Privacy Series

14 DATA PROTECTION IN LATIN AMERICA

VEIRANO ADVOGADOS

This is the fourteenth chapter of the Data Privacy Series. Click here to access the chapter 13.

In 2023, the Brazilian General Data Protection Law (Law No. 13,709/2018 or "LGPD") celebrates 5 years of its publication - now also including the possibility of the application of administrative sanctions by the ANPD since August 2021. The Brazilian National Data Protection Authority ("ANPD") has been active in fostering discussions and disseminating concepts, practices and principles of privacy and data protection, through the publication of several materials for awareness and regulation of the LGPD since its creation.

Veirano Advogados has been following and participating in discussions regarding these issues. For this reason, our Data Protection & Privacy team has prepared the Privacy Series, in which we will periodically publish on different topics related to privacy, bringing not only LGPD concepts, but also ANPD publications on the subject, relevant considerations, among other contents.

1. Brazil

Applicable Law: Law No. 13,709/2018 (the "LGPD"). Entered into force on September 18, 2020, except for the administrative sanctions, which became enforceable as of August 1, 2021. The Brazilian legal landscape on privacy and data protection is complex and has specific sectoral laws, i.e. the LGPD needs to be interpreted as part of a system and not as an isolated law. Examples of laws complementary to the interpretation of the LGPD are: the Consumer Protection Code (Law No. 8,078/1990); the Telephone Interception Law (Law No. 9,296/1996); the Habeas Data Law (Law No. 9,507/1997); the Telecommunications Law (Law No. 9,472/1997); the Bank Secrecy Law (Complementary Law No. 105/2001); the Positive Registration Law (Law No. 12, 414/2011); Access to Information Law (Law No. 12,527/2011 and Decree No. 7,724/2012); the Civil Rights Framework for the Internet (Law No. 12,965/2014 and Decree No. 8,771/2016); the Code of Medical Ethics (Resolution No. 2,217/2018 of the Federal Council of Medicine; the Legal Framework for Artificial Intelligence (Bill No. 2,338/2023); CMN Resolutions No. 4,893/2021 and CMN No. 85/2021 of the Brazilian Central Bank, and Law No. 14,289/2022.

Data localization: While there are no general data residency/localization obligations, there may be such data residency/localization requirements if classified State information (not limited to personal data), or data related to the Federal Public Administration is processed. Moreover, Central Bank's Resolutions No. 4,893/2021 and No. 85/2021 provide certain data residency requirements for cloud service providers.

Appointment of a DPO: Until the ANPD provides more detailed instructions on the subject, it is assumed that every company (public or private) should appoint a DPO. This general obligation extends to all types of activities and volumes of data processing subject to the LGPD (as set out in the "Guidance on Processing Agents and DPO" published by ANPD in May 2021). Said obligation does not apply to small-sized data processing agents, which are allowed to solely provide a communication channel with the data subject under Resolution CD/ANPD N° 2/2022.

Regulator and enforcement:
Brazilian National Data Protection Authority - ANPD.

Breach notification: The controller must report to ANPD and the data subject within a reasonable timeframe if the breach is likely to result in relevant risk or harm to data subjects. The LGPD itself does not set a specific deadline for notifying the ANPD in the event of security incidents. However, according to guidance published by the National Authority on February 22, 2021, the communication must be made within two (2) working days, counted from the date of receiving knowledge of the incident. In addition, according to this guideline, the company or person responsible for the data must internally assess the incident and ascertain the nature, category, and number of data subjects affected. The ANPD must also be communicated in the event of relevant risk or damage to data subjects, using a form available on the ANPD's page (available here). Small-sized data processing agents may comply with the breach notification obligation in under a simplified procedure and with flexible deadlines to be provided by the ANPD under Resolution CD/ANPD N° 2/2022.

Fines: Data processing agents that commit infractions can be subject to administrative sanctions, in a gradual, single, or cumulative manner, including a fine, simple or daily, of up to 2% of the revenues of a private legal entity, group or conglomerate in Brazil, up to R$ 50 million per infraction.

