COUNTRY COMPARATIVE GUIDES 2023

The Legal 500 Country Comparative Guides

Brazil

DATA PROTECTION & CYBERSECURITY

Contributor

Azevedo Sette Advogados

Ricardo Barretto Ferreira da Silva

Senior Partner | barretto@azevedosette.com.br

Lorena Pretti Serraglio

Coordinator | lserraglio@azevedosette.com.br

Bruna Evellyn Pereira Bigas

Associate | bbigas@azevedosette.com.br

Carolina Simioni Perdomo

Associate | cperdomo@azevedosette.com.br

Ingrid Bandeira Santos

Associate | isantos@azevedosette.com.br

This country-specific Q&A provides an overview of data protection & cybersecurity laws and regulations applicable in Brazil.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

BRAZIL
DATA PROTECTION & CYBERSECURITY

1. Please provide an overview of the legal and regulatory framework governing data protection, privacy and cybersecurity in your jurisdiction (e.g., a summary of the key laws; who is covered by them; what sectors, activities or data do they regulate; and who enforces the relevant laws).

The Brazilian Federal Constitution ("CF/88") sets forth the core principles of privacy and data protection. According to the CF/88, privacy, private life, honor, and image of individuals are inviolable, and the right to be compensated for economic and moral damages resulting from violation thereof is ensured. In February 2022, Constitutional Amendment No. 115 changed the Brazilian Constitution to insert in the list of article 5th, expressly, the data protection as a fundamental right.

Brazil enacted, in August 2018, the General Data Protection Act (Law No 13,709/2018 – "LGPD"), most provisions of which came into force in September 2020, following legislative and executive discussions on the issue. The articles that provide for the administrative sanctions applicable to non-compliance agents came into force in August 2021, through Law No. 14,010/2020.

LGPD provides a wide regulation for data protection, including collection, storage, registration, monitoring, processing, and disclosure of personal data processing agents. The LGPD requires that personal data processing activities comply with several principles, such as purpose, transparency, security, free access by the data subject, prevention of damages, and non-discrimination.

The ANPD has been acted by issuing numerous guidelines, all available on its website. Among them, we can highlight:

i. the Guideline on Definitions of Processing Agents and Data Protection Officer, explaining and bringing examples of these two figures defined by LGPD;
ii. the Guideline on How to Protect Your Data, aimed at the data subjects to explain the importance of the matter;
iii. the Guideline on Information Security for Small-Sized Processing Agents, which regulates the applicability of certain aspects of the LGPD on small-sized processing agents, such as the information security measures to be taken, administrative measures and other topics;
iv. the Guideline on the Application of LGPD on Processing Agents in the electoral context, to provide orientation on how to process personal data aiming at preserving data subjects' rights and the integrity of the electoral process, without obstructing the communication between candidate and citizen, which is necessary for the democratic process;
v. the Guideline on Data Processing by Public Agents to establish objective parameters, capable of providing legal certainty to transactions with personal data carried out by public entities;
vi. the Guideline on the use of Cookies, presenting a general overview of the subject, analyzing the main definitions and categories of cookies, examining the applicable legal hypotheses and the requirements to be observed in the use of cookies.

ANPD also updated its communiqué on data breaches, which includes provisions such as the concept of a data breach, actions that must be taken by the controller, recommendations for information in data breach notifications, recommended deadline for communication, a model form of notification to ANPD, among others.

In the first quarter of 2023, ANPD issued new Resolutions: Resolution No. 3/2023, establishing the Committee of Digital Governance of ANPD, of permanent nature and destined to discuss matters pertaining to implementation of digital government actions; and also the Resolution No. 4/2023, approving the Regulation on

How to Proceed with Application of Sanctions, .

In addition to all the specific data protection framework, Brazil also has legislation on Internet matters. Currently, one of the most important sectoral laws is the Brazilian Civil Rights Framework for the Internet (Law No. 12.965/2014, the "Internet Law") which establishes principles, guarantees, rights, and obligations for the use of the Internet in Brazil. Besides, Decree No. 8,771 of May 11, 2016, which regulates the Internet Law, sets forth the rules related to the request of registration data by public administration authorities, as well as the security and confidentiality of records, personal data, and private communications.

There are other sectorial laws and regulations concerning rights to privacy and data protection, including, but not limited to:

- Civil Code (Law No. 10,406/2002) grants general privacy rights to any individual and the right to claim against any attempt to breach such rights by any third party;
- Consumer Code (Law No. 8,078/1990) provides for the principles of transparency, information, and quality of data on its provisions;
- Positive Credit Registry Act (Law No. 12,414/2011) permits databases of 'positive' credit information (i.e., fulfillment of contracted obligations) but prohibits the registry of excessive information (i.e., personal data which is not necessary for analyzing the credit risk) and sensitive data;
- Complementary Law No. 166/2019 that amends the Positive Credit Registry Act, authorizing the inclusion of natural persons and legal entities in positive registration databases, without their prior request;
- Telecommunications Act (Law No. 9,472/1997) grants privacy rights to consumers about telecommunications services;
- Wiretap Act (Law No. 9,296/1996) establishes that interception of communications can only occur by court order upon request by police authorities and the Public Prosecutor's Office for purposes of criminal investigation or discovery in criminal proceedings;
- Bank Secrecy Act (Complementary Law No. 105/2001) requires that financial institutions (and similar entities) hold financial data of individuals and entities in secrecy, except under judicial order issued for purposes of investigation of any illegal acts or discovery in criminal proceedings;
- Resolution 3/2009 of the Internet Steering Committee in Brazil (CGI.br), establishes principles for ensuring privacy and data protection on the use of the Internet in Brazil, mainly regarding activities developed by Internet service providers;
- Resolution 124/2006 of the National Supplementary Health Agency imposes a fine on health insurance companies up to BRL 50,000 for the breach of personal information related to the health conditions of a patient;
- Law No. 13,989/2020 provides for the use of telemedicine during the COVID-19 crisis. The law for the use of telemedicine after the pandemic context is already being studied by the Federal Council of Medicine that intends to elaborate an ethical, technical, and safe law to provide adequate practice of telemedicine in Brazil, considering the privacy and data protection for both parties (patients and doctors).
- Resolution No. 1 of 2020 of the Brazilian Central Bank establishes the Pix payment arrangement (a system created by the Brazilian Central Bank that operate instant payments) and approves its Regulation that provides for the need to obtain formal consent from users for the registration of keys and use of the instant payment method.
- Joint Resolution of the Brazilian Central Bank and the National Monetary Council No. 5 of 2020. Provides for the implementation of Open Finance, which brings privacy and data security as one of the goals of Open Finance, and also imposes the need to obtain formal consent from users;
- Law No. 14,129/2021 provides for principles, rules, and instruments for Digital Government and the increase of public efficiency, and foresees data protection and privacy as a governmental principle, mentioning the compliance with LGPD.
- The PagTesouro digital platform, run by the National Treasury Secretariat of the Special Secretariat for Finance, offers a method of collecting fees due to various governmental offices and bodies, such as the Federal Supreme Court, some regulatory agencies and autarchies. With the novelty, the citizens have the option of making payments by Pix and by credit card, which are added to the existing modality of Federal Tax Liability Payment Form ("GRU") compensation. PagTesouro was established by Decree 10,494/20 as a digital platform for payment and collection of amounts to the National Treasury Single Account;

Brazilian Health Regulatory Agency ("ANVISA")'s Resolution 657/2022 provides for regularization of software as medical device (SaMD). It establishes that patients' data will be processed in accordance with data protection laws, only for the purposes set out in the resolution and as necessary for the evaluation of data on safety and efficacy of the product

2. Are there any expected changes in the data protection, privacy and cybersecurity landscape in 2023-2024 (e.g., new laws or regulations coming into effect, enforcement of any new laws or regulations, expected regulations or amendments)?

