software application he created, the researcher delivered data of all users that adopted the application as well as from all their Facebook friends, if their privacy settings allowed it. Facebook estimates this involved the information 87 million users, whose information was then used to promote political campaigns via targeted and tailored messages exploiting their information and "likes".[8]
- Equifax. The credit bureau disclosed in September of 2017 that a data breach exposed the personal data and credit information of 147.9 million customers, including their U.S. social security numbers, birth dates, addresses, and in some cases drivers' license numbers.[9]
- Uber. The ride-hailing company disclosed, in November of 2017, that one year earlier it had learned that the personal information of 57 million users and 600 thousand of its drivers had been hacked from its systems.[10] The company experienced severe criticism not only for taking one year to make this disclosure, but also because it paid hackers to delete and never made the information public, apparently without any means of verification.[11] It is estimated that the breach was one of the elements that reduced the valuation of the company by billions of USD, in a financing deal with SoftBank that was taking place at the time.[12]
- Marriott. In November 2018, the hotel chain disclosed a breach of personal data of approximately 500 million customers that started in 2014 within the systems of Starwood hotels, which Marriott acquired in 2016. The attackers remained in the system after the deal closed and were not discovered until September 2018, being able to steal names, contact information and passport numbers. For what the hotel chain estimates by more

---

7 See *Yahoo says all three billion accounts hacked in 2013 data theft*, by Jonathan Stempel & Jim Finkle, Reuters Business News, October 3, 2017, available at: www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1.

8 Even if data privacy issues with Facebook can be tracked back to 2010, with the introduction of certain apps that would covertly export users' data beyond the company's platform, the Cambridge Analytica scandal created a tipping point that moved legislators, regulators and the company itself into action about privacy. See *Understanding the Facebook-Cambridge Analytica Story: QuickTake* by By Michael Riley, Sarah Frier and Stephanie Baker, The Washington Post, April 11, 2018, available at: www.washingtonpost.com/business/understanding-the-facebook-cambridge-analytica-story-quicktake/2018/04/11/071f8c84-3d97-11e8-955b-7d2e19b79966_story.html.

9 See *Equifax says website vulnerability exposed 143 million US consumers*, by Steve Ragan, CSO Online, September 7, 2017, available at: www.csoonline.com/article/3223229/security/equifax-says-website-vulnerability-exposed-143-million-us-consumers.html.

10 See *Did Uber throw its CSO under the bus?*, by Steve Morgan, Cybersecurity Business Report, CSO Online, November 28, 2017, available at: www.csoonline.com/article/3238708/regulation/did-uber-throw-its-cso-under-the-bus.html.

11 See *Uber Paid Hackers to Delete Stolen Data on 57 Million People*, by Eric Newcomer, Bloomberg, November 21, 2017, available at: www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data.

12 See *Uber's Rough Year Ends With Big SoftBank Investment*, by Chris Nolter, The Street, December 29, 2017, available at: www.thestreet.com/story/14431727/1/uber-s-rough-road-leads-to-softbank-deal.html.

than 100 million customers, the breach also included their credit card numbers and expiration dates.

These cybersecurity risks have put in jeopardy not only the security of corporate property, reputation and valuation of the concerned companies, but also the privacy and personal data of their customers. As a result, public scrutiny and enforcement activity over the behavior corporations with access to massive amounts of personal data has substantially increased. These customers, employees and other users have surrendered information that is not publicly available under the assumption that their counterpart would fulfill a responsibility of custody, and that their data would not be misused. These two risks help distinguish between privacy and data protection, which are not the same.

On the one hand, privacy is the right people have that their private and family life, home and correspondence will remain private and others will respect that they are off limits, except when laws or contracts says otherwise. Broadly speaking, this includes a range of different aspects of privacy, from defamation issues to the right of people to stop companies from using their image without their permission or preventing them to spam their email account with publicity. On the other hand, data protection refers to the practices and systems of data storage and processing of personally identifiable or identifying data for the protection of privacy. Thus, while data protection is concerned about securing data against unauthorized access, privacy is concerned with who has and grants access to that data, considering who has rights over them, and what for.[13]

Cases like those described above have prompted regulators and legislators all over the globe to action. They have passed or are considering rules or laws to establish data protection frameworks that can allow the digitalization of the economy to move forward without a sea of privacy casualties in its path. As one columnist put it, these regulations "attempt to make sense of newly complex and decentralized relationships among individuals, their data, the state and the private sector that have emerged under globalization."[14]

Among those new rules, legislators and regulators have reserved a role for the corporate governance frameworks of firms, assigning increasingly new responsibilities to boards of directors and top managers. Their expectation is that rules targeting firms' leaders may provide sufficient incentives for them to take data protection seriously in the face of cybersecurity and data misuse risks.

This publication seeks to describe and discuss the relation between cybersecurity, focusing on data protection, and corporate governance with a special interest in the situation in Latin America and the Caribbean. It is structured in five chapters. To provide further context, the next chapter briefly describes some of the international frameworks for data protection that serve as a reference globally. Chapter II outlines the conceptual rationale for why some of those frameworks are targeting corporate governance as a means to boost data protection, and some of the challenges this faces. Chapter III introduces the discussion of data protection in Latin America and the Caribbean, describing a selection of national frameworks. Finally, Chapter IV offers a comparative analysis of the findings and some conclusions.

---

[13] Different jurisdictions use these two concepts with sometimes diverse meaning, but it is important to note the differences as having data protection does not ensure privacy, while ensuring privacy requires data protection as a prerequisite. For more on this see *Privacy vs. Data Protection vs. Information Security*, by Danny Guamán, at Software and Services Engenieering Blog, November 1, 2016, available at: http://blogs.upm.es/sse/2016/11/01/privacy-vs-data-protection-vs-information-security/.

[14] See *Data Subjects of the World, Unite!*, by Atossa Araxia Abrahamian, The New York Times, May 28, 2018, available at: www.nytimes.com/2018/05/28/opinion/gdpr-eu-digital-privacy-law-data-subject-europe.html.

I. International Data Protection Frameworks

Around the world, different frameworks have been developed to address data protection and privacy. Those models respond to citizens' expectations, democracy's mandates and ultimately to policy choices that are shaped by prevailing societal values on the relation between businesses and individuals. As a result, they put slightly more or less emphasis on privacy and a corresponding limitation on businesses' behavior. The diverging views on some of these issues are visible in the actions that the European Commission and some European countries have initiated against some of the large U.S.-based tech giants, on issues of privacy that are not a problem within their domestic jurisdiction.[15]

These models often have a multilateral approach or have important extraterritorial impact, and can carry large influence beyond their borders, particularly if they originate in powerful economies. Some of those frameworks are described briefly in this chapter to inform the discussion in the rest of the document, that will focus on the Latin American and Caribbean region. Where relevant, the corporate governance-related components of the frameworks have been highlighted.

[15] For example, in January of 2019, France's data protection authority, the CNIL, punished Google with a €50 million (57 million USD) fine for its failure to comply with European Union's General Data Protection Regulation. See *France fines Google $57 million for European privacy rule breach* by Mathieu Rosemain, Reuters, January 21, 2019, available at: www.reuters.com/article/us-google-privacy-france/france-fines-google-57-million-for-european-privacy-rule-breach-idUSKCN1PF208.

A. The EU Framework: the GDPR

In April of 2016, after 10 years of negotiations, the European Union repealed its existing data protection rules, contained in Directive 95/46/EC,[16] and replaced them with Directive (EU) 2016/680[17] and Regulation (EU) 2016/679[18] of the European Parliament and of the Council, the General Data Protection Regulation (the GDPR).[19] Generally regarded as the most advanced data protection framework in place, the GDPR has international reach and covers any organization that collects, controls, processes or uses data of any EU citizen, no matter where located.

1. Main aspects

Aimed to harmonize data protection laws across Europe as well as to give greater protection and rights to individuals, the new legislation entered into force on 25 May 2018, after a two-year preparation period created to make adaptation to changes easier. The new rules affect individuals, companies and other organizations that are regarded to be either data controllers (those that determine how data are processed) and data processors (their subcontractors) of personal data and sensitive personal data of EU citizens. Article 4 of the GDPR offers some of the key definitions:

- Personal Data: any information relating to an identified or identifiable natural person (Data Subject);
- Data Subject: an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- Controller: a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal

---

[16] See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679.

[17] See Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC.

[18] See Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[19] For clarification, a regulation under the EU's framework is a binding legislative act that must be applied in its entirety across member countries, while a directive is a legislative act that sets out a goal that all EU countries must achieve via domestic implementation of local rules. The previous data protection framework of the EU was a directive, nw it has been reinforced as a regulation.

data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

- Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- Consent: of the Data Subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Among the 99 articles of the GDPR, the EU set out the rights of individuals and the obligations placed on organizations dealing with their personal data. Individuals are recognized eights fundamental rights:

- Right to access (article 15): allows data subjects to obtain confirmation from a data controller as to whether or not personal data concerning them are being processed, where and for what purpose. Upon request, data controllers must provide a copy of the personal data, free of charge, in an electronic format.
- Right to rectification (article 16): is the right for data subjects to have their inaccurate personal data rectified or completed if incomplete.
- Right to erasure (article 17): also known as the right to be forgotten, gives data subjects the right to force a data controller to erase their personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. There are conditions for exercise of this right, including the data no longer being relevant for its original purpose, or when consent of the data subject has been withdrawn.
- Right to restriction (article 18): is the right of data subjects to request the restriction or suppression of personal data from processing (data are not destroyed but cannot be used).
- Right of notification (article 19): data subjects have the right to be notified of a data breach that is likely to "result in a risk for the rights and freedoms of individuals". The data controller must do this within 72 hours of first having become aware of the breach. Data processors are required to notify data controllers, in turn.
- Right of portability (article 20): is the right of data subjects to receive the personal data concerning them from data controllers in a 'commonly use and machine-readable format' and have them transmitted to another data controller.
- Right to object (article 21): is the right for data subjects to object to the processing of their personal data in certain circumstances, including for direct marketing.
- Right against automated profiling (article 22): the GDPR has rules for automated aspects of processing data and for profiling (automated evaluation of data to classify individuals) for automated decision-making process. This right allows data subjects to ask to be excluded from such processes.

The extraterritorial jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the EU, regardless of their location, is one of the most

salient features of the regime and one that has had effects all over the globe. Pursuant to the regulation, non-EU businesses processing data of EU citizens have to appoint a representative in the EU and are subject to the reinforced penalty systems it created. Breaches of the GDPR can be fined up to the greater of 4% of the annual global turnover of the organization or €20 million, for the most serious infringements. Lower level offenses can result in fines of 2% of the annual global turnover of the organization.

Under the GDPR the destruction, loss, alteration, unauthorized disclosure of, or access to personal data has to be reported to the relevant data protection authorities (DPAs) within 72 hours. These are the authorities of all jurisdictions where data subjects may experience financial loss, confidentiality breaches as well as damage to their reputation as a consequence of the breach.

The GDPR restricts the transfer of personal data to jurisdictions outside the European Economic Area, which includes the EU member states and the European Free Trade Association states, which are Switzerland, Iceland, Norway and Liechtenstein. Any transfer of personal data to a third country, or to an international organization, shall take place only if both controllers and processors comply with the requirements of the GDPR. The European Commission has to decide if those third countries (a territory or one or more specified sectors within each country) or international organizations ensure an adequate level of protection.

2. Accountability and governance

From a corporate governance perspective, data controllers and data processors are also subject to new accountability and compliance obligations. They aim to make their handling of people's personal data more responsible, including the adoption of data protection policies, the use of data protection impact assessments (DPIAs), and the appointment of data protection officers (DPOs), among others.

The GDPR sets out that data controllers must "implement appropriate technical and organizational measures" to protect personal data in a way that ensures "the ongoing confidentiality, integrity, availability and resilience of systems." This creates an expectation that board of directors and senior managers will have to get personally involved in the design, implementation and monitoring of their organizations data protection and information security frameworks.

Among other highlights, the GDPR introduces into the legal framework the concept of "privacy by design", which calls for the inclusion of data protection considerations from the early stages of building data processing systems. Article 23 calls for data controllers to hold and process only the data absolutely necessary for the completion of their duties. Companies with more than 250 employees are also required to map and document the justification for storing and processing personal data, including how long it's being kept in the databases.

Furthermore, companies that have "regular and systematic monitoring" of individuals at a large scale or process significant amounts of sensitive personal data, have to employ a data protection officer (DPO). The DPO position has to be independent and must report directly to the highest level of management about compliance with the GDPR, it is also a point of contact for employees and customers.

B. The U.S. Framework

The United States has enacted numerous rules and legislation at the state and federal levels addressing data privacy and security. Unlike the EU, the U.S. has different regimes dealing with specific subjects and areas of risk, and often has both state and federal rules applying simultaneously.[20] Some of the relevant laws include:

- The Federal Information Security Management Act (FISMA), a federal law part of the larger E-Government Act of 2002, that mandated federal agencies to develop, document, and implement an information security and protection program;
- The Health Insurance Portability and Accountability Act (HIPAA), a set of standards created to force healthcare providers to secure protected health information, and
- The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Modernization Act of 1999, that seeks to protect the personal information of consumers stored in financial institutions.

Some states within the U.S. have adopted frameworks that resemble to certain degree the European standard, most notably California, which has requirements for the notification of security breaches since 2002 and that has recently updated its rules, but in many other states the data protection frameworks set a significantly lower benchmark, setting an uneven playing field.

Since 1 August 2016, companies in the U.S. can join the EU-U.S. Privacy Shield Program,[21] operated by the Department of Commerce, to facilitate U.S. firms' compliance with data protection requirements in Europe. Companies part of the program are eligible for international transfers of data covered by the GDPR, as the EU decided that the U.S. ensures an adequate level of protection for personal data under the EU-U.S. Privacy Shield. U.S. companies can certify online to the Commerce Department that they comply with the Privacy Shield principles after conducting a self-assessment. The authority reviews the applicants' submission information and privacy policy and can also request information regarding onward transfer agreements.

Like in the case of the GDPR, some of the rules within the U.S. framework apply extraterritorially to entities that handle personal data from U.S. individuals outside the United States. The Federal Trade Commission[22] and State attorney generals enforce these rules from the public side, with powers to act against failures to implement reasonable data security measures, compliance with privacy policies as well as in the event of unauthorized disclosures of personal information. Complementing the public enforcement, there is a dynamic private enforcement ecosystem that includes many privacy organizations, such as the American Civil Liberties Union (ACLU) or the Electronic Frontier Foundation (EFF).

Being a country with a supervisory model based on disclosure for capital markets, in the U.S. the Securities and Exchange Commission (S.E.C.) has had cybersecurity disclosure guidance for firms

---

[20] For a complete description of the U.S. frameworks, see Baker McKenzie (2018) Global Privacy and Information Management Handbook, available at: https://tmt.bakermckenzie.com/-/media/minisites/tmt/files/global_privacy_handbook-_2018.pdf?la=en.

[21] See the website of the Privacy Shield Program, available at: www.privacyshield.gov/Program-Overview.

[22] See the website of the U.S. Federal Trade Commission, available at: www.ftc.gov.

since 2011, adopted by the Corporate Finance Section of the authority. In February of 2018 the rules where revamped and the Commissioners themselves got involved in a new version of the Guidance.[23]

In the new guidance, the S.E.C.'s Commissioners say that "given the frequency, magnitude and cost of cybersecurity incidents," the Commission "believes that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion". Then they add that the Commission also believes that "the development of effective disclosure controls and procedures is best achieved when a company's directors, officers, and other persons responsible for developing and overseeing such controls and procedures are informed about the cybersecurity risks and incidents that the company has faced or is likely to face". This puts a high level of responsibility for cybersecurity over the corporate governance of the firm as such disclosures "allow investors to assess how a board of directors is discharging its risk oversight responsibility in this increasingly important area."