Legislative updates: Bill No. 2338/2023 that aims to regulate artificial intelligence systems in Brazil, is currently on analysis by the Brazilian Senate and establishes rights for people affected by their operation, penalties for violations, as well as information regarding the supervising body. ANPD has already published a preliminary analysis (available here) indicating the points of convergence and conflict between the Bill and the LGPD.

2. Uruguay

Applicable Law:

Law No. 18,331/2008 (Law on the Protection of Personal Data and Habeas Data Action) and its Regulating Decree No. 414/009; Law No. 19,670/2018 (Accountability Act and Balancing of Budget Execution of the Exercise 2017) and its Regulating Decree No. 64/2020.

Data localization:

Under Decree N° 92/2014, computer systems of the Central Administration must be located in secure data centers in Uruguay, except in cases where there is no risk to the public entity in accordance with certain guidelines included in said Decree. Thus, except in cases where there is no risk, public entities of the Central Administration must keep their data in the country. Some additional limitations to keep the data abroad may apply to both private or public entities, depending on the activity of the company which orders the service of storage (data controller). For instance, institutions regulated by the Uruguayan Central Bank (UCB) may require prior authorization of the UCB if the storage of information is considered to fall within the concept of data processing from a banking law perspective. In those cases, there would need to be an analysis of whether the data processing abroad was substantial or not.

Appointment of a DPO:

Mandatory in the following cases: (i) public state or non-state entities; (ii) private or partially state-owned entities; (iii) private entities which process sensitive data as a core activity; and (iv) private entities which process large scales of data. Decree No. 64/2020 clarifies that large scales of data means the data processing of more than 35,000 subjects.

Regulator and enforcement:

Regulatory and Personal Data Control Unit (*Unidad Reguladora y de Control de Datos Personales* - URCDP). It is an autonomous entity of the Agency for the Development of Electronic Government and the Information-Based Society (*Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento* - AGESIC).

Breach notification:

Data breaches and data incidents must be reported to the URCDP and to the data subjects. Once the DPO or the data controller confirms the occurrence of a security breach, it must be notified to the URCDP within 72 hours (available here). Notification to data subjects must be done when their rights have been significantly affected once the DPO or the data controller confirms the occurrence of a security breach. Law No. 18,331/2008 requires the notification to be done "as soon as practicable" but fails to spell out a precise time frame for such notice. After the first notification to the Regulator within the first 72 hours after the breach, a second communication must be done by the DPO or the data controller to the URCDP. The second report must indicate all the details of what happened and the measures that were adopted and carried out so that such violation/incident has been mitigated and does not occur again. The Law does not state a time frame for execution of the second report.

Fines:

Warning, monitoring, fines up to USD 60,000, suspension of the data base during five days, and closure of the database.

Legislative updates:

The 2020 Decree established new obligations relating to breach notifications, Privacy by Design, DPO appointments, Data Protection Impact Assessments and security measures. Law No. 20075/2022 entered into force on 1st January 2023 and amends the Uruguayan data protection system, introducing amendments including disclosure to data subjects, as well as the powers of the URCDP.

3. Argentina

Applicable Law:
Personal Data Protection Act No. 25,326/2000 ("Act"); Personal Data Protection Regulatory Decree No. 1558/2001; International Personal Data Transfer Disposition No. E-60/2016; Resolution No. 47/2018, which sets forth the recommended security measures for the processing and retention of personal data in computerized and non-computerized media; Resolution No. 4/2019, which provides interpretation guidelines of Personal Data Protection Law No. 25,326/2000; Resolution No. 332/2020, which regulates the legal and technical aspects involved in audits conducted by the Argentinian Agency for Access to Public Information.

Data localization:
Under the Personal Data Protection Law No. 25,326, there are no specific requirements. However, other regulations do provide data localization requirements (e.g., Communication "A" 6354 issued by the Argentine Central Bank ("BCRA") allows financial entities to outsource Information Technology Services ("ITS") (e.g., Cloud Migration), provided that they do not contain information of clients and/or the general public. The Communication provides that certain documentation must be stored within Argentina (e.g., original copies of accounting books and records and debtors' profiles according to credit management regulations).