Yes. ANPD's Regulatory Agenda for 2023-2024, published through Ordinance 35/2022, in early November 2022, established the list of subjects expected to be regulated by the authority up to the end of 2024. The first subject of Stage 1 has already been regulated in early 2023: Regulation How to Proceed with Application of Sanctions, as mentioned above.

Stage 1 includes items that have already been initiated in 2021 and 2022. Stage 2 covers items the regulatory process of which are expected to take place within 1 year (i.e., until the end of 2023). Stage 3 is for items the process of which will take place within 1 year and 6 months (i.e., by mid-2024). Finally, Stage 4 includes items the process of which will take place within 2 years, i.e., by the end of year 2024, as follows:

STAGE 1		
Subject	**Description**	**Document**
Regulation of Dosimetry and Imposition of Administrative Penalties	Regulate the administrative sanctions for LGPD violations and the methodologies that will guide the calculation of the amount of the fine sanctions	Regulation
Data subject rights	Clarify how to guarantee the rights of data subjects, such as review of automated decisions	Regulation
Data breach notification	Regulate the deadline, standard template and the best way to forward the information to ANPD	Regulation
International transfer of personal data	Regulate the articles of the LGPD that deal with international data transfers	Regulation
Data Protection Impact Assessment (DPIA)	Issuance of regulations and procedures involving the matter.	Regulation
Data Protection Officer (DPO)	Issuance of complementary rules on the definition and attributions of the DPO, as well as hypotheses of waiver.	Complementary Rules
Legal basis for processing activities	Legal bases and hypotheses for the processing of personal data.	Guidance
Definition of "high risk" and "large scale"	Definition of these terms	Regulation
Sensitive personal data for Religious Organizations	Definition of basic measures for LGPD compliance for religious organizations	Document
Use of personal data for academic purposes and for studies by research organizations	Providing recommendations and guidance that can encourage the adoption of best practices and support the processing of personal data carried out for such purposes	Document
Anonymization and pseudonymization techniques	Clarification on the use of anonymization and pseudonymization techniques	Document
Regulation of the provisions of Article 62	This article determines the issuance of specific regulations for access to data processed by the Union for compliance with the Law of Directives and Bases for National Education and to data related to the National System for Evaluation of Higher Education	Regulation

STAGE 2		
Subject	**Description**	**Document**
Data Sharing by Public Authorities	Study that aims to operationalize Articles 26 and 27 of the LGPD, which deal with the sharing of government data with private entities, especially regarding the procedures to be adopted and the information to be sent to ANPD to comply with the provisions of the law	Technical Study
Processing of personal data of children and adolescents	Verify the possible techniques for checking consent or for checking the age of Internet application users; analyze the impacts of platforms and digital games on the Internet on the protection of children's and adolescents' data	Technical Study
Guidelines for the National Policy on Personal Data Protection and Privacy	Direct the actions of all actors involved in the data protection ecosystem, including the ANPD	Guideline
Regulation of criteria for recognition and disclosure of good practice and governance rules	Regulate criteria for the recognition and dissemination of good practice and governance rules to processing agents	Regulation

STAGE 3		
Subject	**Description**	**Document**
Sensitive Personal Data – Biometric data	Guidance on the contexts in which the collection of sensitive/biometric data would be legitimate	Regulation or Guideline
Security, technical and administrative measures (including minimum technical security standards)	Provision of minimum technical standards for processing agents to adopt technical and administrative security measures to protect personal data from unauthorized access and accidental or unlawful destruction, loss, alteration, communication, or any form of inappropriate or unlawful processing	Guideline
Artificial Intelligence	Issuing guidelines on the subject that will also serve as a basis for the development of other rules that may be necessary to discipline the AI system	Guideline or Technical Study
STAGE 4		
Subject	**Description**	**Document**
Conduct Adjustment Commitment (TAC)	In attention to the provisions of art. 55-J, XVII of the LGPD and art. 44 of Resolution CD/ANPD 1/2021, the Conduct Adjustment Commitment – TAC is an instrument that makes up the Inspection Process and the Sanctioning Administrative Process of the ANPD, allowing the interested agent to submit a proposal for agreement as an alternative to the regular progress of the sanctioning process.	Regulation

3. Are there any registration or licensing requirements for entities covered by these laws, and, if so, what are the requirements? Are there any exemptions?

The Brazilian data protection legislation, including LGPD, does not require any prior licensing or registration for data processing activity. On the other hand, companies are required to get licenses/authorizations to be issued by the competent regulatory agencies as regards, for example, the provision of telecommunication, banking, health, and other regulated activities/services. Those are the so-called regulated service sectors.

4. How do these laws define personal data or personally identifiable information (PII) versus special category or sensitive PII? What other key definitions are set forth in the laws in your jurisdiction?

The LGPD defines:

- Personal data as information regarding an

identified or identifiable natural person;
- Sensitive information as personal data concerning racial or ethnic origin, religious beliefs, political opinions, membership in trade unions or religious, philosophical or political organizations, data concerning health or sex life, genetic or biometric data, when related to a natural person.

Other key definitions are:

- Data subject: a natural person to whom the personal data object of processing refers;
- Data controller: a natural person or legal entity, of public or private law, responsible for making decisions about the processing of personal data;
- Data processor: a natural person or legal entity, of public or private law, that processes personal data in the name of the controller;
- Data protection officer: a person appointed by the controller and the processor, who acts as a channel of communication between the controller and the data subjects and the ANPD;
- Processing agents: data controller and data processor;
- Processing: any operation carried out with personal data, including, but not limited to, those concerning collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, deletion, assessment or control of information, modification, communication, transfer, dissemination or extraction;
- ANPD: agency of the public administration responsible for supervising, implementing and monitoring compliance with the LGPD.

5. What are the principles related to the general processing of personal data or PII. For example, must a covered entity establish a legal basis for processing personal data or PII in your jurisdiction, or must personal data or PII only be kept for a certain period? Please outline any such principles or "fair information practice principles" in detail.

Every processing activity of personal data shall observe good faith and the following principles, according to article 6 of LGPD: i) purpose; ii) adequacy; iii) necessity; iv) free access; v) quality of the data; vi) transparency; vii) security; viii) prevention; ix) non-discrimination; and x) accountability.

Also, the LGPD establishes in article 7 that the processing of personal data shall only be carried out in the following cases:

- By means of the data subject's consent;
- For compliance with the legal or regulatory obligations by the controller;
- By the public administration for the processing and shared use of data required for the implementation of public policies;
- For the conduction of studies by research entities, ensuring, whenever possible, the anonymization of personal data;
- When necessary for the performance of a contract or preliminary proceedings related to a contract to which the data subject is a party, at the request of the data subject;
- For the regular exercise of rights in judicial, administrative or arbitral procedures;
- For the protection of the life or physical safety of the data subject or a third party;
- For the protection of health, in procedures carried out by health professionals or sanitary entities;
- When necessary to serve the legitimate interests of the controller or of third parties, except in the event of the prevalence of fundamental rights and liberties of the data subject, which requires protection of the personal data;
- For credit protection including provisions of relevant legislation.