The stock exchanges add disclosures in their listing rules, which apply to cybersecurity risks when they are material. The New York Stock Exchange (NYSE), for example, requires listed companies to "release quickly to the public any news or information which might reasonably be expected to materially affect the market for its securities."[24] NASDAQ also requires listed companies to "make prompt disclosure to the public of any material information that would reasonably be expected to affect the value of its securities or influence investors' decisions."[25]

C. Other

1. The OECD Privacy Guidelines

In July 2013, the OECD revised its Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data,[26] originally adopted in 1980, as a response to what the OECD described as "changing technologies, markets and user behavior, and the growing importance of digital identities." The Guidelines apply to personal data treatment, whether in the public or private sectors, which, due to its processing, nature or use, poses a risk to privacy and individual liberties. OECD members consider them "as minimum standards which can be supplemented by additional measures for the protection of privacy and individual liberties, which may impact cross border flows of personal data."

The Guidelines state that cross-border data flows should be uninterrupted and secure, but that member states may restrict them when the destination country does not yet substantially observe the Guidelines or when the re-export of the data would circumvent its domestic privacy legislation. The Guidelines also state that members should avoid developing laws, policies and practices that create obstacles to international flows of personal data that would exceed requirements for data protection.

---

[23] See the U.S. S.E.C.'s Commission Statement and Guidance on Public Company Cybersecurity Disclosures of February 2018, available at: www.sec.gov/rules/interp/2018/33-10459.pdf.

[24] See: NYSE Listed Company Manual Rule 202.05 – Timely Disclosure of Material News Developments, available at: http://wallstreet.cch.com/LCMTools/PlatformViewer.asp?selectednode=chp%5F1%5F3&manual=%2Flcm%2Fsections%2Flcm%2Dsections%2F.

[25] See: Nasdaq Listing Rule 5250(b)(1), available at: http://nasdaq.cchwallstreet.com/nasdaq/main/nasdaq-equityrules/chp_1_1/chp_1_1_4/chp_1_1_4_4/chp_1_1_4_4_4/chp_1_1_4_4_4_10/default.asp.

[26] OECD (2013), The OECD Privacy Framework, available at: www.oecd.org/internet/ieconomy/privacy-guidelines.htm.

2. The APEC Privacy Framework

The APEC Privacy Framework was created in 2005 to be applied to data controllers in member jurisdictions with the ambition to establish effective privacy protections, which mostly focuses on avoiding barriers to information flows, and ensuring continued trade and economic growth in the Asia Pacific region. The framework contains principles and implementation guidelines, and, since 2011, it also includes an APEC\Cross-Border Privacy Rules (CBPR) system (updated in 2015, in line with OECD's updated rules).

The APEC CBPR system operates as voluntary certification scheme that allows companies to transfer personal data between APEC economies. It is a mechanism for mutual recognition between diverse domestic privacy laws, avoiding the creation of barriers to cross-border information flows. The U.S. was the first country to join the CBPR in 2012, and IBM became the first company to be certified a yard later. Canada, Japan and Mexico have followed suit. Like the EU-U.S. Privacy Shield, the CBPR is based on self-assessment and a compliance review.

II. Corporate governance implications

As shown in the previous chapter, some international data protection and privacy frameworks are incorporating the view that those that create the risk have the primary responsibility to mitigate it. As a result, companies are the main target of the new obligations and related sanctions. The way some regulators and legislators have used, to make sure that companies are paying attention, is to raise the profile of data protection. The aim is to turn it into a risk that those that run firms have to manage, either to prevent the company to suffer consequences or to limit their own liability. This means that data protection and cybersecurity have become an important aspect of corporate governance.

This chapter aims to describe how the management of cyber risk and data protection is viewed from a corporate governance perspective. It also seeks to discuss why the involvement of corporate leaders may be a key to meaningful changes to business models and corporate practices, which can improve data security and privacy.

A. Companies at the center of regulations

The scope of corporate cyber risk is extremely wide, and it will likely continue to increase unless companies improve their commitment to cyber security. A 2018 survey by Kaspersky Lab,[27] a technological consultant firm, collected responses from almost 6,000 businesses across 29 countries, showing that 46% of small and medium-sized companies and 42% of large enterprises have suffered at least one data breach at some point in their history. In 40% of all those cases personal data from customers had been stolen.

[27] See Kaspersky Lab (2018), From data boom to data doom: the risks and rewards of protecting personal data, available at: https://go.kaspersky.com/rs/802-IJN-240/images/Kaspersky_Lab_Business%20in%20a%20data%20boom.pdf.

A 2017 study by the Ponemon Institute and IBM Security, analyzing over 400 companies from 13 jurisdictions, concluded that the average organizational cost of a data breach in 2017 was $3.62 million USD, even if in some countries it was much higher, like in the U.S. where it was $7.35 million USD on average.[28] Class-action lawsuits add to these costs in some jurisdictions, with settlements reaching over $100 million USD for large breaches[29] while, on average, stocks of affected companies decline in price about 5% following the disclosure of such events.[30] But disruption is not only financial, as 31% of those companies in the Kaspersky Lab survey that experienced a breach said they had to also lay off staff as consequence.

As a result, the strategy taken by some regulators to place legal responsibility for data protection on boards and senior management is a sensible approach, naturally aligned with the interest of companies themselves. By bringing cybersecurity and privacy to the attention of the top of firms, regulators are turning data protection squarely into one of the most relevant new issues for corporate governance. Thus, addressing data protection has become wider than an information technology issue, which has to be complied with as part of the obvious duty to comply with laws and regulations. It is becoming a risk that raises serious management challenges, both from financial and reputational perspectives, and that can expose the company and its leaders to material consequences.

B. The responsibility of the board

In line with good corporate governance principles, the board is by design expected to identify and deal with risky issues and oversee management, to ensure that they are mitigated in a way that can ensure the sustainability of the company. The board of directors of a company has to exercise control, oversight and set the risk appetite and tolerance for the organization, in-line with the mission, vision, values and the strategic plan it has set for the business.[31]

Lack of compliance with data protection could have significant business consequences. It will likely prevent companies from doing business with some counterparts or even in entire jurisdictions. It may also expose a company's processes and practices to demands of a third-party audit and due diligence to retain clients. In this point it is important to consider that the responsibility for data protection is not only to prevent it from being stolen, but also about the proper use of that information in relation to individuals' rights, which is harder to audit and verify via due diligence.

---

[28] See Ponemon Institute and IBM Security (2017), Cost of Data Breach Study: Global Overview (Jun. 2017), available at: www.ibm.com/downloads/cas/ZYKLN2E3.

[29] See Southwell, Alexander H. et al, Gibson Dunn Reviews U.S. Cybersecurity and Data Privacy, The CLS Blue Sky Blog (Columbia Law School), February 3, 2017, available at: http://clsbluesky.law.columbia.edu/2017/02/03/gibson-dunn-reviews-u-s-cybersecurity-and-data-privacy/.

[30] See: Ponemon Institute (2017), The Impact of Data Breaches on Reputation and Share Value, May 2017, available at: www.centrify.com/media/4772757/ponemon_data_breach_impact_study_uk.pdf.

[31] The G20/OECD Principles of Corporate Governance establish that boards are expected to have oversight "of the accountabilities and responsibilities for managing risks, specifying the types and degree of risk that a company is willing to accept in pursuit of its goals, and how it will manage the risks it creates through its operations and relationships. It is thus a crucial guideline for management that must manage risks to meet the company's desired risk profile". See OECD (2015), G20/OECD Principles of Corporate Governance, OECD Publishing, Paris, available at: http://dx.doi.org/10.1787/9789264236882-en.

Data protection rules in some jurisdictions are increasing these stakes by stating expressly that board members and top managers are responsible to address these risks. Because of this, they may become personally liable for cybersecurity-related issues, in a way that not even their cyber and "directors and officers" (D&O) insurance may be able to protect them from damages. As suggested by insurance experts,[32] boards' failure to implement due data protection measures may be viewed as a breach of their own duties to comply with the law, promote the success of the company or to exercise due care, skill and diligence. Thus, they may be exposed to damages and termination or disqualification that insurance may not shield them from.

Corporate leaders are therefore being forced to become active participants in protecting customers' data. They are incentivized to ensure that internal processes and policies are in place to address potential breaches, and to oversee an effective implementation of privacy rules, for both the company and their own interest.

Numerous organizations offer advice as how boards can oversee these risks. The EY Center for Board Matters[33] suggest some of the main objectives that boards need to consider to effectively oversee the management of cybersecurity: i) Understanding the cyber risks facing the organization and how they may affect the business; ii) Challenging the effectiveness of the organization's cybersecurity risk management program, and supporting the continued evolution of the program; iii) Gaining confidence in the adequacy of the program; and iv) Having assurance in the information they receive.

Deloitte UK also suggests a number of questions that boards could use to address their responsibilities towards cybersecurity.[34] These are: i) Do we demonstrate due diligence, ownership, and effective management of cyber risk? ii) Do we have the right leader and organizational talent? iii) Have we established an appropriate cyber risk escalation framework that includes our risk appetite and reporting thresholds? iv) Are we focused on, and investing in, the right things? And, if so, how do we evaluate and measure the results of our decisions? v) How do our cyber risk program and capabilities align to industry standards and peer organizations? vi) Do we have a cyber-focused mindset and cyber-conscious culture organization wide? vii) What have we done to protect the organization against third-party cyber risks? viii) Can we rapidly contain damages and mobilize response resources when a cyber incident occurs? ix) How do we evaluate the effectiveness of our organization's cyber risk program? and x) Are we a strong and secure link in the highly connected ecosystems in which we operate?

Some of these steps for ensuring cybersecurity are essential for data protection, but do not go all that way, as they do not sufficiently address the risk of internal misuse of data. External firewalls and encryption may be useless if a rogue employee or a subcontractor with unrestricted access to protected personal data stoles or misuses them. For that, companies and experts have developed additional guidance, including data governance, which focuses on the availability, usability, consistency, integrity and security of data.

---

[32] See *Directors Beware: The EU's General Data Protection Regulation Is Upon Us!*, bolg post by Kevin LaCroix, December 20, 2017, available at: www.dandodiary.com/2017/12/articles/uncategorized/guest-post-directors-beware-eus-general-data-protection-regulation-upon-us/.

[33] See EY Center for Board Matters (2017), The evolving role of the board in cybersecurity risk oversight, July 2017, available at: www.ey.com/us/en/issues/governance-and-reporting/ey-the-evolving-role-of-the-board-in-cybersecurity.

[34] See Deloitte (2017) Assessing cyber risk: Critical questions for the board and the C-suite, available at: www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-ra-assessing-cyber-risk.pdf.

In this broad context of cybersecurity and data protection, the role of the board essentially involves asking the right questions (information), supporting the development of the necessary measures and policies (protection), ensuring proper disclosure (reporting), and keeping active oversight over the functioning of the framework (supervision).

1. Information

The first step to any attempt by the board to tackle data protection risks is to fully understand the relevant risks and assess how they apply to their firm. Developing sound data protection frameworks on top of cybersecurity, requires "a self-assessment risk-based approach to compliance".[35] No regulator or legislator will be in a position to tell companies what to do in their particular case with the data they hold, as it is for each of them to identify their own risks and implement the required measures. The first step is to know what data the company is collecting, what is worth keeping and securing and what may not be needed in the future. This may have important strategic and business planning implications, as well as impact on the budget and bottom line, as the cost of developing secure systems is high.

In the U.S., the National Association of Corporate Directors issued a Cybersecurity Handbook in 2017[36] offering 5 principles that, although designed for cybersecurity more generally, help to summarize what boards should consider to address data protection risks as well:

- Directors need to understand and approach data protection as an enterprise-wide risk management issue, not just an IT issue;
- Directors should understand the legal implications of data protection risks as they relate to their company's specific circumstances;
- Boards should have adequate access to data protection expertise, and discussions about data protection risk management should be given regular and adequate time on board meeting agendas;
- Directors should set the expectation that management will establish an enterprise-wide data protection management framework with adequate staffing, budget and regular reviews; and
- Discussion between the board and management about data protection risk should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach.

Specifically, in terms of data protection and in the context of compliance with the GDPR, the UK's Information Commissioner's Office (ICO) has also produced a check-list[37] that boards can use to self-assess their practices. It invites boards to answer the following questions:

---

[35] See Grigorescu, Catalin, *GDPR is mainly about corporate governance*, LinkedIN blog post, June 22, 2017, available at: www.linkedin.com/pulse/gdpr-mainly-corporate-governance-catalin-grigorescu.

[36] See NACD (2017), Director's Handbook on Cyber-Risk Oversight (January 2017), available at: www.nacdonline.org/insights/publications.cfm?ItemNumber=10687.

[37] See UK ICO (2018), the UK's Information Commissioner's Office Guide to the General Data Protection Regulation (GDPR), August 2, 2018, available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/.

- Do we take responsibility for complying with the GDPR, at the highest management level and throughout our organization?
- Do we keep evidence of the steps we take to comply with the GDPR?
- Do we put in place appropriate technical and organizational measures, such as: adopting and implementing data protection policies (where proportionate); taking a 'data protection by design and default' approach; putting written contracts in place with organizations that process personal data on our behalf; maintaining documentation of our processing activities; implementing appropriate security measures; recording and, where necessary, reporting personal data breaches; carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests; appointing a data protection officer (where necessary); and adhering to relevant codes of conduct and signing up to certification schemes (where possible); and
- Do we review and update our accountability measures at appropriate intervals?

2. Protection

Having a clear understanding of the status quo is essential for boards to be able to move ahead into the adoption the technical and policy measures necessary to increase security of the data. From a technical standpoint, there are a multitude of approaches for developing safeguards around information technology systems, security, encryption, backups and control of data and information. Boards are obviously not expected to implement them, as that is in the hands of management and external experts that the company may need to engage.

However, within corporate governance frameworks, and in line with emerging legal and regulatory expectations such as those included in the GDPR, the board is ultimately responsible for the appropriate integration of data protection concerns in the strategy and business plans of the company. This entails making sure that the technical solutions appropriately fit the company; that the budgets and other resources for their proper implementation are available and that the necessary actions are implemented through the firm to embrace the new security and privacy features.

An eSecurity Planet's Magazine survey[38] that explored the views of the magazine subscribers (from security engineers up to CIOs and CEOs), found that 54% of companies will increase their IT security spending in 2019, and that 30% will increase their spending between 10 - 20%, or more. The survey also documents a strong hiring demand for IT security staff, with 57% of firms planning to recruit such staff within the next 12 months.

But data security cannot be bought, as it is not just a matter of obtaining technology that solves the problem. Preventing cyber risk and protecting data requires a long-term approach looking to make incremental improvements in security and protection by changing the organizational culture. Employees need to turn keeping information safe and following security protocols part of their daily routines. They need to understand what is allowed to do with the data and what is not.

[38] See *Over Half of Companies Are Upping Spending on IT Security: eSecurity Planet Survey*, by Paul Shread, Posted February 6, 2019, available at: www.esecurityplanet.com/network-security/survey-2019-businesses-accelerate-spending-hiring.html.

One way to improve culture around data protection is to work on data governance, which is one of the main trends following the adoption of the GDPR and a sprawling field of work for lawyers, software developers and IT experts. By establishing automated and seamless processes of data recording and storage to ensure effective data management throughout the company, data governance tackles the protection of the data from origin to disposal, facilitating compliance and ensuring the availability of data for business intelligence.[39]

For that, the governance of data is structured around policies, processes and people. Policies are used to classify the data upon collection, uniform its recording to ensure quality and trustworthiness, protect its integrity and the privacy of personal data. Processes make sure that policies are implemented throughout the organization, while leadership and training engage people to adopt a culture of data protection that is imbedded in their day-to-day operation.

Training is essential to build such a culture and to prepare firms for the event of a breach, which is not something that could be completely avoided. Using scenarios and a clear definition of roles for the contingency, firms can prepare to react as best as possible to a breach to data security. If the risk is ever materialized, the company will be able to execute the plans it has prepared to ensure that the incident is contained while the business continues to operate. A well-prepared board would, in such a case, make sure it is quickly briefed about the scale of the attack and the information that has been compromised, to oversee the adoption of the necessary actions, including notifying the authorities and/or the data subjects, as applicable.