Appointment of a DPO:
Generally, there is no specific requirement to appoint a data protection officer. Under certain circumstances, in which special security standards apply, it may be necessary to appoint an officer in charge of data security.

Regulator and enforcement:
Agency for Access to Public Information – AIPP (*Agencia de Acceso a la Información Pública*).

Breach notification:
Not specifically required under data protection law unless the Argentinian Agency for Access to Public Information specifically requests information about data breaches. Therefore, the person responsible for the data must keep records on security breaches since these records may be requested by the Argentinian Agency for Access to Public Information. Failure to notify a data security breach is not in itself a violation of the data protection regime, but may bear on the effects of security violation, especially if lack of such notification results in other security breaches or damages.

Fines:
Warnings, suspensions, fines from AR$ 1,000 to AR$ 100,000 (approximately from USD 10 to USD 1,000 at the current official exchange rate), closure or cancellation of the files, registers, or database. Further, AIPP's Resolution No. 71/2016 establishes that, in case of recidivism, the applicable fines could be increased to up to AR$ 5 million (approximately USD 45,000 at the current official exchange rate), if the breach is qualified as a very serious offense. Violation of data protection rules may constitute a crime subject to prison terms imposed by criminal courts.

Legislative updates:
After a public consultation during September 2022, the AAIP published, on 10 November 2022, Draft Bill 87/2023 – currently on analysis by the Congress - that aims to update the Act and foster a framework that balances the protection of personal data with technological innovation and economic growth. Furthermore, the AAIP issued Resolution 4/2019, which specifies mandatory guidelines for the application of the Act, and addresses topics including video surveillance, automated data processing, consent, and biometric data. In addition, the AAIP issued, on 1st December 2022, Resolution 240/2022 amending Provision No. 9 of 19 February 2015 on the National Directorate for the Protection of Personal Data and No. 13 of 10 March 2015, which establishes the classification of offences under the Act respectively as minor, serious, and very serious, alongside the graduation of sanctions. Lastly, the AAIP issued, on 16 December 2022, Resolution No. 255/2022, regarding the processing of genetic data under the Act.

4. Chile

Applicable Law:

Law No. 19,628/1999 (the Chilean Data Privacy Act), altered by Law No. 21,214/2020; Law No. 20,575/2012 establishes the 'purpose principle' for the processing of personal data of an economic, financial, banking or commercial nature, as well as several rules that apply to the processing of personal data referring to financial, economic, banking or commercial information; Law No. 19,223/1993 establishes criminal sanctions for certain specific conduct related to the theft, destruction, obstruction, modification and illegal access and disclosure of information contained in data processing systems. It does not, however, refer specifically to personal data; Law No. 20,584/2012 sets forth that all information contained in patient files or documentations of medical treatments are sensitive data, and establishes the obligation of healthcare professionals to maintain patient data confidential and to comply with the principle of purpose limitation, and also includes certain specific cases in which such data can be submitted, partially or totally, to the data subject and to other individuals or entities. There are several other provisions on data privacy scattered throughout various bodies of law, including, e.g., the Chilean Labor Code, the Chilean Sanitary Code, Decree with the Force of Law No. 1 issued by the Chilean Ministry of Health in 2006 regarding health insurance, Act 19,799 on electronic signatures, Decree Law 3,500 issued by the Labor and Social Security Ministry in 1980 regarding the pension system, Decree with the Force of Law No. 3 issued by the Chilean Finance Ministry in 1997 regarding banks, the Updated Compilation of Rules issued by the Chilean Commission for the Financial Market etc.

Data localization:

Data localization requirements only exist in very limited cases of the banking industry, where local authorized banks are required to have local copies of the data.

Appointment of a DPO:

The Chilean Data Privacy Act does not require the appointment of a DPO.