According to article 15 of the LGPD, the termination of data processing will occur: (i) when the purpose of the processing is achieved; (ii) at the end of the processing period; (iii) for fulfillment of legitimate request by the data subject; (iv) upon determination by ANPD, when a violation of the LGPD occurs.

Moreover, the storage of personal data after the processing is authorized for the following purposes, provided by article 16 of LGPD:

- Compliance with a legal or regulatory obligation by the controller;
- Study by a research entity, ensuring, whenever possible, the anonymization of the personal data;
- Transfer to third parties, provided that all legal requirements set forth in the LGPD are complied with;
- Exclusive use of the controller, with forbidden access to third parties, and provided the data

has been anonymized.

In addition, sectoral legislation, such as the Consumer Code, National Tax Code, Labor Legislation, among others, provide different rules regarding data storage.

Specifically for Internet applications, the Internet Law establishes that application service providers must keep records of Internet access (*i.e.*, the set of information regarding the date and time of use of a particular Internet application from a particular IP address) applications under secrecy, in a controlled and safe environment, for a minimum term of six months; and, in the provision of Internet connections, the autonomous system administrator shall keep records of the connection logs under secrecy for at least one year.

6. Are there any circumstances where consent is required or typically used in connection with the general processing of personal data or PII?

Consent is one of the legal bases provided for in the LGPD to process personal data and it has specific rules for its use. In the processing of personal data, consent must be a free, informed and unambiguous manifestation by the data subject for a specific purpose, given in writing or by another means that demonstrates his/her manifestation of will. On the other hand, the processing of sensitive personal data requires specific and highlighted consent, for specific purposes.

If consent is provided in writing, the contractual clause must appear highlighted from the other contractual clauses. Additionally, to process child and adolescent data as well, at least one of the parents or the legal guardian shall give his/her specific and highlighted consent.

Also, one of the mechanisms that allow international transfers is the specific and highlighted consent given by the data subject, with prior information about the international nature of the operation, being clearly distinct from other purposes.

In cases where the processing of personal data is based on consent, LGPD establishes that the consent can be revoked at any time by the data subject, using an express, free and facilitated procedure.

Finally, the LGPD also determines that the data subject can require the erasure of personal data processed with the data subject consent, unless the processing occurs under the following conditions, as per article 16 of LGPD:

- compliance with the legal or regulatory obligations by the data controller;
- studies by a research body, subject to the anonymization of personal data, whenever possible;
- transfer to third parties, subject to compliance with data processing requirements; or

for exclusive use by the data controller, with no access by third parties, and provided such data is anonymized.

7. What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

Article 5, XII, LGPD, typifies what the form of consent must be, establishing that the manifestation must be free, informed, and unequivocal, whereby the data subject agrees with the processing of his/her personal data for a specific purpose, as mentioned in question 6.

Therefore, consent must be:

- Free – the data subject cannot be obliged to give his consent, and consent cannot be established automatically, as in a checkbox already pre-selected.
- Informed – the data subject must understand exactly what he is consenting to, the information must be passed on in a complete, transparent and simple way.
- Unequivocal– there can be no doubt about acceptance by the data subject, and companies should strive to ensure this understanding.

Moreover, article 8 of LGPD establishes that consent must be provided in writing or by another means that demonstrates the data subject's manifestation of will.

At last, the LGPD does not specify in which type of document consent must be provided, but, § 4th of article 8 specifies that consent shall refer to specific purposes, and generic authorizations for processing of personal data are null and void. So, as a good practice, the recommendation is that it be incorporated into a specific document or in a highlighted form, so the data subject can have a complete understanding of the document, in compliance with the requirements of the LGPD.

8. What special requirements, if any, are required for processing sensitive PII? Are there any categories of personal data or PII that are prohibited from collection or disclosure?

According to the LGPD, it is not prohibited to collect and process sensitive personal information. However, the processing of sensitive personal data may only occur if the data subject or his/her legal representative consents, in a specific and highlighted way, for such specific purposes. Without the data subjects' consent, the processing of sensitive personal data must follow one of the legal bases listed below, whenever it is indispensable:

- For compliance with the legal or regulatory obligations of the controller;
- By the public administration for the processing and shared use of data required for the execution of public policies;
- For the conduction of studies by research entities, ensuring, whenever possible, the anonymization of personal data;
- When necessary for the performance of a contract or the regular exercise of rights in judicial, administrative or arbitral procedures;
- For the protection of the life or physical safety of the data subject or a third party;
- For the protection of health, in procedures carried out by health professionals or by health entities;

For the guarantee of the prevention of fraud and safety of the data subjects, in processes of identification and authentication of registration in electronic systems, observing the data subject rights, and except in the event of prevalence of fundamental rights and liberties of data subjects that require protection of personal data.

9. How do the laws in your jurisdiction address children's personal data?

According to the Child and Adolescent Statute (Law 8,069/1990 – "ECA"), children and adolescents have a peculiar condition of being in development. In this sense, the LGPD gives them stricter data protection set of rules and determines that the processing of personal data belonging to children and adolescents shall be done in their best interest, pursuant to the rules below and applicable legislation.

Accordingly, article 14 of LGPD sets forth the following rules to process children's and adolescents' personal data:

- The processing of children's and adolescents' personal data requires specific and highlighted consent of at least one of the parents or the legal guardian;
- When processing data based on consent, controllers shall keep public the information on the types of data collected, the way it is used and the procedures for exercising the rights established in the LGPD;
- Children's and adolescents' personal data may be collected without consent when it is necessary to contact the parents or legal guardian, used only once and without storage, or for the children's and adolescent´s protection. Under no circumstances shall the data be transferred to third parties without the proper consent;
- Data controllers shall not condition the participation of data subjects in games, Internet applications or other activities to the provision of personal information beyond what is strictly necessary for the activity;
- The controller shall make all reasonable efforts to verify that the legal guardian for the child or adolescent has given the consent, considering the available technologies;

Information on the processing of children's and adolescents' data shall be provided in a simple, clear and accessible manner, taking into account the physical-motor, perceptual, sensorial, intellectual and mental characteristics of the user, with the use of audiovisual resources when appropriate, to provide the necessary information to the parents or legal guardian and appropriate to the understanding of the child or adolescent.

10. How do the laws in your jurisdiction address health data?

Health data is considered sensitive data according to the LGPD. Therefore, health data can only be processed when an appropriate legal basis exists. It is worth noting that the LGPD prohibits the shared use of health data between controllers when the purpose is to obtain an economic advantage. Health Insurance Providers are also prohibited from processing health data for the practice of risk selection in the contracting of any modality, as well as in the contracting and exclusion of beneficiaries.

11. Do the laws include any derogations, exclusions or limitations other than those

already described? Please describe the relevant provisions.