3. Reporting

Disclosure of risks and risk mitigation strategies is yet another important element in the role of the board towards data protection. Providing shareholders and other stakeholders with appropriate disclosures of the material cyber and data risks the company is exposed, is essential for the market to be able to assess the value of the company and, also, a way for board members to reduce their personal exposure. Considering the frequency, magnitude and cost of cybersecurity incidents, these risks could be material in many sectors and investors are increasingly demanding firms for more and better disclosure.

In 2017, Deloitte suggested seven principles for boards to be able to improve cyber risk disclosures that could easily be adapted to focus on data protection:[40]

- Think carefully if cyber is not identified as a principal risk for your company;
- The damage that cyber-risk can cause if so high that a detailed disclosure is worthwhile to highlight the risks to shareholders and let them know the company is taking them seriously;
- The better disclosures are company-specific, year-specific and provide sufficient detail to give meaningful information to investors and other stakeholders;
- Boards and committees should educate themselves about the cyber-threat and challenge management on how they are dealing with cyber risk;

---

[39] For more information about data governance, see the website for The Data Governance Institute, which provides vendor-neutral data governance best practices and guidance, available at: www.datagovernance.com.

[40] See Deloitte (2017), Just 5% of FTSE 100 companies disclose having a board member with specialist technology or cyber experience, Press Release, February 6, 2017, available at: www2.deloitte.com/uk/en/pages/press-releases/articles/just-5-of-ftse-100-companies-disclose.html#.

- Companies should take credit for what they are doing, including describing who has executive responsibility, board level responsibilities, the policy framework, internal controls, and disaster recovery plans;
- Boards should think about what could be missing from their disclosures, for example a clear indication of the main threats facing the company, who poses those threats, the likelihood, possible impact and detail about what the company – and the board – is doing to manage or mitigate those particular risks; and
- Finally, if the company's disclosure does not look strong enough after taking credit for what the company is doing already, the board should ask itself whether it is actually doing enough to manage cyber-risk.

In the U.S., the Council of Institutional Investors (CII) published a list of questions for investors to pose to boards in an effort to understand how they are prioritizing cybersecurity. The questions suggested by the CII are:

- How are the company's cyber risks communicated to the board, by whom, and with what frequency?
- Has the board evaluated and approved the company's cybersecurity strategy?
- How does the board ensure that the company is organized appropriately to address cybersecurity risks? Does management have the skill sets it needs?
- How does the board evaluate the effectiveness of the company's cybersecurity efforts? and
- When did the board last discuss whether the company's disclosure of cyber risk and cyber incidents is consistent with legal and regulatory requirements?

4. Supervision

Once a data protection framework is in place, a new task starts to make sure it remains up-to-date and functioning effectively. This may be as difficult as designing the system itself, since it involves looking for technical but also human failures. A state-of-the-art system will not be safe if any of the individuals that has access to the data can create a vulnerability by falling for a phishing scam, for example. The same could be said if any insider with access to a USB port can copy and steal sensitive data from the company's systems.

Sound oversight is, thus, both technically complex and time consuming and boards need to ensure that management is active in compliance. A board's guidance should inform the company's policies and procedures, and management should adopt appropriate steps for their effective implementation throughout the company. This has to permeate into its culture, including from a compliance, human capital and information technology perspective, as well as involving all other relevant departments, such as marketing, sales and customer support.

The task for a board is to become conversant in the technical solutions and options available to identify, monitor and improve any gaps in the risk management for data and information storage, processing and control. It has to consider scenarios and develop mitigation plans or contingency measures, working closely with the technical people.

A number of organizations have created frameworks and methodologies to help firms evaluate and report on their cybersecurity programs. The American Institute of CPAs (AICPA) offers

one such guidance for evaluating and reporting on an organization's cybersecurity risk management program and underlying controls.[41] Its use is entirely voluntary and offers tools that can be used to identify gaps and design remediation activities to fill those gaps. Guidance from AICPA and other professional and international bodies offers boards frameworks to guide their efforts in an area that may not be familiar to many of its members, allowing them to have confidence they have asked the right questions and obtained the necessary answers to fulfill their oversight role. It also can also give them a measure by which to compare their firms risk management efforts with those of their peers.

C. Board skills and committees

Recent cybersecurity cases have shown that, unfortunately, many large and sophisticated companies are not sufficiently prepared to tackle the data protection risks facing the company. Some of the key factors that may be preventing them to succeed are the skills set of those who sit at the board and how they allocate responsibilities to specialized board committees.

1. Board composition

A well-organized board of directors involves people with complementary skills and experiences who can collectively address challenging issues. The majority of the directors of today have backgrounds in finance, law and business, which bring into the boardroom skills and experience that have been useful in most firms for decades. Directors with skills and experience involving technology or science are currently a minority, reflecting in part that they area of expertise has become more relevant for the average firm only in recent years. This poses the risk that in the absence of the necessary knowledge at the board, it may act simply as a consumer of metrics and information prepared by management. A number of surveys and studies have picked this as a problem for cybersecurity and data protection, encouraging firms to add specific expertise to their boards, so that they can exercise ownership for these issues.

Yet, a number of surveys and studies show that board's cyber skills are scarce even for leading firms in developed markets. A 2016 report by Russell Reynolds,[42] a consultant firm, analyzed the backgrounds of board members of 300 large companies (Fortune 100 companies in the U.S. as well as Fortune 100-equivalent companies in Europe and Asia/Pacific), looking for the presence of non-executive board members with significant digital experience. Their conclusion was that they account for less than 5% of total board seats, even if this was an improvement from 2014's results.[43]

Similar findings were obtained by a 2017 Deloitte[44] review of the annual returns and board member biographies of FTSE 100 companies. Deloitte's results showed that while 87% of companies identified cyber as a principal risk, only 5% of them had any cybersecurity experience in their board.

---

41 See AICPA (2017), AICPA Unveils Cybersecurity Risk Management Reporting Framework, April 26, 2017, available at: www.aicpa.org/press/pressreleases/2017/aicpa-unveils-cybersecurity-risk-management-reporting-framework.html.

42 See Russel Reynolds (2016), Digital Directors 2016: Diverse Perspectives in the Boardroom, 2016, available at: www.russellreynolds.com/en/Insights/thought-leadership/Documents/2016%20Digital%20Directors%20FINAL.PDF.

43 No further surveys are publicly available from Russel Reynolds to check progress to date under the same methodology.

44 See *Only 5% of FTSE companies have cyber-security expertise on the board*, by Tom Reeve, SC Media, February 6, 2017, available at: www.scmagazineuk.com/5-ftse-companies-cyber-security-expertise-board/article/1475347.

This gap in boards' composition has been detected even in sectors that are particularly exposed to cyber risks, such as banking and finance. Accenture, another consultancy firm, reviewed in 2017 the professional experience in boardrooms of 109 of the largest banks around the world,[45] concluding that: i) only 6% of board members and 3% of CEO had technology professional backgrounds; and ii) 43% of banks did not have any board members with a professional technology background, while 30% had only one such person. Several other sources report similar findings in most developed markets.

But, adding a person with expertise to the board is not the only way to address this potential gap. It is also possible to improve the skills of those already at the board or to complement it with experts made available from within management. In the first case, the obvious tool is training, yet only a few companies are providing cyber-risk training to their boards.

According to a 2018 UK Government's survey[46] of FTSE 350 companies, while 57% of respondents reported they have clear understanding of the potential impact of loss of or disruption to key information or data assets, 68% said they have not received any training on how to deal with a cybersecurity incident. Regarding data protection in particular, only 6% of companies declared themselves ready for the entry into force of the GDPR under that survey.

Further, looking into the availability of external cyber expertise to boards, a 2018 survey of chief information officers (CIOs) by Gartner,[47] a research and advisory company, showed that 35% of firms declare not having cyber-security experts in their management and that they are unsure how to protect their organizations' sensitive information, communications or data. This, despite the fact that 91% of CIOs declared that they expect cyber-threats to increase over the next three years.

2. Specialized committees

Board committees are also a way to help boards to deal with particularly complex issues, as they allow the board to have a smaller group of members, sometimes with the help of external experts, spending sufficient time on such issues to prepare the discussion at the board level, where they subsequently report.

Across all industries, boards generally rely on three committees that are the most commonly required by laws and regulations: audit, compensation, and nomination/governance. This means that issues like cybersecurity and data protection have to either be discussed at the full board level or assigned to one of these three committees. Many firms assign cybersecurity issues to the audit committee, where they have to compete for attention with a number of other important priorities and risks.

Cybersecurity committees, where they exist, can take primary responsibility for all cyber risk matters, even if the board would still remain responsible as a whole. They tend to have a charter

---

45 See Accenture (2016), Bridging the technology gap in financial services boardrooms, by Richard Lumb et al., 2016, available at: www.accenture.com/t20160118T152822__w__/us-en/_acnmedia/PDF-4/Accenture-Strategy-Financial-Services-Technology-Boardroom.pdf.

46 See the UK Government (2017), FTSE 350 Cyber Governance Health Check Report, July 2017, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/635605/tracker-report-2017_v6.pdf.

47 See Gartner (2018), The 2018 CIO Agenda, by Kasey Panetta, October 27, 2017, available at: www.gartner.com/smarterwithgartner/the-2018-cio-agenda-infographic/.

that sets as their objective to identify, evaluate and monitor all cybersecurity activities within the firm and to determine how they align with the overall corporate risk profile.

These committees take a wide-angle view of the cybersecurity risks, considering all aspects within the firm, but then they focus of specific threats, often using scenarios and simulations. They check how well prepared the company is to prevent them, to mitigate the damage they may cause, and to recover the essential functionalities that may have been affected. By doing so, they get a deeper analysis of these complex issues and distill the essential information the board needs to make informed decisions, identifying issues that deserve a high priority and helping the board to prioritize them in their oversight.

Creating a committee to deal with cybersecurity issues, and perhaps also more generally with technology and science, is nevertheless a decision that will force a board to consider issues like the size of the firm, IT budget and the expertise available (at the board or through external advisors). In practice, it is not common for firms to have committees dealing specifically with cybersecurity, let alone with data protection, and most firms stay with the three traditional committees already mentioned.

In a 2018 survey that tracked board structures in S&P 500 companies, EY concluded that board committee structures have stayed largely the same over the past six years.[48] Since 2013 only a few companies have created committees that focus on compliance (16%), risk (11%) and technology (7%). Further, only 10% of companies included in the sample assigned responsibility for cybersecurity, digital transformation and information technology to a specific committee, often technology, risk or compliance committees.

D. The role of regulation

One after another, the surveys and reports discussed above show mixed results. On the one hand, they show that firms are significantly increasing their awareness of cyber risks in general, and of the need to better protect personal data in particular. But, on the other, they show that firms are far from ready to implement this, and that boards have a long way to go before being able to handle these technological risks with the same ease as they deal with financial ones, for example. There is a significant gap and a pressing need to address it.

Undoubtedly, there is room for regulation to help bridge this gap. As a general matter, however, policy interventions in technological matters involving fast pacing innovations are not easy for regulators of any size. There is a need to understand clearly the underlying elements behind the technology not to tie the rules to specific technical applications that may become obsolete overnight. Principle-based rules are often a good way to ensure technological neutrality and foster innovations, while sandboxes and grandfathering periods also help fine tuning the rules.

Another important challenge is to tailor the rules and requirements to the particular characteristics of the market and the companies in it. While it may be tempting to adopt the same standards introduced in other, often more developed markets, policymakers already know that adaptation is essential as institutions and practices vary widely among jurisdictions. Countries like the U.S. may be able to rely on disclosure and private enforcement, within a context of a precise

[48] See Klemash, Steve W. et al. (2018), EY Center for Board Matters, *A Fresh Look at Board Committees*, at Harvard Law School Forum on Corporate Governance and Financial Regulation, July 10, 2018, available at: https://corpgov.law.harvard.edu/2018/07/10/a-fresh-look-at-board-committees/#1.

definition of board fiduciary duties and well-functioning courts. But in many countries around the globe, successful litigation in the absence of clear legal obligations may be an uphill road even for the regulator itself.

Differences in legal culture, capital concentration, market supervision regimes or even the sophistication and integrity of key players, can play a large part in rendering a data protection regime effective or inefficient, regardless of the letter of the law. Authorities have therefore to carefully determine the tools available to intervene, from hard to soft law; from setting legal obligations to inverting the burden of proof; from the adoption of education programs and dissemination to the drafting of dissuasive sanctions, among others.

For this, a good starting point is to have sufficient information about current practices, locally and across the region. That may allow policymakers to draw a reasonable road map to move their national frameworks towards the desired standards, within a suitable timeframe and with sufficient guarantees for both individuals and businesses.

The EU's GDPR and the U.S. S.E.C.'s guidance are moving data protection forward, among other means, by shaping the way in which boards of directors are addressing cybersecurity and data protection in their jurisdictions. They are requiring boards to be personally involved in the design of data protection systems, and their effective integration into the strategy and business model of firms. They are creating management positions dedicated to these topics, like the DPO, mandating the use of DPIAs, and more.

These new rules are forcing firms to increase their attention towards cybersecurity and data protection, in line with firms' own assessment that they are indeed important topics. By turning these risks into compliance matters, regulation can help ensure that they will not be set aside for other more pressing issues the firm may be facing, and that budgets and other necessary resources will be made available, as they may look more affordable once the size of potential fines is factored in.

Interestingly, while it is common for industry leaders and business lobbyist to be reluctant about the prospects of new rules, often suggesting that self-regulation is a better alternative, cybersecurity and data protection seem to be an exception. This is one area where a consensus is forming about the need to have national, if not global, benchmarks.

In the latest Spencer Stuart survey on the views of boards of directors,[49] board members say that cybersecurity risk is a top concern for companies and that, in their perception, the risks are intensifying. While 78% of them answered in 2017 that additional regulation would have little effect in curbing cyber-attacks and would overburden companies, by 2018 60% were now in favor of such regulation. About 20% percent of those interviewed said that high-profile breaches have persuaded them to change their stance in favor of more cyber regulation.

The next chapters of this paper will explore these issues in the context of Latin America and the Caribbean, aiming to assess the role regulation is playing or could play to further enhance cybersecurity and data protection, using the corporate governance framework of firms in the region.

[49] See Spencer Stuart (2018), What Directors Think, 2018, available at: https://www.spencerstuart.com/-/media/2018/april/what-directors-think-2018.pdf.

III. Data protection in the region

A. Overview

The development of data protection rules in Latin America has followed a path were, like in other parts of the world, two strong forces have battled for dominance: privacy versus transparency.

Privacy as under its modern concept was developed many decades ago as a response, among others, to the actions of governments and the risk that an authoritarian regime could use personal information to undermine people's rights, freedoms and democracy. In this context, privacy is understood as the protection of personal data so that people can live their lives any way they see fit, without interference from others, as long as they respect other people's rights. This concept applies today also to any other, non-governmental organization, that may want to use peoples' personal information, especially that of a sensitive nature, to discriminate or violate their rights due to their race, religion, sexual or political orientation, and the like.

Transparency, on the contrary, is premised on the idea that keeping information secret is the germ for many of the evils that corrode our institutions. Laws granting public access to certain information are therefore viewed as anti-corruption tools that keep organizations and people honest. That *transparency is the best disinfectant* is a motto for many regulators and NGOs in a number of fields, from bribery of public officials and tax enforcement agencies. The same is true for organizations that would like to use e-government and e-collaboration platforms to generate spaces for public participation and cooperation that can ensure accountability of those in power, weather political, economic or from any other source.