Regulator and enforcement:

There is no special authority dedicated to overseeing matters related to data protection concerning processing activities performed by private persons or entities exists. Law 20,285/2008 on access to public information provides that the Chilean Transparency Council – CPLT (Consejo para la Transparencia, the control body to ensure compliance with the aforementioned law which provides the rights to transparency and access to information of the state administration) shall ensure proper compliance with the data protection law by the organs of the state administration; however, the Chilean Transparency Council does not have powers to impose fines. Since December 24, 2021, due to a provision in the newly adopted so-called Pro-Consumer Law (Law 21,398/2021), the consumer protection agency (Servicio Nacional del Consumidor - SERNAC) has the competency to monitor compliance with the provisions of the data protection law in consumer matters. The SERNAC cannot impose fines but may initiate and participate in judicial proceedings and collective voluntary proceedings. This is the first time that private controllers' processing of (consumer) personal data has been subject to regulatory control. A special data protection authority is to be created under the Bill that regulates the protection and processing of personal data and creates the Agency for the Protection of Personal Data (Bulletin 11,144-07, consolidated with Bulletin 11,092-07). To date, there is no clear timeline for when to expect this bill to pass.

Breach notification:

No obligation to report a data breach.

Fines:

Since there is no special data protection authority in Chile, data protection violations must be challenged with a Constitutional Protective Action based on an alleged violation of the constitutionally guaranteed right to protection of personal data, or with an action before the ordinary civil courts. In addition, the Chilean Data Privacy Act provides for a special type of action in the event that a controller fails to respond in a timely manner to a request to assert data subject rights ("Habeas Data"). With the entry into force of the Pro-Consumer Law and the competency thereby granted to SERNAC, consumers can lodge complaints alleging the violation of the data protection law to this authority. The SERNAC cannot impose fines but may initiate and participate in judicial proceedings and collective voluntary proceedings.

Legislative updates:

Bill No. 11144-07 regulating the Processing and Protection of Personal Data and Creating the Personal Data Protection Authority is under discussion in the Chilean Senate, which takes inspiration from the GDPR. In particular, the Bill would bring Chile in line with international standards by establishing rights for access, rectification, cancellation, or deletion of personal data, and data portability, as well as introducing new legal basis for data processing, and special categories of personal information. Bill No. 14847-06 establishes a Framework Law on Cybersecurity and Critical Information Infrastructure regulating public and private institutions that possess critical information infrastructure and establish requirements associated with responses to cybersecurity incidentes is currently under discussion in the Chilean Senate.

5. Colombia

Applicable Law:

Statutory Law No. 1,266/2008 regulates the processing of financial data, credit records and commercial information collected in Colombia or abroad,defines general terms on habeas data and establishes basic data processing principles, data subject rights, data controller obligations and specific rules for financial data. Law 1,266 was amended by Law No. 2,157/2021. Statutory Law No. 1,581/2012 regulates all personal data processing, as well as databases, defines special categories of personal data, including sensitive data and data collected from minors, regulates the obtention of authorization to treat personal data and the procedures for data processing, and creates the National Register of Data Bases ("NRDB"). Decree No. 1,377/2013 is a piece of secondary regulation related to Law No. 1,581 which outlines requirements for personal and domestic databases regarding authorization of personal data usage and recollection, limitations to data processing, cross-border transfer of data bases and privacy warnings and requires controllers and processors to adopt a privacy policy and privacy notice. Decree No. 886/2014 and Decree No. 090/2018 issued by the Ministry of Commerce, Industry and Tourism as well as the Resolution 090 of 2018 issued by the Superintendence of Industry and Commerce, regulate the NRDB and set deadlines for registration of existing data bases in Colombia.

Data localization:

There are no general data storage/localization obligations.

Appointment of a DPO:

Companies are required to appoint either a specific person, or a designated group within the company to be in charge of personal data matters, specifically the handling of data subjects' rights and privacy requests.