According to article 4th of LGPD, this law does not apply to the processing of personal data:

- Carried out by a natural person for strictly personal and non-economic purposes;
- Carried out exclusively for journalistic, artistic, or academic purposes;
- Carried out exclusively for purposes of public safety, national defense, state security, or activities of investigation and prosecution of criminal offenses;
- Originated from outside the national territory and which are not the object of communication, shared use of data with Brazilian processing agents or subject to the international transfer of data with another country that is not the country of origin, provided that the country of origin has a level of personal data protection suitable for the provisions of LGPD.

12. Does your jurisdiction impose requirements of 'data protection by design' or 'data protection by default' or similar? If so, please describe the requirement and how businesses typically meet the requirement.

The LGDP establishes that processing agents shall adopt security, technical and administrative measures able to protect the personal data from unauthorized access and accidental or unlawful situations during the design phase of the product or service until its implementation.

The concept of privacy by default is implicit in the LGPD as companies are subject to the following principles, among others:

- Purpose: processing for legitimate, specific and explicit purposes, previously informed to the data subject, with no possibility of subsequent processing incompatible with these purposes;
- Necessity: limitation of the processing to the minimum necessary to achieve its purposes, covering data that are relevant, proportional and non-excessive in relation to the purposes of the data processing.
- Accountability: demonstration by the processing agents of the adoption of effective measures capable of proving compliance with the rules of personal data protection and its enforcement, including the effectiveness of such measures.

Business typically meet these requirements through an adequacy program, where they need to: i) keep records of personal data processing operations carried out by them; ii) prepare a Data Protection Impact Assessment ("DPIA"), with a description of the types of data collected, the methodology used for collection and for ensuring the security of information and the analysis by the controller regarding the adopted technical and administrative measures, safeguards and mechanisms of risk mitigation; and iii) adopt good practices of privacy and be transparent.

The ANPD may provide for minimum technical standards to render applicable the provisions of LGPD, taking into consideration the nature of the information processed, specific data processing characteristics and the available technology, in particular in the case of sensitive personal data.

13. Are owners/controllers or processors of personal data or PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so, please describe how businesses typically meet these requirements.

Both the controller and the processor must keep records of the personal data processing operations they carry out (article 37 of LGPD), especially when based on legitimate interest. Also, it is highly recommendable to the controllers and processors to have an updated data mapping, to present a Data Protection Impact Assessment (DPIA) whenever required, complying with the principle of accountability.

This topic was addressed by the ANPD in the Guideline of Definitions of Personal Data Processing Agents and Data Protection Officer, which it confirms the responsibility of both processing agents (controller and processor) to keep records of personal data operations.

This subject may be complemented by the LGPD Good Practices Guideline that will be issued by ANPD or in the Guidelines for the Rights of data subjects, both as a priority for regulation under the regulatory agenda 2023/2024 biennium by ANPD.

14. Do the laws in your jurisdiction require

or recommend having defined data retention and data disposal policies and procedures? If so, please describe these data retention and disposal requirements.

The LGPD determines, in article 15, that the termination of the processing shall take place when (i) in the event of verification that the purpose has been achieved or the data are no longer necessary or relevant to achieve the specific purpose; (ii) in the event of the end of the processing period; (iii) in case of data subject's notice to exercise his/her rights, including the right to revoke consent; or (iv) in the event of a decision of the ANPD, in case of violations of the LGPD.

Moreover, in article 16, LGPD specifies that personal data shall be erased after the end of their processing, except if (i) necessary to comply with the legal or regulatory obligations by the controller; (ii) for purposes of studies by a research body, subject to the anonymization of the personal data, whenever possible; (iii) to transfer to third parties, subject to compliance with data processing requirements, and; (iv) for exclusive use by the data controller, with no access by third parties and provided such data is anonymized.

Finally, these matters may be the object of further regulation by the ANPD. In the meantime, companies are adopting the best practices and observing compliance with the principles brought by LGPD in its article 6º.

15. When are you required to, or when is it recommended that you, consult with data privacy regulators in your jurisdiction?

There is no legal provision requiring or recommending consultation with regulators to process personal data. However, considering that the ANPD is in a solid performance, the referred Authority offers a "contact us" tab on its website, and it is possible to communicate in cases of (i) Filing a petition of the data subject against the data Controller; (ii) Lodge a complaint of non-compliance with the LGPD; (iii) Doubts about the LGPD; (iii) Personal Data Breaches; (iv) Sending invitations or documents to the ANPD; (v) Press; (vi) Ombudsman; (vii) Requests for access to Information based on the applicable law.

The website is available at: *https://www.gov.br/anpd/pt-br/canais_atendimento.*

16. Do the laws in your jurisdiction require or recommend conducting risk assessments regarding data processing activities and, if so, in what circumstances? How are these risk assessments typically carried out?

According to article 38 of LGPD, the ANPD may require that the controller must prepare a data protection impact assessment (DPIA), including sensitive data, referring to its data processing operations, per regulations, with due regard for trade and industrial secrets. The DPIA shall contain the description of all personal data processes that could generate risks to civil liberties and fundamental rights of the data subjects, as well as measures, safeguards and mechanisms to mitigate these risks.

Also, when processing is based on legitimate interest, it must be carried out under the processing of data strictly necessary for legitimate purposes, considered from concrete situations, therefore, the ANPD may request for the controller a data protection impact assessment (DPIA), provided by the article 10, §3º, of LGPD.

The ANPD held three technical meetings to discuss the data protection impact assessment (DPIA) in June 2021, and according to the ANPD regulatory agenda for the 2021/2022 biennium, the matter would be the object of a resolution that was scheduled for the first half of 2021. However, up to this point the ANPD has not yet issued a resolution on the topic that is as a priority for regulation under the regulatory agenda 2023/2024 biennium.

17. Do the laws in your jurisdiction require appointment of a data protection officer or a chief information security officer (or other person to be in charge of privacy or data protection at the organization), and what are their legal responsibilities?

According to the LGPD, the controller shall nominate a Data Protection Officer – DPO. The identity and contact information of the DPO shall be publicly disclosed, in a clear and objective, preferably on the controller's website. Although LGPD does not impose the nomination as an obligation to the processors, they also may appoint a DPO, according to article 5º, VIII.

The activities of the DPO consist of:

- Accept complaints and communications from data subjects, provide clarifications and adopt measures;
- Receive communications from the ANPD and adopt measures;

- Guide employees and contractors regarding the practices to be taken in relation taken about the privacy and data protection processes;
- Perform other duties determined by the controller or established in complementary rules.

In addition, the ANPD published the Guideline of Definitions of Personal Data Processing Agents and Data Protection Officer, which makes the following points:

i. The LGPD does not specifically determine in which circumstances an organization must appoint a DPO, adopting as a general rule that every organization must appoint a DPO;
ii. the LGPD does not determine whether the DPO should be a natural or legal person, an employee of the company, or an external agent. In any case, the guide indicates that the DPO must be appointed by a formal act;
iii. as a good practice, the DPO must have freedom in performing his duties, as well as knowledge of data protection and information security.
iv. The LGPD does not prohibit the DPO from having the support of a multidisciplinary data protection team.

ANPD may establish additional rules on the definition and duties of the DPO, including events of waiver of the appointment requirement, according to the nature and size of the entity, or volume of data processing operations.

This topic has been regulated by Resolution N. 2 of 27th January 2022, which regulates the application of the LGPD for Small-Sized Processing Agents. Processing agents that fit the criteria of the resolution may refrain from appointing a DPO, but if they do, it will be considered good practice. The criteria are budgetary according to the size of the company and material, whereby if the agent performs the high-risk processing, it will not be able to benefit from the referred Resolution.