At different moments in time these two forces have been at battle in the rules adopted by countries in the Latin American and Caribbean region. At times, the rights of individuals may have been exposed to unwarranted harm in the interest of transparency, while in many others privacy

considerations have prevented public access to information that would have contributed to a better functioning democracy, or a less corrupt society.[50]

Finding the balance is an ongoing task that has several decades in the making, but one where privacy has generally had an advantage over transparency. Privacy principles are present in almost all the constitutions of the region in an explicit manner, including the recourse of habeas data,[51] and also found in the American Convention on Human Rights.[52] Nevertheless, the advancement of transparency, mainly in the form of laws granting access to public information as a way to increase accountability of those in power, has helped reaching a more balanced result. The American Court of Human Rights had a chance to show this in a seminal ruling of 2004, where it concluded that the right to privacy couldn't be used to prevent the disclosure of newsworthy information concerning public officials.[53]

The appointment of authorities to deal with data protection within the region is an example that shows the intimate link between privacy and transparency. Mexico, Peru, Uruguay and Argentina share the same regulator for data protection and for transparency and access to public information. In some cases, privacy was added as a new area of competence to already exiting transparency agencies, while in others, the data protection agency was charged also with transparency. Sometimes this genesis has visible consequences in the emphasis with which agencies with dual mandate reconcile the inevitable conflicts they face between privacy and transparency.

Eventually, the region has seen the emergence of data protection rules that are responding to the need to facilitate business development at par with protecting the rights of individuals. Argentina and Uruguay were pioneers of data protection as they decided early on that they needed to comply with the European framework to facilitate the outsourcing of services to Europe. When some of those businesses decided to relocate within the region, many governments moved to improve their privacy frameworks to attract them. The processing of personal data of Europeans,

---

50 As a regional expert of the subject has argued: [...] "we have seen how, incorrectly, the personal data legislation has been blocking legitimate access to information that would serve to make the State more transparent [...] but equally wrong are the positions to consider the legislation of personal data as an impediment to access information [...] going against personal data legislation is not understanding privacy as a basic and fundamental human right" (text is a free translation from the original Spanish language). See *Protección de Datos Personales y Acceso a la Información: Dos lados de la misma moneda*, by Erick Iriarte, La República, November 11, 2014, available at: https://larepublica.pe/tecnologia/833431-proteccion-de-datos-personales-y-acceso-a-la-informacion-dos-lados-de-la-misma-moneda.

51 "Habeas Data is a constitutional right granted in several countries in Latin America. It shows variations from country to country, but in general, it is designed to protect, by means of an individual complaint presented to a constitutional court, the image, privacy, honor, information self-determination and freedom of information of a person. Habeas Data has been described as: 'a procedure designed to safeguard individual freedom from abuse in the information age'. The importance that this figure has is stressed by the fact that it can be a mechanism available to citizens that will insure a real control over sensible personal data, stopping the abuse of such information, which will be detrimental to the individual." See Guadamuz A, Habeas Data vs the European Data Protection Directive, 2001 (3), The Journal of Information, Law and Technology (JILT), available at: http://elj.warwick.ac.uk/jilt/01-3/guadamuz.html.

52 Article 11. "Right to Privacy: 1. Everyone has the right to have his honor respected and his dignity recognized. 2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.3. Everyone has the right to the protection of the law against such interference or attacks." See the full text of the American Convention of Human Rights, available at: www.oas.org/dil/access_to_information_American_Convention_on_Human_Rights.pdf.

53 See Corte Interamericana de Derechos Humanos, Herrera Ulloa vs. Costa Rica, ruling of July 2, 2004, available at: www.corteidh.or.cr/docs/casos/articulos/seriec_107_esp.pdf.

mostly by call centers in the region, has thus been an important factor in promoting better data protection rules and regulations.

The regional data protection frameworks have also adapted to technological advancement and have become more compatible with the digitalization of the economy. Privacy protections are put to the test with electronic data that are a far more elusive object to protect than the contents of a written document. Indeed, data are traded and exchanged, evolve, get out of date or can be updated, can be duplicated without detriment, and be stored and move anywhere in the world. This has forced the development of legislation that can cope with the demands of the modern information society.[54]

On top of these developments, trade agreements and international cooperation have continued to raise awareness about data protection. The increased trade and economic ties among countries in the region has also brought more attention to issues of cross border data transfers, and to protection of data privacy beyond citizens' own jurisdiction.

As a result of all these trends, today most jurisdictions in the region, if not all, have some sort of data protection framework, although with significant variation in terms of levels of development. Most of them show the influence of some foreign model, which has been adapted more of less to the local reality, while trying to remain compliant with the original. This is in part explained by several regional initiatives that have helped shape data protection in the region and the influence of foreign and international frameworks.[55]

- As already discussed in Chapter II, the OECD, which from the region currently includes Mexico and Chile, and will soon welcome Colombia and Costa Rica, developed privacy guidelines that inspired the development of the GDPR. The European model has had large impact in the Argentinean and Uruguayan frameworks.
- In turn, APEC, which includes Chile, Peru and Mexico from the region, focused on keeping data flows between countries unobstructed to sustain economic integration and trade between Pacific Ocean economies. APEC's Privacy Framework has been very influential in the development of the data protection frameworks of Mexico, Colombia and Peru.
- Specifically for the region, the Ibero-American Data Protection Network, organized and led at its origin by Spain, developed Data Protection Standards that essentially followed the European model under the Directive that preceded the GDPR.
- ECLAC's eLAC initiative also generated a dialogue that aims to use digital technologies as instruments of sustainable development for the Latin America and Caribbean region.

The following paragraphs will describe the last two of these regional efforts and the following sections will present the national frameworks of a selection of countries in the region.

---

[54] See CEPAL (2005), Estado situacional y perspectivas del derecho informático en América Latina y el Caribe, by Erick Iriarte Ahon, available at: https://repositorio.cepal.org/handle/11362/31919.

[55] For more details, see CEPAL (2008), Meta 25 eLAC2007: Regulación en la Sociedad de la Información en America Latina y el Caribe, by Erick Iriarte Ahon, available at: www.cepal.org/socinfo/noticias/noticias/2/32222/GdT_eLAC_meta_25.pdf.

1. Ibero-American Data Protection Network Standards

The Ibero-American Data Protection Network (RIPD, after its acronym in Spanish) adopted its Data Protection Standards of the Ibero-American States[56] in June of 2017, fulfilling the desire of its member countries to facilitate effective cooperation related to data protection and privacy in the region. The Standards' aim "to promote and contribute to the strengthening and adaptation of regulatory processes in the region, through the elaboration of guidelines that serve as a parameter for future regulations or for the revision of existing ones." Section 1.1. of the Ibero-American Standards further states that their purpose is to:

"a. Establish a set of principles and rights for the protection of personal data, which the Ibero-American States can adopt and develop in their national legislation, with the purpose of guaranteeing an appropriate treatment of personal data and having homogeneous rules in the region.

b. Raise the protection level of individuals, regarding the treatment of their personal data, as well as among the Ibero-American States, which answers to the international needs and demands that the right to the protection of personal data demands in a society in which information and knowledge technology are increasingly relevant in all matters of daily life.

c. Guarantee the effective exercise and safeguarding of the right to the protection of personal data of any individual in the Ibero-American States, by establishing common rules that ensure due treatment of their personal data.

d. Facilitate the flow of personal data among the Ibero-American States and beyond their borders, with the purpose of helping the social and economic growth of the region.

e. Drive the development of mechanisms for the international cooperation among the control authorities of the Ibero-American States, the control authorities that do not belong to the region, and international authorities and entities on the matter."

2. Economic Commission for Latin America and the Caribbean's eLAC

Within the umbrella of United Nations, ECLAC has developed a dialogue that sees the use of digital technologies as instruments of sustainable development for the Latin America and Caribbean region. The dialogue promotes the advancement of the digital ecosystem in the region "through a process of regional integration and cooperation, strengthening digital policies that promote knowledge, inclusion and equity, innovation and environmental sustainability."

The initiative traces back to regional dialogue on the information and knowledge society that started in year 2000, with the Declaration of Florianópolis and the commitment to design and implement programs for the access and use of information technologies and communications. During its Sixth Ministerial Conference, which took place in April 2018, eLAC approved the Cartagena Declaration[57] and the Digital Agenda for Latin America and the Caribbean (eLAC2020).[58] Colombia chairs eLAC's 2020 Digital Agenda and ECLAC provides technical secretariat.

---

[56] See Red Iberoamericana de Protección de Datos (2017), Standards for Personal Data Protection, available at: www.redipd.es/documentacion/common/Estandares_eng_Con_logo_RIPD.pdf.

[57] See eLAC (2018), Declaración de Cartagena de Indias, available at: https://conferenciaelac.cepal.org/6/sites/elac2020/files/cmsi.6_declaracion_de_cartagena.pdf.

[58] See the webpage for eLAC 2020 *Agenda digital para América Latina y el Caribe*, available at: www.cepal.org/es/proyectos/elac2020.

The eLAC 2020 Digital Agenda includes 7 action areas and 30 objectives. One of the seven pillars deals with governance for the information society. There, one of the lines of work is to "coordinate actions aimed at guaranteeing privacy, protection of personal data, online consumer protection, access to public information and freedom of expression, in the digital environment."

B. Regional legal and regulatory framework

The following paragraphs describe the main features of the data protection frameworks of a selection of jurisdictions in the region. In each case, the information includes the main legal and regulatory sources, essential definitions and key concepts. It also lists the fundamental rights of data subjects, the rules for transfers to data processors and across borders, as well as the enforcement and sanctions settings. The use of DPO and DPIAs, as well as the relevant accountability and governance rules of each country complete the information presented.

1. Argentina

Applicable rules

The rules and laws that conform the Argentinian framework for data protection include the following:

- Law 25.326, Law on the Protection of Personal Data, of year 2000;59
- Decree 1558 of year 2001,60 which contains the regulation of Law 25.326;
- Decree 899/2017 on Access to Public Information;61 and
- The resolutions of the Argentinian data protection agency (DPA), Agencia de Accesso a la Información Pública (AAIP),62 including Resolution 47/2018,63 which recently replaced the outdated existing rules, Disposiciones DNPDP 11/2006 and 9/2008.

Definitions

- Personal Data: defined as information of any kind referring to ascertainable physical persons or legal entities (data subjects).
- Sensitive Personal Data: Personal data revealing racial and ethnic origin, political opinions, religious, philosophical or moral beliefs, labor union membership, and information concerning health conditions or sexual habits or behavior.
- Jurisdiction/Territoriality: Law 25.326 applies to any physical person or legal entity having a legal domicile, or local offices or branches in Argentina. Registers, data files, databases or databanks that are interconnected through networks at an inter-jurisdictional, national or international level fall within the federal jurisdiction, and are thus subject to the provisions of the Law.

---

59 See the full text of the Law at: www.track.unodc.org/LegalLibrary/LegalResources/Argentina/Laws/Argentina%20Personal%20Data%20Protection%20Act%202000.pdf.

60 See a comparative chart of Act Nº 25.326 and Regulatory Decree Nº 1558/01 Personal Data Protection, available at: http://ceic.org.ar/integrated_chart_act_25326.pdf.

61 See the full text of the Decree at: http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do;jsessionid=1AB78EF4CC7A5889EF30BFE93CBD889C?id=285903.

62 See the webpage of Argentina's Agencia de Acceso a la Información Pública, available at: www.argentina.gob.ar/aaip.

63 See the full text of the AAIP's Resolution at: http://servicios.infoleg.gob.ar/infolegInternet/anexos/310000-314999/312662/norma.htm.

Consent

In general, data subject's consent is required prior to collection, processing and disclosure of personal data. It may be required in writing or otherwise, depending on the circumstances of the interaction. It is however not required when personal data is obtained from unrestricted public access sources, collected for rendering of public services in a legal manner, and when collected by financial entities in connection with financial transactions involving the data subject, among others.

Rights of individuals

Data subjects have the following rights regarding their personal data: information; access; correction; deletion and/or destruction, and the writ of habeas data.

Data protection officers

Although not required by Law 25.326, Data Protection Officers (DPOs) are included in the regulation of the AAIP. In cases of audits and inspections there must be a person accountable for the privacy of databases. In those cases, it is required that the person has residency in Argentina.

International transfers

Transfer of personal data beyond Argentina is limited to countries that provide equivalent levels of data protection as established by Argentinean law, with the exceptions of transfers: i) conducted with the consent of data subjects; ii) within the framework of international treaties signed by Argentina; iii) conducted as part of an international data transfer agreement as approved by the AAIP; iv) for international judicial, intelligence or enforcement cooperation; v) for medical purposes in relation to the data subject or for epidemiology uses; and vi) related to financial and stock trading transfers.[64]

Transfer to data processors

A transfer of personal data to data processors is possible provided it is regulated contractually or by other means that protect it. Data controllers and data processors are jointly liable for data breaches.

Enforcement and sanctions

Violation of the personal data protection framework in Argentina may result in investigations and audits by the AAIP, orders by the AAIP, administrative fines, penalties and sanctions, as well as civil lawsuits or class actions, and criminal proceedings. Depending on the type of infringement, sanctions and fines may range from a fine of 1,000 to 25,000 Argentinean pesos ($23 to $500 USD) for small infringements to suspension of 31 to 365 days and fines up to 5 million Argentinean pesos ($115,500 USD) for the most serious infringements.[65]

Notification of data breaches

The Argentinean framework does not require notification of a data breach to the AAIP or the affected data subjects.

DPIAs and accountability

Data controllers are in some cases required to conduct data protection impact assessments (DPIAs) prior to the implementation of innovations to their databases containing personal data. There are no specific accountability or governance rules.

---

[64] DPA Rule No. 60-E/2016 (Rule 60) provides a list of jurisdictions which the DPA considers provide an adequate level of protection.

[65] See Fernandez, Diego, Argentina Chapter, Data Protection & Privacy 2019, Seventh edition, Getting the Deal Through, available at: https://gettingthedealthrough.com/area/52/jurisdiction/4/data-protection-privacy-argentina/.

2. Brazil

Applicable rules

Within the Brazilian framework for data protection the rules are distributed among several sources, beginning with the Federal Constitution:

- Article 5, X, of the Brazilian Federal Constitution[66] contains the basic individual rights to intimacy, privacy, honor and image;
- Article 21 of the Brazilian Civil Code[67] sets the right to privacy;
- The Brazilian Consumer Protection Code (Law 8.078 of 1990)[68] rules the collection, storage and use of consumer databases;
- Law 12.965 of 2014, the Internet Legal Framework,[69] establishes the legal framework for the Internet in Brazil and the protection of privacy of online data;
- Decree 8.711/2016, regulating the Internet Legal Framework;
- The Brazilian Criminal Code, which sets the criminal part of the framework;
- Additional rules and regulation can be found within several other sources.[70]

Recently, the Brazilian government adopted a new law, the General Data Protection Law,[71] that will enter into force in 2020. It creates a new legal framework for the use of personal data in Brazil that will replace the multitude of specific laws and regulations that currently exist.

Some of the highlights of the new legislation are: i) it will have transversal, multi-sectoral application to all sectors of the economy, both public and private, online and offline; ii) like the GDPR, it will have extraterritorial application: iii) defines personal data broadly and distinguishes sensible data as well; iv) demands a legal basis for collecting, storage and processing data, including consent and others; v) lists 10 principles that should be taken into account in the processing of personal data, including the principle of accountability for data controllers and processors; vi) requires notification of breaches to the data protection authority; vii) incorporate new rules for international transfers of personal data, DPOs, DPIAs and privacy by design, and ix) creates administrative sanctions for up to 2% of the company's, group's or conglomerate's turnover in Brazil in its last fiscal year (with a limit of 50 million Reais – about $12,880,500 USD).

The Brazilian president vetoed three articles of the bill of law, which dealt with the protection of personal data and access to information requests, the transfer of personal data between public authorities and private entities, and transparency on the use of data shared between public entities.