Regulator and enforcement:

According to Law No. 1,266, there are two different authorities on data protection and data privacy matters. The first of them, which acts as a general authority, is the Superintendent of Industry and Commerce (*Superintendencia de Industria y Comercio* - SIC). The second authority is the Superintendence of Finance (*Superintendencia Financiera de Colombia* - SOF), which acts as a supervisor of financial institutions, credit bureaus and other entities that manage financial data or credit records and verifies the enforcement of Law No. 1,266. Nevertheless, under Law No. 1,581, the SIC is the highest authority regarding personal data protection and data privacy, since it is empowered to investigate and impose penalties on companies for the inappropriate collection, storage, usage, transfer, and elimination of personal data.

Breach notification:

Both the data controller and the data processor shall notify the SIC in case of a breach of security, security risk, or a risk for data administration.

Fines:

SIC is allowed to investigate (as mentioned above), request information, initiate actions against private entities, and impose fines up to approximately USD 534,000, and order or obtain temporary or permanent foreclosure of the company, entity or business. Also, the Criminal Code of Colombia sets out in section 269F that anyone who, without authorization, seeking personal or third-party gain, obtains, compiles, subtracts, offers, sells, interchanges, sends, purchases, intercepts, divulges, modifies or employs personal codes or data contained in databases or similar platforms, will be punishable by 48 to 96 months of prison, and a fine of approximately USD 26,700 to USD 267,000.

Legislative updates:

There are no relevant legislative updates.

6. Mexico

Applicable Law:

Federal Law on the Protection of Personal Data held by Private Parties - FLPPDPP (*Ley Federal de Protección de Datos Personales en Posesión de los Particulares*), which entered into force on July 6, 2010. Subsequently, the Executive Branch has also issued the following: the Regulations to the Federal Law on the Protection of Personal Data held by Private Parties (*Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*), which entered into force on December 22, 2011; the Privacy Notice Guidelines (*Guía para Elaborar el Aviso de Privacidad*), which entered into force on April 18, 2013; the Recommendations on Personal Data Security, on November 30, 2013; the Parameters for Self-Regulation regarding personal data, which entered into force on May 30, 2014; and the General Law for the Protection of Personal Data in Possession of Obligated Subjects (*Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*), which entered into force on January 27, 2017

Data localization:

There are national security provisions, which state that information processed by governmental entities classified as national security and public information shall be stored within the facilities of the relevant public entities.

Appointment of a DPO:

All data controllers are required to designate a personal data officer or department (each, a Data Protection Officer) to handle requests from data subjects exercising their ARCO rights (access, rectification, cancellation, or objection) under the Law. DPOs are also responsible for overseeing and advising on the protection of personal data within their organizations.

Regulator and enforcement:

National Institute of Transparency for Access to Information and Personal Data Protection (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales - INAI) and the Ministry of Economy (Secretaría de Economía) serve as Mexico's data protection authorities.

Breach notification:

Security breaches occurring at any stage of the processing that materially affect the property or moral rights of the data subject must be promptly reported by the data controller to the data subject.

Fines:

Data subjects can enforce their ARCO rights, when no response is obtained from the data controller via INAI and ultimately the court system. If any breach of the Law or its Regulations is alleged, INAI may perform an on-site inspection at the data controller's facilities to verify compliance with the Law. Violations of the Law may result in monetary penalties or imprisonment, including the following: (i) INAI may impose monetary sanctions in the range of 100 to 320,000 times the Mexico City minimum wage (currently, MX $88.36, updated every year) - sanctions may be increased up to double the above amounts for violations involving sensitive personal data; (ii) three months to three years of imprisonment may be imposed on any person authorized to process personal data who, for profit, causes a security breach affecting the databases under its custody - penalties will be doubled if sensitive personal data is involved; and (iii) six months to five years of imprisonment may be imposed on any person who, with the aim of obtaining unlawful profit, processes personal data deceitfully, taking advantage of an error of the data subject or a person authorized to process such data. Penalties will be doubled if sensitive personal data is involved. The sanctions imposed by the INAI are without prejudice to any further civil or criminal liability.

Legislative updates:

There are no relevant legislative updates.