18. Do the laws in your jurisdiction require or recommend employee training? If so, please describe these training requirements.

The LGPD provides that the DPO must educate the company's employees and contractors about governance and good data protection practices. Although the LGPD does not express the controller's obligation to raise awareness and train its employees, it is an indispensable measure for the compliance of the companies with the LGPD.

19. Do the laws in your jurisdiction require businesses to provide notice to data subjects of their processing activities? If so, please describe these notice requirements (e.g., posting an online privacy notice).

Yes. The data subject has the right to easy access to the information about the processing of his or her data, which should be provided in a clear, adequate and ostensible manner concerning it, including other aspects provided for in regulations for compliance with the principle of free access, per article 9° of LGPD, such as:

- The specific purpose of the processing;
- Form and duration of the processing, observing business and industrial secrets;
- Data controller identification;
- Information about the shared use of data by the controller and for which purpose;
- Responsibilities of the agents that will carry out the processing;
- Rights of the data subject, explicitly mentioning the rights provided in the LGPD.

If there is a change in specific purposes of the processing, type or duration of the processing, identification of the controller and information regarding the shared use of data, the controller shall inform the data subject, with a specific highlight of the content of the changes.

In the cases in which the legal basis of the processing is consent, whenever there are changes in the purposes of the processing of personal data that are not compatible with the original consent, the controller shall previously inform the data subject of the amendments of the purpose, and the data subject may revoke the consent whenever there may exist disagreements with the amendments.

Also, if the processing of personal data is a condition for the supply of a product, the provision of a service or the exercise of a right, the data subject shall be informed of this fact and of how the exercise of the rights outlined in the LGDP may be carried on.

The matter about data subject's rights is a priority for regulation under the regulatory agenda 2023/2024 biennium by ANPD, which might add some rules to the notice requirements imposed on businesses in Brazil.

20. Do the laws in your jurisdiction draw any distinction between the owners/controllers and the processors of personal data, and, if so, what are they? (For example, are obligations placed on processors by operation of law, or do they typically only apply through flow-down contractual requirements from the owners/controller?)

Yes, the LGPD defines controllers and processors as "processing agents" and distinguishes their concepts, in article 5º, items VI, VII and IX of LGPD. A data controller is a natural person or legal entity of public or private law that has the competence to make decisions regarding the processing of personal data and a data processor is a natural person or legal entity of public or private law that processes personal data on behalf of the controller.

Furthermore, LGPD foresees, in article 39, that the processor shall carry out the processing according to the instructions provided by the controller, which shall verify compliance with its instructions and the rules governing the matter.

The LGPD also sets the responsibility in its articles 42 to 45, of the controller or the processor who, as a result of carrying out activities of processing personal data, causes material, moral, individual, or collective damage to others, in violation of the aforementioned data protection legislation, shall redress/repair it.

The data processor is jointly liable for any damages caused by the processing if it fails to comply with the obligations of the data controller, or fails to follow the lawful instructions of the controller in which case the processor is deemed equivalent to the controller, except if they prove that:

- They did not carry out the processing of personal data that is attributed to them;
- Although they carried out the personal data processing attributed to them, there was no violation of the LGPD;
- The damage results from the exclusive fault of the data subject or any third party.

The controller or the processor who neglects to adopt security information measures foreseen in the LGPD shall be held liable for the damages caused by the violation of the data security, like data breaches.

21. Do the laws in your jurisdiction require minimum contract terms with processors of personal data or PII, or are there any other restrictions relating to the appointment of processors (e.g., due diligence or privacy and security assessments)?

There is no legal provision requiring minimum contract terms or other restrictions related to hiring service providers. Companies shall negotiate contract limits and restrictions between themselves. Nonetheless, the LGPD provides general guidelines related to security issues for data processors and data controllers.

Moreover, the ANPD addressed aspects of this issue in the Guideline of Definitions of Personal Data Processing Agents and Data Protection Officer such as the processor's obligation to sign contracts that establish, among other matters, the provisions of activities and responsibilities with the controller. Also, the LGPD establishes that this matter can be further regulated by the ANPD.

According to LGPD, the service providers (Controllers and Processors) may formulate rules for good practice and governance that set forth conditions of organization, procedures, complaints, and petitions for data subjects, technical standards, and specific obligations for the involved parties, among others, per the article 50 of the LGPD.

Also, when creating these rules, the controller and the processor should consider some items at the moment of the creation and implementation of good practice rules and data governance, regarding the data processing, such as nature, scope, purpose, probability, and the risks and benefits that will result from the processing of data subject's data.

According to ANPD regulatory agenda and planning, one of the priorities is education. The ANPD has undertaken to engage in dialogue with governmental and non-governmental bodies to produce guides and educational materials with best practice recommendations on personal data protection, as it has done up to this moment by publishing educational material and guidelines.

These discussions might also be reflected in the LGPD Good Practices Guideline, which shall be issued by the ANPD within one year, according to phase two of the ANPD's regulatory agenda 2023/2024 biennium.

22. Please describe any restrictions on monitoring, automated decision-making or

profiling in your jurisdiction, including the use of tracking technologies such as cookies. How are these terms defined, and what restrictions are imposed, if any?

In attention to the principle of transparency, provided for in article 6º, item VI of the LGPD, the controller must inform the data subject about the use of tracking technologies on its websites and/or applications, explaining what each of them is for.

Concerning automated decision-making and profiling, LGPD grants data subjects the right to request a review of decisions solely taken based on automated processing of personal data that affects their interests, including decisions intended to define their personal, consumer, and credit profiles or aspects of his/her personality.

In the specific case of Cookies, the Regulatory Authority published in October 2022 a guideline on the use of cookies and the protection of personal data, the document brings important recommendations on how cookies should be used.

In this regard, based on the principles of the LGPD, especially purpose, necessity, adequacy, free access, and transparency, the document lists several guidelines:

- Ensuring a high level of transparency to the data subjects, with clear and complete privacy notices and policies;
- Provision of information on how the user can manage cookies, guiding that the websites contain tools for changing preferences about cookies in a practical and easy way;
- Classification of cookies according to their purposes. Although other classifications may be adopted, the guide classifies cookies into categories (application, need, purpose and retention time), also the same cookie may be inserted in more than one category.

The guide has also provided information regarding the appropriate legal basis for processing of each data collected. The classification of the cookie will directly reflect the purpose of the data being processed and the legal basis authorizing the data processing carried out through the cookies.

Regard to data collection by advertising cookies, the guide states that the most appropriate legal basis is “consent.” Such guidance implies measures that must be taken by those responsible for the websites in order for the collection of consent to be carried out properly and in compliance with the LGPD. Generic authorizations commonly collected through “agree”, “accept” or “aware” buttons do not represent valid consent.

The guide also provides the possibility of applying the legal basis of legitimate interest of the controller, taking into account the use of necessary cookies.

Another point of great relevance concerns the layout and configuration of the cookie management tool. The guide directs that this tool be arranged in a system of “banners” in levels, in which the first level offers more general options such as “reject cookies that are not necessary” and the second level enables detailed understanding and specific management of cookies by the user.