---

66 See the full text of the Brazilian Constitution at: http://english.tse.jus.br/arquivos/federal-constitution.

67 See the full text of the Brazilian Civil Code at: https://wipolex.wipo.int/en/details.jsp?id=9615.

68 See the full text of the Law at: www.planalto.gov.br/ccivil_03/leis/l8078.htm.

69 See the full text of the Law at: https://wipolex.wipo.int/en/legislation/details/15514.

70 These include: Executive Order 7,962/2013 on e-commerce; Law 12,414/2011 on credit history; Law 10,703/2003 on the registration of prepaid cellphone users; Law 12.527 of 2011 on access to public information; Law 13,787/2018 on the digitalization and utilization of computer systems for storage and manipulation of medical record; Law 9,472/1997, regulating the telecommunication services and Regulation 614/2013 of the National Telecommunication Agency; Supplementary Law 105/2001 on bank secrecy and Resolution CMN 4,658/2018, which provide for the cyber security policy and the requirements for contracting services of data processing, data storage and cloud computing; and Executive Order 9,637/2018 on Information Security Policy.

71 See the full text of the Law at: http://dataprivacy.com.br/protecao_de_dados_pessoais.docx.

It also vetoed the articles creating penalties of suspension and prohibition to maintain databases, as well as the creation of a data protection authority. Some of these issues were recently addressed by Executive Order 869/2018, of December 28, 2018.

Definitions

- Personal Data: Decree 8.711 of 2016 defines it as any data related to an identified or identifiable individual, including identification numbers, location data or electronic identifiers when these are related to a person.
- Jurisdiction/Territoriality: the Brazilian Framework applies to any personal data processing carried out in the Brazilian territory or that has for an objective the offer or the supply of goods or services, or the data processing of individuals located in the national territory. It also covers the processing of personal data that have been collected in the Brazilian territory.

Consent

Consent of the data subject is required prior to the collection, use, processing, transfer and disclosure of personal data, and this consent may be withdrawn at any time. According to the new General Data Protection Law, article 5º, XII, consent is defined as "the free, informed and unequivocal pronouncement by means of which the data subjects agree to the processing of their personal data for a specific purpose". There are also specific provisions for the consent for processing sensitive (special) data and the personal data of children and adolescents.

Rights of individuals

Data subjects in Brazil have in relation to their personal data the rights to: information; access; correction; deletion and/or destruction; and to exercise the writ of habeas data.

The new General Data Protection Law establishes also the subject's right to limitation of noncompliant processing and the rights to data portability and of demand for a revision of the decisions taken solely by automated processing of personal data that affects their interests, including the decisions meant to define their personal, professional, consumption and credit profiling or aspects of their personality.

Data protection officers

There is no requirement for the appointment of a DPO in Brazil yet. However, the new General Data Protection Law requires controllers and data processors to appoint a DPO.

International transfers

In Brazil, the transfer of personal data aboard requires the consent of the data subject. Article 33 of the new General Data Protection Law establishes the cases of legal international transfer of data, which are similar to the GDPR cases, highlighting the importance of the appropriate level of data protection.

Transfers to data processors

Transfers of personal data to third parties requires the consent of the data subject and the use of contractual or other means to protect it, such as informing the data subject and the assurance of a proper level of data protection. Data controllers and data processors could be jointly liable for data breaches.

Enforcement and sanctions

Violation of the personal data protection framework in Brazil may give rise to administrative fines, penalties, sanctions, as well as civil and criminal proceedings. Pursuant to Law 12.965, fines can reach up to 10% of the gross revenues of the last fiscal year obtained by the economic group in Brazil, as well as the suspension or prohibition of any data collection within the country.

Under the new General Data Protection Law, fines could reach up to two percent (2%) of the sales revenue of the legal entity, group or conglomerate in Brazil in its last fiscal year, excluding taxes, with an overall limitation of 50 million Reais (about $12,880,500 USD).

Notification of data breaches

The Brazilian framework does not require notification of a data breach to the Federal or State authorities, nor to the affected data subjects. When the new General Data Protection Law comes into force the controller will have to notify the supervisory authority, and the data subject, of the occurrence of any security incident that may result in any relevant risk or damage to data subjects.

DPIAs and accountability

DPIAs are not required in Brazil and there are no specific accountability rules. They will be required pursuant to the new General Data Protection Law, especially when the grounds of the processing are its legitimate interest (article 11, paragraph 3) or in the case of processing sensitive data (article 38).

3. Chile

Applicable rules

The Chilean data protection framework is set by Law 19.628 of 1999, the Personal Data Protection Law, and is admittedly outdated and insufficient for the expectations of regulators and the private sector. Unfortunately, efforts to replace it had been constantly delayed and a lack of enforcement is regarded as an urgent problem.[72]

After a series of recent and high-profile bank hackings, the banking regulator adopted changes to its rules making data protection and issue for ongoing supervision, while the government appointed a cybersecurity tsar and created an ad-hoc commission to develop a new framework, which will replace that created by Law 19.628. A bill of law is currently under discussion in the Senate of the Chilean Congress that would introduce a GDPR-like system and a Data Protection Authority.[73]

In June 2018, Law 21.096[74] introduced a new subsection to Article 19 N0. 4 of the Chilean Constitution,[75] explicitly recognizing the constitutional right to the protection of personal data. The authors of the initiative explain that this was a manner to enhance personal data protection via constitutional actions.

---

[72] See the full text of the Law at: www.leychile.cl/Navegar?idNorma=141599.

[73] The main aspects covered in the bill of law are: i) the express recognition of principles such as finality, proportionality, quality, security, liability and legality of data processing; ii) a more accurate definition of 'consent' as the main source of the legitimacy of data processing and a new statute of exceptions for consent, and iii) the creation of a data protection authority and the establishment of new proceedings to prosecute liabilities.

[74] See the full text of the Law at: www.leychile.cl/Navegar?idNorma=1119730.

[75] See the full text of the Chilean Constitution at: www.camara.cl/camara/media/docs/constitucion_politica.pdf.

Finally a number of sectorial laws and regulations address privacy issues for specific purposes, including Law 20.584, addressing the privacy of medical records; Law 19.496, regarding credit information; Law 18.290, on the privacy of a driver's information; Law 19.799 regarding electronic signatures, which contains the right to privacy of the holder of an electronic signature, and article 154-bis of the Labor Code, which establishes that the employer shall keep confidential all the information and private data of workers under an employment relationship.[76]

Definitions

- Personal Data: any information relating to identified or identifiable individuals.
- Sensitive Personal Data: Personal data that refers to the physical or moral characteristics of data subjects or to facts or circumstances of their private life such as personal habits, racial origin, political ideologies and opinions, religious beliefs, the status of their physical and mental health, and their sexual life.

Consent

In general, consent of data subjects is required, and they should be informed about the purpose of the collection, processing and storage of personal data. According to the Law, however, consent is not required for personal data available from public sources or when used for statistical purposes and the like.

Rights of individuals

Data subjects have the following rights regarding their personal data: information; access; correction; deletion and/or destruction, and the writ of habeas data.

Data protection officers

There is no requirement for the appointment of a DPO in Chile.

International transfers

The current rules do not contain any restrictions, but the bill of law currently being discuss in Congress contains restrictions.

Transfer to data processors

Transfers of personal data to third parties require the use of contractual or other means to protect it. Data controllers and data processors are jointly liable for data breaches.

Enforcement and sanctions

Failure to comply with data protection in Chile may result in civil and class actions. Breaches of data protection caused by improper processing of data may eventually lead to fines determined by the Law (ranging generally from $75 to $760 USD, or from $760 to $3,800 USD if the breach relates to financial data). Fines are viewed and determined in a summary trial.

Notification of data breaches

The Chilean framework does not require notification to the authorities or to the affected data subjects of a data breach.

---

[76] See Magliona, Claudio, Nicolás Yuraszeck and Carlos Araya, Chilean chapter, Data Protection & Privacy 2019, Seventh edition, Getting the Deal Through, available at: www.garciamagliona.cl/pdf/Getting_The_Deal_Through_2018_Data_Protection.pdf.

DPIAs and accountability

DPIAs are not required in Chile and there are no specific accountability rules.

4. Colombia

Applicable rules

The Colombian framework for data protection is structured as follows:

- The Colombian Constitution[77] guarantees individuals right to self-determine the collection, use, storage, processing and transfer of their personal data;
- Law 1.581 of 2012[78] regulates privacy rights in respect of personal data collected and processed in any type of database;
- Law 1.266 of 2008,[79] regulates data privacy for commercial and financial credit rating;
- Law 1.273 of 2009, which amends the Criminal Code, provides the felonies and penalties related to the protection of information and personal data;
- Decree 1.377 of 2013, unified in Decree 1.074 of 2015, partially regulates Law 1.581; and
- Decree 090 of 2018, the National Database Registry.

Definitions

- Personal Data: defined by Law 1581 as any information linked or which may be associated with one or more specific or identifiable individuals. Further, Law 1.581 offers a classification of personal data into three categories: i) private data; ii) semi-private data, which is data that third parties may need to legitimately interact with the data subject; and iii) public data, which refers to information contained in public records or documents.
- Sensitive Personal Data: data that affect the privacy of the data subject or whose improper use may lead to discrimination such as those that disclose racial and ethnic origin, political opinions, religious, philosophical or moral beliefs, labor union membership, membership of social or human rights organizations or organizations promoting the interests of any political party or ensuring the rights and guarantees of opposition political parties and information concerning health conditions or sexual preferences or habits and behavior and biometrical data.
- Jurisdiction/Territoriality: the Colombian framework applies to all data processing carried out in Colombia and data processing carried out abroad but performed by a data processor or data controller whose acts are under the Colombian framework, which is the case when they process personal data of individuals domiciled in Colombia. Interestingly, in January of 2018 the Colombian authorities scaled back the scope of application of some of these rules to exclude SMEs, after noticing the difficulty that they were having to comply with the requirements.[80]

---

[77] See the full text of the Colombian Constitution at: www.corteconstitucional.gov.co/inicio/Constitucion%20politica%20de%20Colombia.pdf.

[78] See the full text of the Decree at: https://iapp.org/media/pdf/knowledge_center/DECRETO_1377_DEL_27_DE_JUNIO_DE_2013_ENG.pdf.

[79] See the full text of the Law at: www.redipd.org/legislacion/common/legislacion/Colombia/LEY_1266_31_12_2008_HabeasData_COLOMBIA.pdf.

[80] See Decree 090 of January of 2018, from the Ministry of Trade, Industry and Tourism, available at: http://es.presidencia.gov.co/normativa/normativa/DECRETO%2090%20DEL%2018%20ENERO%20DE%202018.pdf.

Consent

In general, the collection, use, transfer, storage and processing of personal data requires prior, express and informed consent from the data subject, but there are exceptions for cases of: i) legally authorized processing for record keeping, statistical, scientific, and other purposes; ii) public personal information; iii) information required by a public authority within its legal authority; iv) medical or sanitary emergencies; and v) information related to the civil registry.

The consent must be granted by any mechanism that may be subject to further consultation and must comply with the principles of finality and safety. Processing personal data of a child is forbidden, unless the processing is in the best interest of the child or has been authorized by his legal representative.

Rights of individuals

Data subjects have the following rights regarding their Personal Data: to know, update and rectify their personal data; to request proof of the data processing authorization granted to data controller; to know the type of processing that is being given to their personal data; to file complaints before Superintendence of Industry and Commerce for violation of data protection law; to revoke the consent and request the deletion or destruction of the personal data, and to access their data. They also have the writ of habeas data.

Data protection officers

DPOs or an equivalent function performed by a group of people are required under the Colombian framework to be responsible for the privacy practices of the organization. It may be located abroad but must be available to interact with the local authorities.

International transfers

Transfers of private or semi-private personal data must be authorized by data subjects and it are not allowed to jurisdictions that the Superintendence of Industry and Commerce (the Colombian DPA) regard as not providing adequate levels of protection. This is determined by DPA's Circular 5 of 2017.[81]

Exceptionally, beyond those cases, international transfers are allowed by Law 1.581: i) for medical, health and public hygiene reasons; ii) for exchange of financial information for transfers and banking operations; iii) pursuant to international treaties joined by Colombia; iv) for contracts involving the data subject and a counterpart; and v) when required by public interest.

Transfers to data processors

Transfers of personal data to third parties require the use of contractual or other means to protect it. Data controllers and data processors are jointly liable for data breaches.

Enforcement and sanctions

Violation of the personal data protection framework in Colombia may trigger investigations and audits by the authorities, authorities' orders, administrative fines, penalties and sanctions, as well as civil and criminal proceedings.

Sanctions foreseen in Law 1.581 of 2012, dealing with databases, are: i) fines of a personal and institutional nature up to the equivalent of two thousand (2,000) legal monthly minimum wages in

[81] See the full text of Circular No. 5 of 2017 by Colombia's Superintendency of Industry and Commerce at: http://suin-juriscol.gov.co/viewDocument.asp?ruta=Circular/30035611.

force at the moment of the imposition of the sanction (currently about $531,000 USD). The fines may be successive as long as the non-compliance that originated them persists; ii) suspension of activities related to the data processing up to a term of six months. In the act of suspension, the corrections that must be adopted will be indicated; iii) temporary closure of the operations related to the data processing once the suspension term has elapsed without having adopted the corrective measures ordered by the DPA; and iv) immediate and definitive closure of the operation that involves the processing of sensitive data.

In turn, Law 1.266 of 2008 contains the following sanctions for commercial and credit information: i) fines of a personal and institutional nature up to the equivalent of one thousand five hundred (1,500) legal monthly minimum wages in force at the moment of the imposition of the sanction (currently about $400,000 USD). The fines may be successive as long as the non-compliance that originated them persists; ii) suspension of activities related to the data processing up to a term of six months (with the suspension, the corrections that must be adopted will be indicated), and iii) temporary closure of the operations related to the data processing once the suspension term has elapsed without having adopted the corrective measures ordered by the DPA.

Notification of data breaches

Law 1.581 establishes a notification obligation to the DPA for both data controllers and data processors in the event of any security breach and risks in the management of personal data. There is no obligation to inform data subjects, but this is encouraged by the authority's guidance.

DPIAs and accountability

The Colombian DPA issued accountability guidelines for data controllers and data processors.[82] The Guidelines set out voluntary measures that they may take to demonstrate they have adopted effective and appropriate internal measures to guarantee that: i) there is an administrative structure directly proportional to the structure and size of the Data Controller within the organization; ii) there are internal mechanisms to implement the organizations' privacy policy and provide training to employees; and iii) to respond to requests from data subjects.

Furthermore, the DPA designed a personal data management program that organizations can follow where some of the key elements include the use of DPIAs and relevant governance components, under which boards and top managers are expected to be actively involved in developing, implementing and verifying compliance with data protection within the organization. Implementation of these measures may grant organizations a more lenient treatment by the authorities in case of breaches.

5. Mexico

Applicable rules

The Mexican data protection framework is composed of:

- The Constitution of the United Mexican States[83] (articles 16 and 73);

---

[82] See Colombia's Superintendency of Industry and Commerce (2017), Guía para la Implementación del Principio de Responsabilidad Demostrada, January 18, 2017, available at: www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf.

[83] See the full text of the Mexican Constitution at: www.oas.org/juridico/mla/en/mex/en_mex-int-text-const.pdf

- The Federal Law on Protection of Personal Data Held by Private Parties (effective as of July 6, 2010);[84]
- The Regulations of the Federal Law on Protection of Personal Data Held by Private Parties (in force since December 22, 2011);[85]
- The Federal Law on Transparency and Access to Public Government Information, of November 2002;[86]
- The Law on Protection and Defense of Banking Services Users, of January 1999;[87]
- The Federal Law on Consumer Protection, of December 1992;[88]
- The General Health Law, of February 1984;[89] and
- A large number of recommendations, guidelines and parameters that address a variety of specific issues, including security measures, the design and implementation of a privacy office or function.