The Veirano Experience has a holistic, multidisciplinary, and business-oriented approach. In order to cover all the needs related to Compliance with LGPD, our Data Protection & Privacy team have developed several project formats, which comprise different scopes of work and meet specific demands of each client, whether national or international:

1. Full Compliance

With the performance of a multidisciplinary team, this project is aimed for clients whose goal is to identify and assess all ongoing processing activities within the company and based on that, identify vulnerabilities and structure an action plan for the creation of an effective privacy and data protection program based on legal, procedural, information security, and corporate governance pillars.

2. DPO as a Service

In this model, we take on the role of Data Protection Officer (DPO) on behalf of the client. To this end, we allocate a professional to perform the activities of managing and monitoring the client's data protection and privacy program.

3. M&A Legal Assistance

Designed to assist clients in the legal due diligence of merger and acquisition transactions, in order to identify relevant legal issues (red flags) and mitigate potential risks related to data protection and personal data security issues of the target company.

4. LGPD Pocket

A “pocket” advisory service for the adequacy of the activities and/or products developed by the company, regardless of its size or field of business, considering a reduced number of deliverables.

5. LGPD on Demand

LGPD On Demand is aimed at organizations that wish to have multidisciplinary advisory service on legal, information security, and corporate governance issues, with specific and timely action related to the protection of personal data.

6. LGPD Legal Helpdesk

The Helpdesk is designed to assist clients with LGPD legal consultations and demands within a monthly package of hours, either before, during, or after the initial compliance process.

7. Task Force For Security Incident Assessment And Reporting (VA Cybersecurity)

Specific and multidisciplinary legal advice in aspects related to the suspicion or occurrence of a security incident, in accordance with the most updated instructions from the ANPD and other applicable laws and regulations.

8. Representation in Administrative and Judicial Actions Involving Data Protection

Representation of clients in any administrative and/or judicial actions or potential actions involving data protection.

9. Analysis of Administrative and Judicial Decisions on Data Protection Matters

Periodic monitoring of decisions rendered in judicial and administrative proceedings involving the company or not, in order to present the authorities’ understanding and the impacts for the company or economic sector to the client in a summarized format.

10. Development and Updating of a Data Protection Impact Report

The ANPD may request from the controller to prepare a personal data protection impact report ("RIPD" or DPIA). Our team has expertise on the subject and can assist the company with the preparation and updating of the RIPD.

11. Development of Workshops

Development and application of training about the main concepts related to privacy and data protection to train its employees.

12. Playbook for Negotiating Commercial Contracts

Creation of playbooks for the negotiation of commercial contracts, to facilitate and speed up internal processes of commercial, technical, and legal teams.

13. Handbook to Reply the Data Subjetcs

Development of materials to assist the companies in prompt answering the data subjects' requests, as well as in the procedure to be followed by the company when answering the data subject, according to the business model developed by the company.

14. International Data Transfer

We help clients to understand the context of the international transfer, adapt it to the applicable legal basis, assess data localization requirements, add contracts, draft and review intra-group data sharing agreements, and generally respond to queries related to the harmonization of foreign with Brazilian regulations.

15. Privacy and Data Protection Auditing

We conduct audits to evaluate the company's level of maturity, presenting recommendations for risk mitigation.

16. Development and Review of Documents Pursuant to the Financial Sector

Our team has expertise in drafting security policies in accordance with the Central Bank's specific information security regulations, and in answering questions on the subject.

We are at your disposal in case of any questions or in the need of any additional information.

FÁBIO PEREIRA
+55 11 2313 5906
fabio.pereira@veirano.com.br

CINTIA ANDRADE
+55 21 3824 4655
cintia.andrade@veirano.com.br

DENISE LOUZANO
+55 11 2313 5912
denise.louzano@veirano.com.br

ISABEL HERING
+55 11 2313 5726
isabel.hering@veirano.com.br

PAOLA LORENZETTI
+55 11 99976 8480
paola.lorenzetti@veirano.com.br

CECILIA COUTINHO
+55 11 2313-4855
cecilia.silva@veirano.com.br

This material was last updated on August 18, 2023 and published on August 18, 2023. For more updated information please contact us.