23. Please describe any restrictions on targeted advertising and cross-contextual behavioral advertising. How are these terms or related terms defined?

Behavioral advertising is advertising delivered through the use of data and information from the data subject. This can be demographic data, economic status, gender, age, employment, lifestyle, interests, purchase history. Personalization of ads is possible as a result of online monitoring. LGPD does not prohibit behavioral advertising, but creates mechanisms and principles so that it does not become unlawful. Therefore, the principles established in the LGPD will guide how processing agents will perform behavioral advertising.

The practice of behavioral advertising cannot go against the guarantees provided in article 2º of the LGPD:

- Right to privacy;
- Informational self-determination;
- Freedom of information and communication;
- Inviolability of privacy, honor and image and the free development of personality.

Therefore, Article 18 establishes the need for security and transparency in data processing, guaranteeing rights that the data subject can exercise. We await further definitions on the subject by the ANPD, so that the LGPD can be applied more objectively and with clear recommendations.

In addition, The Internet Law, in article 7, determines a need to provide clear and complete information for the processing of personal data.

Moreover, the Consumer Code, in its article 36, establishes that advertising should be conveyed in a way that the consumer immediately understands that it is an advertisement.

Although in Brazil there is no express regulation about behavioral advertising, the requirements outlined in Brazilian laws must be respected.

Also in this regard, the cookie guide published by the ANPD should be taken into consideration, advising the user how to manage them, as well as offering the owner the possibility to refuse cookies that are not necessary for navigation and informing them that it is possible for cookies to be deleted or disabled is a good practice that can be carried out through banners on the web page or detailed in privacy policies or notices.

24. Please describe any laws in your jurisdiction addressing the sale of personal data. How is "sale" or related terms defined, and what restrictions are imposed, if any?

There are no specific determinations regarding the sale of personal information in Brazilian jurisdiction. But in all cases, the provisions of the LGPD must be respected, including the existence of an appropriate legal basis for the processing. It is worth noting that public entities fined companies that were commercializing personal data in the near past, as they did not have express authorization from the data subjects to sell their data. Consent was considered, in this particular case, the legal basis necessary to legitimate the processing, which was not collected.

25. Please describe any laws in your jurisdiction addressing telephone calls, text messaging, email communication or direct marketing. How are these terms defined, and what restrictions are imposed, if any?

The National Telecommunication Agency ("Anatel") approved, through Act No. 10.413, the obligation for telephone operators to use the code 0303 at the beginning of the number of any call for marketing purposes. This standardization aims to allow the data subject to identify telemarketing calls, avoiding unwanted calls. The procedure was approved by Anatel in 2021 and entered into force in March 2022.

Additionally, there are public opposition lists created by state laws in Brazil where the individual/data subject can subscribe to indicate he/she does not want to receive marketing communications via telephone calls and SMS. These lists are monitored by the Procon (Consumer Protection Office) from each state, and the obligation to observe the lists applies to controllers and processors that use these means to send advertising of their products and services to individuals whose area codes are from states that adopt official opposition lists.

Notwithstanding, all communications with the data subject for marketing purposes must comply with the principles and good practices established by the LGPD, as well as with the Consumer Code that contains provisions that grant overall consumer protection against, among other topics, abusive marketing in advertising products and services.

Finally, the LGPD does not define the term "direct marketing", nor does it bring specific responsibilities in its text for this type of advertising. Thus, to carry out direct marketing, the controller must observe the particularities of the processing activity and ensure compliance with the LGPD legal provisions, especially concerning the data subject's rights and their legitimate expectation of receiving specific advertisements content.

26. Please describe any laws in your jurisdiction addressing biometrics such as facial recognition. How are these terms defined, and what restrictions are imposed, if any?

The LGPD foresees biometrics data as a sensitive category of personal data. The LGPD considers as sensitive any data related to racial or ethnic origin, religious beliefs, political opinions, membership of trade unions or religious, philosophical or political organizations, data concerning health or sexual life, genetic or biometric data, when related to a natural person.

The processing of biometric data shall observe the specific list of legal bases (article 11) and other provisions, because of the high risk that the processing of this category of personal data poses to data subjects' fundamental rights.

There is still no specific law about facial-recognition in Brazil, but there are some Bills under discussion by the House of Representatives.

One of these, is Bill No. 2537 of 2019, which obliges all commercial establishments that use facial recognition software to alert consumers with signs or stickers fixed at the entrance of their facilities. If approved by the House of Representatives, this Bill will be submitted to the Federal Senate for analysis.

Others are Bills No 4612/2019 and 4901/2019, which

were joined to PL 12/2015 that intends to regulate the development, application, and use of facial and emotional recognition technologies, as well as other digital technologies aimed at the identification of individuals and behavior prediction or analysis. This project is still proceeding in the House of Representatives and, if approved, has the potential to complement the provisions of biometric data in the Brazilian legislation, in special, LGPD.

The most recent bill presented on this matter is Bill No. 2392/2022, presented in August 2022, which provides for the use of facial recognition technologies in the public and private sectors. The idea of the Bill is to prohibit the use of facial recognition technologies for identification purposes in the public and private sectors without a prior report on the impact on people's privacy – Data Protection Impact Assessment (DPIA). The bill is currently in the House of Representatives.

27. Is the transfer of personal data or PII outside the jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism? Does a cross-border transfer of personal data or PII require notification to or authorization from a regulator?)

LGPD regulates the transfer of data outside the jurisdiction in articles 33 to 36. The international transfer of personal data is only allowed in the following cases:

- To countries or international organizations that provide a level of protection of personal data that is adequate to the provisions of the LGPD;
- When the controller offers and proves a guarantee of compliance with the principles, rights of the data subject and the regime of data protection established in the LGPD, in the form of:
    a. Specific contractual clauses for a given transfer;
    b. Standard contractual clauses;
    c. Global corporate rules;
    d. Regularly issued stamps, certificates and codes of conduct;
- When the transfer is necessary for international legal cooperation between public intelligence and investigation bodies, per instruments of international law;
- When the transfer is necessary for the protection of the data subject's or a third party's life or physical safety;
- When the ANPD authorizes the transfer;
- When the transfer is the result of a commitment assumed in an international cooperation agreement;
- When the transfer is necessary for the execution of a public policy or legal attribution of public service;
- When the data subject has provided specific and highlighted consent for international data transfer, with prior information about the international nature of the operation, with this information being clearly distinct from other purposes;
- For compliance with the legal or regulatory obligation by the controller, when necessary for the performance of a contract or preliminary proceedings related to a contract to which the data subject is a party, at the request of the data subject and for the regular exercise of rights in judicial, administrative or arbitral procedures.

Although the articles related to international data transfer of LGPD is in full force since September 2020, the efficacy of some of its provisions requires regulation by the ANDP, what is expected for the coming years.

28. What security obligations are imposed on personal data or PII owners/controllers and on processors, if any, in your jurisdiction?

The LGPD establishes that processing agents shall adopt security, technical and administrative measures able to protect personal data from unauthorized access and accidental or unlawful situations of destruction, loss, alteration, communication or any type of improper or unlawful processing.

The controllers and processors shall ensure the security of the information as provided in the LGPD, even when the processing is over. Besides, the software or systems used for processing personal data shall be structured to comply with the security requirements, standards of good practice and governance, general data protection principles and other sectorial regulatory rules.