Definitions

- Personal Data: any information that refers to an identified or identifiable individual including information of groups, such as customers and potential customers, employees, and others.
- Sensitive Personal Data: any data that may affect the privacy and intimacy of the data subject, including data that reveals racial or ethnic origin, present or future health conditions, genetic information, religious, philosophic or moral beliefs, union affiliation or sexual preference.
- Jurisdiction/Territoriality: the framework is applicable to any individual or entity having a legal domicile or local office or branch in Mexico, or when the managed databases are located in Mexico. However, data protection rules apply also to data controllers not based in Mexico, if they use means located within the Mexican territory for the processing of personal data.

Consent

Consent is generally required prior to the collection, processing and disclosure of personal data of a data subject, but there are exceptions.

Rights of individuals

Data subjects have the following rights regarding their personal data: information; access; correction; deletion and/or destruction, and the writ of habeas data.

---

[84] See the full text of the Law at: www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf.
[85] See the full text of the Regulation at: http://inicio.ifai.org.mx/English/2%20Regulations%20to%20the%20FLPPDHPP.pdf.
[86] See the full text of the Law at: www.oas.org/juridico/spanish/mex_res5.pdf.
[87] See the full text of the Law at: www.gob.mx/cms/uploads/attachment/file/174496/Ley_de_Protecci_n_y_Defensa_al_Usuario_de_Servicios_Financieros.pdf.
[88] See the full text of the Law at: www.profeco.gob.mx/juridico/pdf/l_lfpc_ultimo_camdip.pdf.
[89] See the full text of the Law at: https://wipolex.wipo.int/en/legislation/details/16107.

Data protection officers

In Mexico organizations are required to appoint a DPO or other individual to be accountable for data protection.

International transfers

International transfers require either information to the data subjects or their or consent, as well as the adoption of reasonable measures to ensure protection of the data at destination, which include transfer agreements.

Transfer to data processors

Transfer of personal data to data processors is allowed provided that contractual or similar measures are in place to safeguard the privacy of the data. Data controllers and data processors are jointly liable for data breaches.

Enforcement and sanctions

Violation of the personal data protection framework in Mexico may cause investigations or audits by the authorities, authorities orders, administrative fines, penalties or sanctions, as well as civil and criminal proceedings.

Notification of data breaches

Pursuant to the Mexican framework, breaches of personal data may have to be informed to the data subjects and the authorities, together with the adoption of additional measures to reduce the impact of the breach, depending on its extent and scope.

DPIAs and accountability

In Mexico, organizations are required to conduct data privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of personal data.

6. Peru

Applicable rules

The Peruvian framework for data protection is built from 3 main sources:

- The Political Constitution,[90] which recognizes the right to privacy;
- Law 29.733 of 2011, the Peruvian Data Protection Law;[91]
- Supreme Decree 003-2013-JUS,[92] the Regulation of Law 29.733;
- Legislative Decree 1.357 of 2017,[93] which creates the Transparency and Public Access to Information Authority and reforms Law 29.733, and
- Supreme Decree 019-2017-JUS,[94] the Regulation of Legislative Decree 1.357 of 2017.

---

[90] See the full text of the Peruvian Constitution at: www.oas.org/juridico/spanish/per_res17.pdf.

[91] See the full text of the Law at: www.informatica-juridica.com/ley/ley-no-29733-proteccion-datos-personales/

[92] See the full text of the Decree at: www.minjus.gob.pe/wp-content/uploads/2013/04/DS-3-2013-JUS.REGLAMENTO.LPDP_.pdf.

[93] See the full Tex of the Decree at: https://busquedas.elperuano.pe/normaslegales/decreto-legislativo-que-crea-la-autoridad-nacional-de-transp-decreto-legislativo-n-1353-1471551-5/.

[94] See the full text of the Decree at: https://busquedas.elperuano.pe/normaslegales/aprueban-el-reglamento-del-decreto-legislativo-n-1353-decr-decreto-supremo-n-019-2017-jus-1565834-5/.

Definitions

- Personal Data: any information regarding a natural person that identifies him/her or makes him/her identifiable through means that can be reasonably used.
- Sensitive Personal Data: includes biometric data, data related to racial and ethnic origin; income; opinions or convictions regarding politics, religion, philosophy or morality; union membership; and information related to health or sexual life.
- Jurisdiction/Territoriality: The Peruvian framework applies to personal data contained or intended to be included in databases whose processing is performed within the Peruvian territory.

Consent

In Peru the processing of personal data requires prior consent, which must be express. It is not required, however, for specific cases such as: i) in relation to a person's health or for medical emergencies; ii) for public health reasons; iii) when the data is publicly available or when it relates to the financial solvency or the creditworthiness of the data subject; iv) when needed for anti-money laundering and prevention of the financing of terrorism; or v) when related to the exercise of the right to freedom of information.

Rights of individuals

Data subjects have the following rights regarding their personal data: information; access; correction; deletion and/or destruction, and the writ of habeas data. These rights were revised in 2017 by Legislative Decree 1.357.

Data protection officers

Some organizations may be required to designate a DPO or other individual to be accountable for data protection.

International transfers

Transfers of personal data beyond Peruvian territory require consent from data subjects. Transfers can be conducted towards jurisdictions with similar levels of data protection as under the Peruvian framework and, subject to a privacy guarantee from the data controller, to jurisdictions with lower levels.

However, the following transfers are generally allowed: i) those taking place as part of an international cooperation agreement, for enforcement, intelligence, trade or the like; ii) those needed to execute a contractual relationship, medical treatment or a scientific or professional relation involving the data subject; and iii) those conducted for finance and securities trading. Notification to the DPA is required for international transfers.

Transfers to data processors

Transfers of personal data to data processors are allowed provided that they comply with the Peruvian framework. Upon completion of the processing data must be deleted by the data processor unless the data subject has expressly authorized otherwise.

Enforcement and sanctions

Violation of the personal data protection framework in Peru can result investigations or audits by the DPA, DPA orders, administrative fines, penalties or sanctions, as well as civil and criminal proceedings. The classification of violations between mild, moderate and severe was reformed in 2017 by Supreme Decree 019.

Notification of data breaches

The Peruvian framework does not require notification of a data breach to the authorities, nor to the affected data subjects.

DPIAs and accountability

DPIAs are not required in Peru and there are no specific accountability rules, but the law encourages data controllers and processors to adopt a code of conduct for data protection.

7. Uruguay

Applicable rules

The data protection framework in Uruguay is built around two main sources:

- Law 18.331 of 2008, on Personal Data Protection and Habeas Data Action;[95] and
- Decree No. 414/2009,[96] which regulates the Law.
- Law 19.670, of October 2018,[97] which amended Law 18.331.

Definitions

- Personal Data: any kind of information regarding identified or identifiable natural or legal persons.
- Sensitive Personal Data: data revealing racial or ethnic origin, political preferences, religious and moral beliefs, trade union membership and information regarding health or sex life.
- Jurisdiction/Territoriality: the Uruguayan framework applies when the data processor is located in Uruguay; when the treatment activities are related to the offer of goods or services addressed to inhabitants of Uruguay or with the analysis of their behavior; when provided for by rules of public international law or a contract, and when the processing uses means located in Uruguay, except if they are used exclusively for transit purposes and provided that the responsible for processing designates a representative, domiciled within Uruguay, before the DPA.

Consent

In general consent from data subjects is required for the collection and processing of personal data, with some exceptions, such as when: i) data is publicly available; ii) data is collected for the legitimate performance of a public function set by law; and iii) the data was obtained as part of a contractual relation scientific or professional relationship involving the data subject, and it is necessary for the rendering of the contracted services.

Rights of individuals

Data subjects have the following rights regarding their personal data: information; access; correction; deletion and/or destruction, and the writ of habeas data.

Data protection officers

Article 37 of Law 19.670, of October 2018, introduced relevant changes to Law 18.331. Among them, it established the requirement to appoint or designate a data privacy officer or other

---

[95] See the full text of the Law at: www.agesic.gub.uy/innovaportal/v/302/1/agesic/ley_n%C2%B0_18331_de_11_de_agosto_de_2008.html.

[96] See the full text of the Decree at: www.agesic.gub.uy/innovaportal/v/295/1/agesic/decreto-n%C2%B0-414_009-de-31-agosto-de-2009.html.

[97] See the full text of the Law at: https://legislativo.parlamento.gub.uy/temporales/docu3082693291176.htm.

individual accountable for the privacy practices of the organization, for all entities that treat sensitive data as a core business or deal with large volumes of data.

The functions of the DPO, as set in the law, are to: i) advise on the formulation, design and application of policies of personal data protection; ii) supervise the compliance with regulations on such protection; iii) propose all the measures that she deems pertinent to conform to the regulations and international standards on protection of personal data, and iv) act as a link between the entity and the DPA. The DPO appointed must meet some necessary conditions for proper performance of her functions and is to act with technical autonomy.

International transfers

Transfers are generally allowed to jurisdictions that comply with data protection levels required by Uruguay, as listed by the Uruguayan DPA.[98] The DPA may also authorize a transfer to a country not meeting those levels subject to a contractual guarantee from the data controller.

However, transfer are generally allowed when they are: i) conducted for international cooperation for enforcement or intelligence; ii) conducted for exchange of medical information as required by health or public hygiene; iii) needed for executing financing or securities transactions; are part of the framework of international treaties joined by Uruguay; and iv) consented by the data subject in its own interest, among others.

Transfers to data processors

Transfers of personal data to data processors are allowed. Upon completion of the processing data must be deleted by the data processor unless the data subject has expressly authorized otherwise.

Enforcement and sanctions

Violation of the personal data protection framework in Uruguay may give rise to observations and warnings by the DPA, administrative fines, suspension or prohibition of any data collection within the country, as well as civil proceedings.

Notification of data breaches

The Uruguayan framework requires notification of a data breach, with details about it and the measures taken by the data controller or processor, to the data subjects and the DPA. Notification must take place immediately after the responsible person becomes aware of the occurrence of the security breach. Law 19.670 of 2018, sets forth that a regulation will determine the content of the notification of security breaches.

DPIAs and accountability

Article 12 of Law 18.331, of 2008, as amended by Law 19.670, of 2018, establishes that those responsible for databases or processing of personal data, as well as the DPO, when applicable, will be held personally responsible for the violation of the provisions of the law. Further, it establishes that in the exercise of proactive responsibility, they must adopt the appropriate technical and organizational measures: privacy by design, default privacy and DPIAs, among others, in order to guarantee an adequate treatment of personal data and demonstrate its effective implementation.

The law delegates to a regulation the determination of the required measures according to the types of data, treatments and managers, as well as the opportunity to its revision and update.

---

[98] See Resolución N0. 4 of 2019 by Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales, available at: http://dof.gob.mx/nota_detalle.php?codigo=4652777&fecha=07/02/1984.

IV. Comparison and analysis

As shown in the preceding chapter, all jurisdictions analyzed have data protection frameworks in place. They all share certain key features, using similar definitions and conferring data subjects relatively the same rights. But they also differ in a good number of matters. Arguably, most of the differences stem from the date of adoption of the rules and regulations, with some jurisdictions having had the ability to keep their frameworks more updated than others. Some of those differences also reflect a degree of alignment with the stricter European model or the more flexible approach taken by the United States and promoted by APEC.

The European influence is explained in large part by trade agreements, which may impose compliance with certain key elements of the European framework on its counterparts. Within the region, the EU has concluded trade agreements with the Cariforum (comprising the 15 Caribbean Community states and the Dominican Republic), the Central America group (comprising Honduras, Nicaragua, Panama, Costa Rica, El Salvador and Guatemala), a multiparty trade agreement with Colombia, Ecuador, and Peru, as well as bilateral agreements with Mexico and Chile (both being renegotiated to be updated).

The sway of the EU's GDPR is visible in many of the existing frameworks and ongoing reforms. Both Brazil, with its recently adopted new law, and Chile, with its framework currently under legislative discussion, follow the European model to reshape their own. Uruguay, which has traditionally followed the European framework, has recently updated its rules to include the role of the DPO and accountability measures, ensuring they will remain recognized by the EU as being compatible with the GDPR standards. Interestingly, despite having a legal framework adopted many years ago, the Argentinian DPA, one of the pioneers of data protection in the region, has managed

to keep its rules updated to the European standards in order to be also recognized by the EU as eligible for international transfers of personal data under the GDPR.[99]

The influence of APEC's Privacy Framework is also visible in some jurisdictions that take a more flexible approach than that promoted by the GDPR, with a view to facilitating cross border flows of data and trade within the region. This model has worked well for trade and services with the U.S. and Mexico, Colombia and Peru have followed this approach to some extent.

With important parts of the U.S. currently moving towards higher levels of data protection, such as the State of California that will impose higher standards by January 2020,[100] the attractiveness of being regarded as compliant with the higher data protection requirements, to export data processing services worldwide in a globalized and digital economy, is likely to induce further convergence within the region.

Table 1
Selection of data protection measures of national frameworks

	Argentina	Brazil[a]	Chile[a]	Colombia	Mexico	Peru	Uruguay
Definitions of personal data and sensitive personal data	✓	only personal	✓	✓	✓	✓	✓
Extraterritoriality	✓	✓	×	✓	✓	×	✓
Consent requirements	✓	✓	✓	✓	✓	✓	✓
Rights of individuals (IACDdH)[b]	✓	✓	✓	✓	✓	✓	✓
Restriction to international transfers to jurisdictions	✓	×	×	✓	×	×	✓
Restrictions to transfers to data processors	✓	✓	✓	✓	✓	✓	✓
Sanctions	✓	✓	✓	✓	✓	✓	✓
Mandatory notification of breaches to authority and/or data subjects	×	×	×	to authority	✓	×	✓
Data protection authority	✓	×	×	✓	✓	✓	✓

Source: Author's elaboration.
[a] Brazil has adopted these measures under the scope of new law that will enter into force in 2020 and Chile has included some of them in the bill of law currently in Congress.
[b] Those considered in this table are the following I: information; A: access; C: correction; D: deletion; d: destruction, and H: habeas data.

Table 1, above, offers a simplified and generic description of some of the features of the national frameworks in force, as described in the preceding chapter. It obviously does not fully reflect the complexity of the national laws and regulations, or the many exceptions and special cases they consider, but may be useful as a summary of the regional landscape. It also serves to show the

[99] See the list of jurisdictions meeting the adequacy requirements as set by the EU at: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.
[100] See Ghosh, Dipayan, What You Need to Know About California's New Data Privacy Law, July 11, 2018, Harvard Business Review, available at: https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law.

important degree of coverage of data protection already achieved in some areas, and the scope for further convergence.

The following sections of this chapter will discuss some of these issues in more detail. They will focus on aspects of the data protection frameworks that relate to the corporate governance of companies and how they run their business within the playing field created by the regions' national data protection frameworks.

A. Corporate governance aspects

As discussed in the previous chapters of the report, some of the most advanced data protection frameworks in the world have begun to involve boards and senior managers in the responsibility for the design, implementation and supervision of company's data protection systems. This way, they raise the profile of data protection and enroll support from corporate decision-makers.

Table 2, below, simplifies and summarizes some of the features of the national data protection frameworks discussed in the previous chapter. It looks specifically for issues that have a relation to the corporate governance practices of companies. First, the appointment of a data protection officer (DPO), which pursuant to the GDPR model that many jurisdictions among the region have used as example, is set to help raise the status of data protection to the attention of the top managers and the board. Second, is the use of data protection impact assessments (DPIAs) and the responsible approach it imposes over those that manage databases and IT systems. Finally, measures related to the principle of accountability that establish that the design, implementation and supervision of data protection frameworks within companies should have direct involvement and responsibility of top managers and boards, which is present in the EU's GDPR and in the U.S. S.E.C.'s guidance.

Table 2
Selection of data protection measures related to corporate governance

	Argentina	Brazil	Chile	Colombia	Mexico	Peru	Uruguay
Mandatory DPOs	exceptionally	×	×	✓	✓	exceptionally	✓
Mandatory DPIAs	✓	×	×	recommended	✓	×	✓
Accountability	×	×	×	✓	×	×	✓

Source: Author's elaboration.
Note: Brazil has adopted some of these measures under the new law that will enter into force in 2020 and Chile has included some of them in the bill of law currently in Congress.

1. DPOs

Within the GDPR, DPOs are required for companies that have 'regular and systematic monitoring' of individuals at a large scale or when they process significant amounts of sensitive personal data. The functions of the DPO include facilitating compliance through the implementation of accountability tools and acting as intermediaries between relevant stakeholders.

The DPO is a management position but has to be independent, in a way that guarantees that she will be able to exercise its duties professionally without fear of dismissal and with enough resources to perform adequately. For the same reason, it is expected that the DPO will report directly to the highest level of the company and be a point of contact for employees and customers with complaints or concerns about the data protection practices of their organization.

The EU Guidelines for the appointment of DPOs under the GDPR, clearly state that DPOs are not personally responsible in case of non-compliance with the rules, because it is the controller or the processor who has responsibility for compliance. They have to enable the DPO to perform effectively by appointing a competent person and giving her sufficient autonomy and resources to carry out her tasks.[101]

As table 2, above, shows, the appointment of DPOs is currently only mandatory in Colombia, Mexico and Uruguay, among the jurisdictions analyzed in this report. It is further used in Argentina for audits and inspections and may be required in some cases in Peru.[102] While currently not in force, it is also included in the new Brazilian law that will enter into force in 2020 and considered in the bill of law being discussed by the Chilean Congress.

According to a forthcoming survey of companies within the Latin American and Caribbean region, currently being conducted by ECLAC,[103] preliminary results available at the time of writing this report show that about half of respondents have already appointed a DPO or someone responsible for data protection within their company. Another third of respondents say they have not yet done so, while the rest deem this not to be applicable to their companies.

Despite this apparent general adoption of DPOs within the region, some important differences appear when comparing the figure with its European counterpart, particularly in relation to the requirements for appointment and the scope of its duties. In Colombia, for example, data controllers and data processors have the choice to either appoint a person as DPO, or to identify a group of persons to be in charge of the company's data protection compliance program. The group could be a data privacy group or other area within the legal or compliance department.

Further, looking at the list of functions that the Colombian DPA suggests for the DPO in their accountability guidance, the function is quite focused to compliance and does not share some of the more complex features of the GDPR's version. The lack of direct line to the top of the organization and the absence of independence requirements, are important differences with the European version of the DPO. This somehow undermines the role the DPO can play in increasing the attention to data protection from the company's governance arrangements.[104]

Nonetheless, as previously discussed, regulations inspired in foreign rules need to adapt to the reality in which they are deployed, so perhaps this revised version of the DPO is what the Colombian data protection needs at this time. Some of the regional jurisdictions that are not yet

---

[101] See EU (2016) Guidelines on Data Protection Officers ('DPOs'), December 13, 2016, available at: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf.

[102] See Baker McKenzie (2018) Global Privacy and Information Management Handbook, available at: https://tmt.bakermckenzie.com/-/media/minisites/tmt/files/global_privacy_handbook-_2018.pdf?la=en.

[103] The full results of this survey will be made available by ECLAC after this report is completed. The questionnaire for the survey can be accessed at: https://icts-surveys.unog.ch/index.php/575779?lang=en.

[104] See Heidy Balanta, *La Figura del Oficial de Protección de Datos Personales en el Contexto Colombiano*, blog post at website DerechoInformatico.co, available at: http://derechoinformatico.co/la-figura-del-oficial-de-proteccion-de-datos-personales-en-el-contexto-colombiano/.

using this figure may want to consider these issues when implementing the role in their frameworks, as to use the DPO role to its full potential.

Under article 38(3) of the GDPR, controllers and processors are required to ensure that the DPO "does not receive any instructions regarding the exercise of [his/her] tasks," and that "whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner". The EU's DPO Guidelines explain that this means that, in fulfilling their tasks according to Article 39, "DPOs must not be instructed how to deal with a matter, for example, what result should be achieved, how to investigate a complaint or whether to consult the supervisory authority. Furthermore, they must not be instructed to take a certain view of an issue related to data protection law, for example, a particular interpretation of the law."

The Guidelines further explain that the DPO should be given the possibility to make his or her dissenting opinion clear to those making the decisions, if the controller or processor plans to adopt measures that are incompatible with the GDPR rules and the DPO's advice. Article 38(3) of the GDPR also requires that DPOs should "not be dismissed or penalized (…) for performing [his/her] tasks." This grants the function a degree of independence that many compliance and audit functions require to be able to escalate complex issues.

2. DPIAs

One of the important functions of DPOs under the GDPR is facilitating the conduction of data protection impact assessments, which are viewed by the European framework as an important accountability tool. Under the GDPR, a DPIA is a process designed to describe the processing, assess its necessity and proportionality, and help manage the risks it creates to the rights and freedoms of data subjects. The risks are assessed and measures to address them are determined in advance, and ideally in prevention, of an event that could put personal data at risk.

In practice, this means that controllers must continuously assess the risks created by their processing activities, in order to identify when a type of processing is likely to result in a high risk to the rights and freedoms of data subjects.[105] Within the European framework, DPIAs are thus conceived as accountability tools because they help controllers to comply with requirements of the GDPR and, in the event of a breach, they can also serve as means to produce evidence that appropriate measures were taken to achieve compliance. This may help demonstrate that the breach is not the result of mere negligence.

Table 2, above, shows that within the region DPIAs are mandatory in Argentina, Mexico and Uruguay, while recommended by the Colombian DPA. Brazil has adopted them in the new law not yet in force and they are foreseen in the bill of law currently discussed at the Chilean Congress.

Although the Mexican data protection framework does not mention DPIAs directly, it refers to the obligation by controllers to implement "a procedure to deal with the risk to the protection of personal data by the implementation of new products, services, technologies and business models, as well as to mitigate them."[106] As in the case of the GDPR, Mexican law makes DPIAs applicable for instances where new technologies or changes to existing systems are likely to result in increased

[105] See EU (2017), Guidelines on Data Protection Impact Assessment (DPIA), of April 4, 2017, available at: https://ec.europa.eu/newsroom/document.cfm?doc_id=47711.

[106] See article 44.V of the Regulations to the Federal Data Protection Law.

risk to the privacy or to the rights and freedoms of data subjects. In this sense, this regional version of DPIAs do not differ much from their European counterparts.

DPIAs seem to be a data protection tool that has adapted well into the region's national frameworks, but it may however be too early to assess whether it use has been effective, as there is little evidence about the results of their use in the available literature. The preliminary results of the abovementioned forthcoming survey by ECLAC suggest, for now, that the use of DPIAs may be quite limited in the region. When asked if their company understood when to conduct a DPIA and if it had developed procedures for doing so, only 19% of respondents said yes. Ten percent answered they were planning to do so. Forty three percent said they have not implemented or planned the use of DPIAs, and the rest deemed DPIAs were not applicable to them.

3. Accountability

The GDPR adopts the principle of accountability, by which organizations are required to put in place appropriate technical and organizational measures to protect personal data and be able to demonstrate what they did, and its effectiveness, when requested. Such measures include, among others, to document what personal data are processed, how, to what purpose and how long. Also, to document processes and procedures aiming at tackling data protection issues at an early stage, when building information systems or responding to a data breach.

In essence, as stated by the GDPR, the expectation is that companies will protect personal data in a way that ensures 'the ongoing confidentiality, integrity, availability and resilience of systems.' This is a task in which the GDPR expects boards of directors and senior managers to get personally involved, as it taps directly into the business model and strategy of the company.

Within the region, as shows in table 2, above, only Uruguay and Colombia currently foresee such a direct link in their national data protection frameworks. In the case of Uruguay, the accountability principle is reflected in article 12 of Law 18.331, which states that those in charge of databases and their treatment are responsible for the violation of the legal provisions. For this, the law defines that "in the exercise of proactive responsibility, they must adopt the appropriate technical and organizational measures: privacy from the design, default privacy, impact evaluation to data protection, among others, in order to guarantee an adequate treatment of the personal data and demonstrate its effective implementation."[107]

In Colombia, the principle of accountability is contained in Decree 1.377 of 2013, which regulates Law 1.581. It says that controllers must be able to demonstrate that they have implemented internal compliance policies that are proportional to: i) the organization's nature, structure and size; ii) the nature of the data that are being processed; iii) the kind of processing being conducted, and iv) the potential risks that such processing may cause. Controllers must also guarantee the adoption of mechanisms to implement the internal policies, including implementation tools, training and education programs, and the adoption of proceedings to answer any queries, petitions and claims made by data subjects.

[107] See article 12 of Law 18.331.

As mentioned already, Colombia's Superintendence of Industry and Commerce has issued an excellent Accountability Guideline[108] that aims to guide the efforts of the private sector on implementing accountability. The regulator is also empowered to recognize demonstrable compliance with such recommendations as an element to award a more lenient treatment in case of violations of the law.

As in the case of DPIAs, there is little literature reporting on the adoption of these measures or their impact where they have been adopted. The forthcoming survey by ECLAC may be able to shed some light on this, but its results are still inconclusive at the time of writing this document. Preliminary findings only show that across the region boards and senior managers of respondent firms seem to be perceived well prepared to discharge their duties regarding data protection. More than half of the companies declare having a data protection policy and one third has planned or is in the process of implementing one.

Asked if their board of directors oversees compliance with data protection policies and periodically review the effectiveness of data management and security controls, 43% of respondents to the survey answered yes. A further 19% said their boards plan to do that or are in the process of doing it. When required to assess if the board and senior management of their company understand the impact on the business of the risks related to personal data, and whether they are capable of managing them effectively, 47% responded in the affirmative. Twenty percent said they are moving in that direction, while the rest are roughly equally divided between those that do not deem this applicable to them, and those that have not yet planned or implemented this behavior.

Finally, in relation to the so-called '*tone from the top*', 38% of respondents declared that their board of directors and top management demonstrate support for data protection activities and promote a positive culture of compliance with data protection regulations across all areas of the business. Another 29% declared to have partially implemented such measures.

B. Cross border data transfer

As shown in the description of the national frameworks reviewed in this report and in table 1, transfer of personal data between jurisdictions in the region is far from a simple issue. Despite the fact that the GDPR has serve as source of inspiration for many data protection authorities, which have taken measures to prevent international transfers that could put data privacy of their own citizens at jeopardy, they have paid little attention to the fact that the GDPR rules first and foremost create a large block of countries within which data can flow safely and unencumbered. In the Latin American and Caribbean region, instead, each country has or is in the process of setting its own rules and mechanisms to define the requirements for international transfers of personal data.

[108] See Colombia's Superintendency of Industry and Commerce (2017), Guía para la Implementación del Principio de Responsabilidad Demostrada, January 18, 2017, available at: www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf.

Table 3
Authorization for international transfers of personal data

From: To:	Argentina	Brazil	Chile	Colombia	Mexico	Peru	Uruguay
Argentina		✓	✓	✓	✓	✓	✓
Brazil	×		✓	×	✓	✓	×
Chile	×	✓		×	✓	✓	×
Colombia	×	✓	✓		✓	✓	×
Mexico	×	✓	✓	✓		✓	×
Peru	×	✓	✓	✓	✓		×
Uruguay	✓	✓	✓	✓	✓	✓	

Source: Author's elaboration.

Table 3, above, shows the existence of general restrictions for transfers of personal data from one jurisdiction to another. The horizontal axis defines the originating country and the vertical axis, the recipient. It shows that Argentina, Colombia and Uruguay have restrictions on transfers to the other countries included in this study. Pursuant to their rules, those other jurisdictions are not yet generally regarded as having a level of data protection in line with their own. They are thus regarded as not offering sufficient protection for safe international transfers.

The fact that in the rest of the countries international transfers are generally allowed to other jurisdictions does not mean that transfers make take place at the will of the data controller, or that they are completely free. While in some cases there are no specific rules, in most cases frameworks impose obligations on data controllers that make the transfers to ensure they are directed towards jurisdictions with enough protection, making them accountable for the privacy of data transferred. In some other cases the rules require the consent of the data subjects prior to the transfer, or the signing of a transfer agreement. The approach taken in most instances is defined case-by-case.

In practice, this national approach to an international problem creates a maze that is difficult to navigate for companies operating across several of the region's jurisdictions, hindering trade and creating an uneven playing field. This is the exact opposite of what the GDPR was created for in Europe. It is obvious that the big difference is that in Europe they have created a continental union and institutions that, despite their difficulties, have been able to tackle complex issues like data protection in a collective manner.

The forthcoming survey being conducted by ECLAC hints, preliminary, that companies do perceive the lack of coordination within the national data protection frameworks in the region as a problem. Results available at the time of writing this report show that about half of the companies are subject to legal or regulatory restrictions for the transfer of personal data from one jurisdiction to another. From those, about two thirds assert that restrictions affect their ability to organize optimally to process and store personal data, while the rest declares that the restrictions do not have much effect on them.

C. Summary and conclusions

Within a context of advancing globalization and the economy turning digital at a fast pace, data have become an asset that more and more companies are exploiting. They can use them in ways that improve their ability to generate value and enhance their customers' experience. But in the process companies are also exposing personal data of customers, employees and others to the risks of theft and misuse, in the face of sprawling cybersecurity and privacy threats.

Those threats have prompted regulators and legislators all over the globe to pass rules or laws to establish or reinforce data protection frameworks. Some of these new rules have reserved a prominent role for the corporate governance frameworks of companies in data protection. They have assigned new privacy responsibilities to boards of directors and top managers in those firms, in the expectation this will provide sufficient incentives for them to take data protection seriously.

The most prominent example of this approach is the EU's General Data Protection Regulation (GDPR) adopted in April of 2016. It is generally regarded as the most advanced data protection framework in place and has an international reach, as it covers any organization that collects, controls, processes or uses data of any EU citizen, no matter where located. From a corporate governance perspective, the GDPR imposes new accountability and compliance obligations on data controllers and data processors, including the adoption of data protection policies, the use of data protection impact assessments (DPIAs), and the appointment of data protection officers (DPOs), among others.

The motivation for such new rules is that those that create risks over people's personal data should have the primary responsibility to mitigate them. This is achieved by tapping into the responsibility and duties of boards and senior managers, which are forced to pay attention to data protection to prevent the company to suffer consequences, if not to limit their own liability. Of course, this is something that competent boards and senior managers in many companies would have done anyway.

Good corporate governance principles dictate that the board is, by design, expected to identify and deal with risky issues and oversee management to ensure that they are mitigated in a way that can promote the sustainability of the company. Boards have to exercise control, supervision and set the risk appetite and tolerance for the organization, drawing their guidance from the mission, vision, and values of the company, which have to inform the strategy they define and help build the right corporate culture.

In the context of cybersecurity and data protection, the role of the board essentially involves asking the right questions (information), supporting the development of the necessary measures and policies (protection), ensuring proper disclosure (reporting), and keeping active oversight over the functioning of the framework (supervision). To improve their chances to preform adequately, boards may add skilled members, resort to training and create specialized board committees.

But as many surveys and reports listed throughout this paper show, while companies are significantly increasing their awareness of data protection, boards have a long way to go before being able to handle these issues with the same ease as they deal with financial risks. Data breaches are significant and privacy victims are counted in millions. There is a significant gap and a pressing need to address it, so regulators around the world are using the tools they have, to guide how companies are tackling cybersecurity and data protection in their jurisdictions.

Within the Latin American and Caribbean region, all jurisdictions analyzed in this paper have data protection frameworks in place that share key features, but also differ in significant matters. Most of the differences seem to be explained by the date of adoption of the respective frameworks and to some degree the influence of different international models, within a general tendency to move towards some convergence.

This implies that there is also a potential for regulation in the region to impose on boards and senior managers an express responsibility for the design, implementation and supervision of company's data protection systems. The analysis of the national frameworks currently in place proves that this has started but leaves ample room for further development.