Also, the Internet Act provides security requirements for internet service providers. Decree 8.771/2016 provides the security standards for handling personal data and private communications, as follows:

- Definition of responsibilities and

authentication mechanisms to ensure individualization of the persons who will have access to and handle data, as well as detailed access logs;
- Creation of detailed inventory of access to connection records and access to applications containing time, duration, the identity of the designated employee or individual responsible for the access in the company and the accessed file; and
- Management solutions of records through techniques that ensure the inviolability of data, such as the use of encryption or equivalent protection measures. The safeguard and availability of connection logs and access data, as well as personal data and the content of private communications, must meet the security requirements to preserve intimacy, privacy and image of the parties directly or indirectly involved.

29. Do the data protection, privacy and cybersecurity laws in your jurisdiction address security breaches, and, if so, how does the law define "security breach"?

ANPD defines a security breach as a confirmed adverse event that compromises the confidentiality, integrity or availability of personal data. It may arise from voluntary or accidental actions that result in disclosure, alteration, improper loss, or unauthorized access to personal data, regardless of the medium on which it is stored.

It is important to remember that not every security incident involves personal data. Incidents that involve only anonymized data or do not relate to identifiable natural persons do not need to be reported to the ANPD.

30. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecoms, infrastructure, artificial intelligence)?

There are several sectorial laws and regulations concerning security requirements for specific regulated sectors and industries, such as, but not limited to:

- The Internet Law, which provides security requirements for internet service providers, and Decree 8.771/2016, which provides security standards for handling personal data and private communications for internet service providers;
- Cybersecurity Regulation Applied to the Telecommunications Sector of the National Agency for Telecommunications – ANATEL which aims to establish conducts and procedures for the promotion of security in telecommunications networks and services, including cybersecurity and the protection of critical telecommunications infrastructures. The regulation was approved on December 17, 2020 and is in force since January 4, 2021, with a 180-day deadline for adequacy and implementation of service provider companies.
- Decree 9.637/2018, which institutes the National Information Security Policy and provides for the governance of information security, and the Normative Ruling 4/2020 of the Institutional Security Office, which provides on the minimum requirements cyber security requirements to be adopted when establishing 5G networks;
- Complementary Law 105/01, which provides for the secrecy of operations in financial institutions, the Resolution 3.380/06 of the Brazilian Central Bank (BACEN), which provides for the implementation of an operational risk management structure for financial institutions, and the Resolution 4.658/2018 of BACEN , which provides on the cyber security policy and the requirements for hiring data processing and storage services and cloud computing to be observed by financial institutions and other institutions authorized to operate by BACEN;
- Provisional Measure No. 2.200-2/01, establishes the Brazilian Public Key Infrastructure – ICP-Brazil, to ensure the authenticity, integrity and legal validity of documents in electronic form, support applications and qualified applications that use digital certificates, as well as secure electronic transactions;
- Circular 249/04 and 285/05 of the Superintendence of Private Insurance – SUSEP, which determine internal controls of activities and information systems insurance companies, capitalization companies and public pension entities and establish information security policy requirements, as well as Circular 599/2020 of SUSEP, which establishes that the request for accreditation by an entity registering insurance operations, open supplementary pension, capitalization and reinsurance must present an executive summary of data secrecy and cyber security policies and a declaration that these policies comply with the legislation and regulations in

force;
- Resolution 656/15 of the National Telecommunications Agency (Anatel), which establishes standards on Risk Management of Telecommunications Networks and Use of Telecommunications Services in Disasters, Emergency Situations and Public Disaster;
- NBR ISO/IEC 27001 and 27002 were approved in 2013 by the Brazilian Association of Technical Standards (ABNT), which provides security techniques, information security management systems and a Code of practice for information security management.

31. Under what circumstances must a business report security breaches to regulators, to individuals or to other persons or entities? If breach notification is not required by law, is it recommended by the regulator, and what is the typical custom or practice in your jurisdiction?

The Communication of security breaches ("CIS") is a mechanism pointed out by LGPD to fulfill the controller's obligation to communicate to the regulatory authority and to the data subject the occurrence of a security breaches that may cause risk or relevant damage to data subjects (Article 48, LGPD). This communication occurs by sending a form, made available by the ANPD's website.

The controller that is subject to the LGPD must communicate the incident to the ANPD and to data subjects.

Prior to reporting the security breaches, the controller must conduct a risk assessment to decide whether or not the incident is likely to be reported to the ANPD and/or to the data subjects. In this assessment, according to ANPD, should be considered among other aspects:

- The context of the data processing activity;
- The categories and quantities of data subjects affected;
- The types and quantities of data breached;
- The potential material, moral and reputational damage caused to the data subjects;
- Whether the data breached were protected in such a way as to make it impossible to identify the data subjects;
- The mitigation measures adopted by the controller after the incident.

As per the ANPD guidelines, an incident needs to be reported if it meets, cumulatively, the following criteria:

1. It Has the occurrence confirmed by the controller;
2. It involves personal data subject to the LGPD;
3. It entails a relevant risk or harm to the data subjects.

Thus, under the terms of the LGPD (art. 48, § 1, I to VI) and according to the document published by ANPD, the communication must contain, at a minimum (without prejudice to additional information), the following:

- description of the nature of the affected personal data;
- information about the data subjects involved;
- indication of the technical and security measures used for data protection, respecting industrial and commercial secrets;
- the risks related to the incident;
- the reasons for the delay, in case the communication was not immediate;
- the measures that have been or will be adopted to revert or mitigate the effects of the damage;
- description of how the organization became aware of the incident;
- when it occurred and when it was made aware of it;
- statement about the size of the controller's company, in accordance with Resolution CD/ANPD 2/2022;
- inform to which other authorities the incident was communicated, if applicable;
- more detail on the communication of the incident to the data owners;
- indicate impacts in a more detailed manner, for example, whether it affected confidentiality, integrity or availability of data alone or jointly;
- separation between sensitive data and common data breached;
- examples of probable consequences and impacts to the data subjects;
- inform if a Data Protection Impact Assessment (DPIA) was performed.

The content of the notice to data subjects may be requested by the ANPD and must be rectified if it does not meet the minimum requirements. This notice must use clear language and contain at least the following information: (i) summary and date of occurrence of the incident; (ii) description of the personal data affected; (iii) risks and consequences to the data subjects; (iv) measures taken and recommended to mitigate its effects, if applicable; (v) contact details of the controller

for further information about the incident.

The LGPD only mentions that the CIS must be performed within a reasonable period of time, as defined by the Regulatory Authority (art. 48, §1). In the form, however, the ANPD suggests the communication deadline is up to 2 (two) working days after the security breaches is known. In addition, the form indicates the deadline of 30 (thirty) calendar days for submission of additional information when the communication made by the controller is preliminary (partial). Unjustified delay in communicating a security incident may subject processing agents to the administrative sanctions provided for in the LGPD.

Incident reporting and specification of the notification deadline is one of the items foreseen in Phase 1 ANPD's Regulatory Agenda 2023-2024, in the phase that covers topics whose regulation process was already started in the previous biennium. Therefore, it will be important to continue following the development of this topic.

Finally, the Brazilian Computer Emergency Response Team (CERT.br) presents some recommendations for the notification of security incidents, giving guidance about what to notify, whom to notify and formats for the notification, among other instructions.