The appointment of DPOs is already in use in some of the countries in the region, even if their attributes and duties are not tailored as within the GDPR, possibly to better adapt to local practices. DPIAs are also considered in some of the national data protection rules and may prove to become a useful tool, imposing a responsible approach on the management of databases and systems.

Further, only two jurisdictions covered in this report have so far adopted measures related to the principle of accountability. They expect direct involvement and responsibility of corporate leaders over the design, implementation and supervision of data protection frameworks within their companies. The approach is accompanied with guidance and a promise of leniency in the face of breaches, if companies can demonstrate meaningful compliance.

Perhaps the most complex area is that relating to the transfer of personal data between jurisdictions in the region. Unlike under the GDPR, the adoption of uncoordinated national rules has led a complex web of permissions, consents and restrictions. Companies operating across borders in the region find obstacles to an optimal organization of their data protection efforts, so existing international initiatives for harmonization should be supported.

This paper was set to describe and discuss the relation between cybersecurity and corporate governance, with a special interest on data protection in Latin America and the Caribbean. As shown in the preceding paragraphs, some jurisdictions have taken this direction, and there is undoubtedly a long road ahead for regulation to enhance data protection using the corporate governance framework of firms. There are good models, already influential in the region, and some surveys show that these issues are top concerns for corporate leaders, and there is a growing appetite for the development of coordinated benchmarks.

Bibliography

Abrahamian, Atossa Araxia, *Data Subjects of the World, Unite!*, The New York Times, May 28, 2018, available at: www.nytimes.com/2018/05/28/opinion/gdpr-eu-digital-privacy-law-data-subject-europe.html.

Accenture (2016), Bridging the technology gap in financial services boardrooms, by Richard Lumb, Mauro Macchi and Juan Pedro Moreno, 2016, available at: www.accenture.com/t20160118T152822__w__/us-en/_acnmedia/PDF-4/Accenture-Strategy-Financial-Services-Technology-Boardroom.pdf.

AICPA (2017), AICPA Unveils Cybersecurity Risk Management Reporting Framework, April 26, 2017, available at: www.aicpa.org/press/pressreleases/2017/aicpa-unveils-cybersecurity-risk-management-reporting-framework.html.

Baker McKenzie (2018) Global Privacy and Information Management Handbook, available at: https://tmt.bakermckenzie.com/-/media/minisites/tmt/files/global_privacy_handbook-_2018.pdf?la=en.

Corte Interamericana de Derechos Humanos, Herrera Ulloa vs. Costa Rica, ruling of July 2, 2004, available at: www.corteidh.or.cr/docs/casos/articulos/seriec_107_esp.pdf.

Deloitte (2017) Assessing cyber risk: Critical questions for the board and the C-suite, available at: www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-ra-assessing-cyber-risk.pdf.

_____ (2017), *Just 5% of FTSE 100 companies disclose having a board member with specialist technology or cyber experience*, Press Release, February 6, 2017, available at: www2.deloitte.com/uk/en/pages/press-releases/articles/just-5-of-ftse-100-companies-disclose.html#.

ECLAC (2005), Estado situacional y perspectivas del derecho informático en América Latina y el Caribe, by Erick Iriarte Ahon, available at: https://repositorio.cepal.org/handle/11362/31919.

_____ (2008), Meta 25 eLAC2007: Regulación en la Sociedad de la Información en America Latina y el Caribe, by Erick Iriarte Ahon, available at: https://www.cepal.org/socinfo/noticias/noticias/2/32222/GdT_eLAC_meta_25.pdf.

_____ (2018), Declaración de Cartagena de Indias, available at: https://conferenciaelac.cepal.org/6/sites/elac2020/files/cmsi.6_declaracion_de_cartagena.pdf.

EU (1995), Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

_____ (2016), Directive 2016/680 of the European Parliament and of the Council of 27 April 2016, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG& toc=OJ:L:2016:119:TOC.

_____ (2016), Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016 R0679.

_____ (2016), Guidelines on Data Protection Officers ('DPOs'), December 13, 2016, available at: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf.

_____ (2017), Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, April 4, 2017, available at: https://ec.europa.eu/newsroom/document.cfm?doc_id=47711.

EY Center for Board Matters (2017), The evolving role of the board in cybersecurity risk oversight, (July 2017), available at: www.ey.com/us/en/issues/governance-and-reporting/ey-the-evolving-role-of-the-board-in-cybersecurity.

Fernandez, Diego, Argentina Chapter, Data Protection & Privacy 2019, Seventh edition, Getting the Deal Through, available at: https://gettingthedealthrough.com/area/52/jurisdiction/4/data-protection-privacy-argentina/.

Gartner (2018), The 2018 CIO Agenda, by Kasey Panetta, October 27, 2017, available at: www.gartner.com/smarterwithgartner/the-2018-cio-agenda-infographic/.

Grigorescu, Catalin, *GDPR is mainly about corporate governance*, LinkedIN blog post, June 22, 2017, available at www.linkedin.com/pulse/gdpr-mainly-corporate-governance-catalin-grigorescu.

Ghosh, Dipayan, *What You Need to Know About California's New Data Privacy Law*, July 11, 2018, Harvard Business Review, available at: https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law.

Guadamuz, A, 'Habeas Data vs the European Data Protection Directive', 2001 (3) The Journal of Information, Law and Technology (JILT), available at: http://elj.warwick.ac.uk/jilt/01-3/guadamuz.html.

Guamán, Danny, *Privacy vs. Data Protection vs. Information Security*, Software and Services Engenieering Blog, November 1, 2016, available at: http://blogs.upm.es/sse/2016/11/01/privacy-vs-data-protection-vs-information-security/.

Iriarte, Erick, *Protección de Datos Personales y Acceso a la Información: Dos lados de la misma moneda*, La República, November 11, 2014, available at: https://larepublica.pe/tecnologia/833431-proteccion-de-datos-personales-y-acceso-a-la-informacion-dos-lados-de-la-misma-moneda.

Kan, Michael, *Yahoo execs botched its response to 2014 breach, investigation finds*, IDG News Service, March 2, 2017, available at: www.csoonline.com/article/3176181/security/yahoo-execs-botched-its-response-to-2014-breach-investigation-finds.html.

Kaspersky Lab (2018), From data boom to data doom: the risks and rewards of protecting personal data, available at: https://go.kaspersky.com/rs/802-IJN-240/images/Kaspersky_Lab_Business%20in%20a%20data%20boom.pdf.

Klemash, Steve W., et al, EY Center for Board Matters, *A Fresh Look at Board Committees*, Harvard Law School Forum on Corporate Governance and Financial Regulation, July 10, 2018, available at: https://corpgov.law.harvard.edu/2018/07/10/a-fresh-look-at-board-committees/#1.

LaCroix, Kevin, *Directors Beware: The EU's General Data Protection Regulation Is Upon Us!*, blog post, December 20, 2017, available at: www.dandodiary.com/2017/12/articles/uncategorized/guest-post-directors-beware-eus-general-data-protection-regulation-upon-us/.

Magliona, Claudio, Nicolás Yuraszeck and Carlos Araya, Chilean chapter, Data Protection & Privacy 2018, Seventh edition, Getting the Deal Through, available at: www.garciamagliona.cl/pdf/Getting_The_Deal_Through_2018_Data_Protection.pdf.

McKinsey Global Institute (2016), Digital Globalization: The New Era of Global Flows, March 2016, available at: http://ma.mckinsey.com/practicecrm/MGI/MGI_Digital_globalization_Full_report_March_2016.pdf.

Morgan, Steve, *Did Uber throw its CSO under the bus?, Cybersecurity Business Report*, CSO Online, November 28, 2017, available at: www.csoonline.com/article/3238708/regulation/did-uber-throw-its-cso-under-the-bus.html.

NACD (2017), Director's Handbook on Cyber-Risk Oversight (January 2017), available at: www.nacdonline.org/insights/publications.cfm?ItemNumber=10687.

Nasdaq Listing Rule 5250(b)(1), available at: http://nasdaq.cchwallstreet.com/nasdaq/main/nasdaq-equityrules/chp_1_1/chp_1_1_4/chp_1_1_4_4/chp_1_1_4_4_4/chp_1_1_4_4_4_10/default.asp.

Newcomer, Eric, *Uber Paid Hackers to Delete Stolen Data on 57 Million People*, Bloomberg, November 21, 2017, available at: www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data.

Nolter, Chris, *Uber's Rough Year Ends With Big SoftBank Investment*, The Street, December 29, 2017, available at: www.thestreet.com/story/14431727/1/uber-s-rough-road-leads-to-softbank-deal.html.

NYSE Listed Company Manual Rule 202.05 – Timely Disclosure of Material News Developments, available at: http://wallstreet.cch.com/LCMTools/PlatformViewer.asp?selectednode=chp%5F1%5F3&manual=%2Flcm%2Fsections%2Flcm%2Dsections%2F.

OAS, American Convention of Human Rights, available at: www.oas.org/dil/access_to_information_American_Convention_on_Human_Rights.pdf.

OECD (2013), The OECD Privacy Framework, available at: www.oecd.org/internet/ieconomy/privacy-guidelines.htm.

_____ (2015), G20/OECD Principles of Corporate Governance, available at: http://dx.doi.org/10.1787/9789264236882-en.

Ponemon Institute (2017), The Impact of Data Breaches on Reputation and Share Value, May 2017, available at: www.centrify.com/media/4737054/ponemon_data_breach_impact_study.pdf.

Ponemon Institute and IBM Security (2017), Cost of Data Breach Study: Global Overview, June 2017, available at: www.ibm.com/downloads/cas/ZYKLN2E3.

Ragan, Steve, *Equifax says website vulnerability exposed 143 million US consumers*, CSO Online, September 7, 2017, available at: www.csoonline.com/article/3223229/security/equifax-says-website-vulnerability-exposed-143-million-us-consumers.html.

Red Iberoamericana de Protección de Datos (2017), Standards for Personal Data Protection, available at: www.redipd.es/documentacion/common/Estandares_eng_Con_logo_RIPD.pdf.

Reeve, Tom, *Only 5% of FTSE companies have cyber-security expertise on the board*, SC Media, Feb 06, 2017, available at: www.scmagazineuk.com/5-ftse-companies-cyber-security-expertise-board/article/1475347.

Riley, Michael et al., *Understanding the Facebook-Cambridge Analytica Story: QuickTake*, The Washington Post, April 11, 2018, available at: www.washingtonpost.com/business/understanding-the-facebook-cambridge-analytica-story-quicktake/2018/04/11/071f8c84-3d97-11e8-955b-7d2e19b79966_story.html.

Rosemain, Mathieu, *France fines Google $57 million for European privacy rule breach*, Reuters, January 21, 2019, available at: www.reuters.com/article/us-google-privacy-france/france-fines-google-57-million-for-european-privacy-rule-breach-idUSKCN1PF208.

Russel Reynolds (2016), Digital Directors 2016: Diverse Perspectives in the Boardroom, 2016, available at: www.russellreynolds.com/en/Insights/thought-leadership/Documents/2016%20Digital%20Directors%20FINAL.PDF.

Shread, Paul, *Over Half of Companies Are Upping Spending on IT Security: eSecurity Planet Survey*, Posted February 6, 2019, available at: www.esecurityplanet.com/network-security/survey-2019-businesses-accelerate-spending-hiring.html.

Superintendency of Industry and Commerce (2017), *Guía para la Implementación del Principio de Responsabilidad Demostrada*, January 18, 2017, available at: www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf.

Southwell, Alexander H. et al, *Gibson Dunn Reviews U.S. Cybersecurity and Data Privacy*, The CLS Blue Sky Blog (Columbia Law School), February 3, 2017, available at: http://clsbluesky.law.columbia.edu/2017/02/03/gibson-dunn-reviews-u-s-cybersecurity-and-data-privacy/.

Spencer Stuart (2018), What Directors Think, 2018, available at: www.spencerstuart.com/-/media/2018/april/what-directors-think-2018.pdf.

Stempel, Jonathan & Jim Finkle, *Yahoo says all three billion accounts hacked in 2013 data theft*, Reuters Business News, October 3, 2017 , available at: www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1.

U.S. National Initiative for Cybersecurity Careers and Studies (NICCS) Portal's cybersecurity lexicon, available at: https://niccs.us-cert.gov/about-niccs/glossary#C

U.S. Securities and Exchange Commission (2018), Commission Statement and Guidance on Public Company Cybersecurity Disclosures of February 2018, available at: www.sec.gov/rules/interp/2018/33-10459.pdf.

UK Government (2017), FTSE 350 Cyber Governance Health Check Report, July 2017, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/635605/tracker-report-2017_v6.pdf.

UK ICO (2018), Information Commissioner's Office Guide to the General Data Protection Regulation (GDPR), August 2, 2018, available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/.

World Economic Forum, Global Risks Report 2017, 12th Ed., January 2017, available at: www.weforum.org/reports/the-global-risks-report-2017.

Zuckerberg, Mark, *A Privacy-Focused Vision for Social Networking*, Facebook Blog, March 6, 2019, available at: https://m.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/.

UNITED NATIONS

ECLAC

Series Production Development

Issues published

A complete list as well as pdf files are available at www.eclac.org/publicaciones

223. Corporate governance and data protection in Latin America and the Caribbean, Héctor J. Lehuedé (LC/TS.2019/38), 2019.
222. El financiamiento de la bioeconomía en países seleccionados de Europa, Asia y África: experiencias relevantes para América Latina y el Caribe. Adrián G. Rodríguez, Rafael H. Aramendis y Andrés O. Mondaini (LC/TS.2018/101) 2018.
221. The long-run effects of portfolio capital inflow booms in developing countries: permanent structural hangovers after short-term financial euphoria, Alberto Botta (LC/TS.2018/96) 2018.
220. Agencias regulatorias del Estado, aprendizaje y desarrollo de capacidades tecnológicas internas: los casos del Servicio Nacional de Pesca y Acuicultura y el Servicio Nacional de Geología y Minería de Chile, Rodrigo Cáceres, Marco Dini y Jorge Katz (LC/TS.2018/40) 2018.
219. Capital humano para la transformación digital en América Latina, Raúl L. Katz (LC/TS.2018/25), 2018.
218. Políticas de fomento productivo para el desarrollo de sectores intensivos en recursos naturales. La experiencia del Programa Nacional de Minería "Alta Ley", Jonathan Castillo, Felipe Correa, Marco Dini y Jorge Katz (LC/TS.2018/16), 2018.
217. El estado de la manufactura avanzada: competencia entre las plataformas de Internet industrial, Mario Castillo (LC/TS.2017/123), 2017.
216. Políticas para la atracción de inversión extranjera directa como impulsora de la creación de capacidades locales y del cambio estructural: el caso de México, Luz María de la Mora Sánchez (LC/TS.2017/122), 2017.
215. Bioeconomía en América Latina y el Caribe: contexto global y regional y perspectivas, Adrián G. Rodríguez, Andrés O. Mondaini y Maureen A. Hitschfeld, (LC/TS.2017/96), 2017.
214. Agenda 2030 para el Desarrollo Sostenible y sistemas alimentarios sostenibles. Una propuesta para la formulación de políticas integradoras, Adrián G. Rodríguez (LC/TS.2017/89), 2017.
213. Las empresas manufactureras de cobre en Chile, Lilia Stubrin y Joaquín Gana, (LC/TS.2017/64), 2017.

PRODUCTION DEVELOPMENT

Issues published:

223. Corporate governance and data protection in Latin America and the Caribbean
Héctor J. Lehuedé

222. El financiamiento de la bioeconomía en países seleccionados de Europa, Asia y África: experiencias relevantes para América Latina y el Caribe
Adrián G. Rodríguez, Rafael H. Aramendis y Andrés O. Mondaini

221. The long-run effects of portfolio capital inflow booms in developing countries: permanent structural hangovers after short-term financial euphoria
Alberto Botta

ECLAC
Economic Commission for Latin America and the Caribbean (ECLAC)
Comisión Económica para América Latina y el Caribe (CEPAL)
www.eclac.org