32. Does your jurisdiction have any specific legal requirement or guidance regarding dealing with cybercrime, such as the payment of ransoms in ransomware attacks?

The Senate has approved the country's adherence to the Convention on Cybercrime, which aims to facilitate and strengthen the means available to prevent and face cybercrime. By June 2021, the Convention had been ratified by 66 countries and the Brazilian initiative was added to the Internet law, for the criminal prosecution of cyber crimes and the Brazilian General Data Protection Act.

Beyond that, Law 12,737/12 amended the Brazilian Criminal Code (Decree-Law 2,848/1940) and provided for the criminal classification of computer-related crimes, such as the intrusion of a computing device, for example.

In the same way, Law 12,735/12 determined the installation of police stations and specialized teams to combat digital crimes. In conjunction with the police stations specialized in cybercrime, there are non-governmental institutions that work in partnership with the Government and the Public Prosecutor's Office to combat cybercrime, such as SaferNet Brazil, which offers a service for receiving anonymous reports of crimes and violations against Human Rights on the Internet.

Other normative instruments can be nominated, such as Law 11,829/08, which institutes the crime of child pornography on the Internet, and Law 13,185/15, which establishes a mandatory program to fight to cyberbully.

The payment of ransoms in ransomware attacks and other cybercrimes related to money laundering, financial pyramids and crimes related to cryptocurrencies, among others can be addressed by the Judiciary on the infractions provided for in the Brazilian Criminal Code or specific regulations.

33. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

Brazil does not have a separate cybersecurity regulator. In this regard, cybersecurity challenges might be dealt with by public authorities, such as the Public Prosecutor's Office, or by the Judiciary, when the demand is brought to its attention, with the help of independent agencies or entities, such as Computer Security Incident Response Teams (CSIRTs). In cases of incidents of cybersecurity involving the Brazilian Public Administration, for example, the Computer Network Security Incident Processing Center of the Federal Public Administration (CTIR) should be contacted.

34. Do the laws in your jurisdiction provide individual data privacy rights such as the right to access and the right to deletion? If so, please provide a general description of the rights, how they are exercised, what exceptions exist and any other relevant details.

The LGDP sets forth that all-natural people are ensured the ownership of their personal data and the guarantee of the fundamental rights to freedom, intimacy, and privacy. It also establishes that data subjects have the right to obtain from the controller, according to articles 17 to 22 of LGPD, at any time and upon request:

- Confirmation of the existence of the processing;
- Access to the data;
- Correction of incomplete, inaccurate, or outdated data;
- Anonymization, blocking, or erasure of unnecessary or excessive data or data

processed in non-compliance with the provisions of the LGPD;
- Portability of data to another service or product provider, upon express request, by the regulations of the ANPD, observing commercial and industrial secrets;
- Deletion of the personal data processed with the consent of the data subjects, except in cases of:
    a. Compliance with a legal or regulatory obligation by the controller;
    b. Conduction of studies by a research entity, ensuring, whenever possible, the anonymization of the personal data;
    c. Transfer to third parties provided that all legal requirements outlined in this Law are complied with;
    d. Exclusive use of the controller, with forbidden access to third parties, and provided the data has been anonymized;
- Information about public and private entities with which the controller has shared data;
- Information about the possibility of denying consent and the consequences of the denial;
- Revocation of consent;
- Opposition to processing carried out based on one of the situations of waiver of consent if there is noncompliance with the provisions of LGPD;
- Review of decisions taken by the controller solely based on automated processing of personal data that affects the data subject's interests, including decisions intended to define his/her personal, professional, consumer, or credit profile or aspects of his/her personality.

All the rights aforementioned shall be exercised through the express request by the data subject or his/her legal representative, to the controller. This request shall be fulfilled without costs to the data subject, and, in case it is not possible to promptly take the actions, the data controller shall send to the data subject a reply in which it may: (I) inform that it is not the data processing agent, indicating, if possible, the agent; or (II) point out legal and factual grounds preventing prompt action.

Data subjects have the right to petition about their data against the controller before the ANPD. The defense of the interests and rights of data subjects may be carried out in court, individually or collectively.

The rights of confirmation of existence and access to data will be provided immediately, in a simplified format; or within fifteen (15) days from the date of the data subject's request, through a clear and complete declaration that indicates the origin of the data, the nonexistence of record, the criteria used and the purpose of the processing, subject to commercial and industrial secrecy. Information and data may be provided by electronic means or in printed form. Also, when the processing is based on consent or in a contract, the data subject may request a complete electronic copy of its personal data, observing commercial and industrial secrecy, in a format that allows its subsequent utilization, including for other processing operations.

The ANPD Resolution N. 2 of 27th January 2022, approved the Regulations for the application of the LGPD for Small-Sized Processing Agents. This Resolution provides, in its articles 14, I, III, and 15, double time for the fulfillment of the data subject's rights provided in the LGPD, including the provision of a simplified declaration of processing of personal data in 15 days.

The matter related to the rights of data subjects will be further clarified by the ANPD within one year, according to phase one of the ANPD's regulatory agenda 2023/2024 biennium.

Besides, the Consumer Code sets forth those individuals have the right to access all data stored about themselves in consumer-related databases, and request changes, corrections, and even removal from the database. This right to access might also be exercised before consumer-defense entities.

Finally, according to the Internet Law, users have the right to request at the end of their contract with internet application providers the definitive exclusion of personal data, respecting the mandatory log retention rule.

It is also worth remembering that the protection of personal data is now considered a fundamental right under Brazilian Constitution.

35. Are individual data privacy rights exercisable through the judicial system or enforced by a regulator or both?

Both. The Federal Constitution establishes that the law shall not exclude from the Judiciary's assessment injury or threat to rights; therefore, the defense of the interests and rights of data subjects may be exercised in court, individually or collectively, by the provisions of the relevant legislation, regarding the instruments of individual and collective protection.

In addition to this guarantee, LGPD stipulates that data subjects have the right to petition concerning their data against the controller before ANPD. The right to access might also be exercised before consumer-defense entities.

36. Does the law in your jurisdiction provide for a private right of action and, if so, in what circumstances?

Yes. According to the Federal Constitution, any individual can file a judicial action pursuing compensation for economic and moral damages for violation of privacy or intimacy. Furthermore, the Brazilian Code of Civil Procedure determines that the exercise of the right of action depends on the interest and legitimacy of the claimant.

The CF/88 established, in February 2022, the protection of personal data as a fundamental right, in its article 5º, LXXIX. Also, the CF/88 assures Brazilians and foreign nationals the right to rectify their data, and the Consumer Code provides that individuals have the right to access all data stored about themselves, and request changes.

The Internet Law provides for the user´s right to request the definitive exclusion of personal data, by the end of the relationship with the internet application provider. Also, LGPD provides that the data subject may exercise their rights and interests through a court, individually.

37. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection, privacy and/or cybersecurity laws? Is actual damage required, or is injury of feelings sufficient?

According to LGPD, in its articles 42 to 45, the controller or processor, as a result of carrying out their activity of processing personal data, causes material, moral, individual, or collective damage to others, in violation of personal data protection legislation, is obliged to redress it. Also, the processing agent who neglects to adopt measures to avoid security incidents shall be held liable for the damages caused by the violation of the data security that caused the damage.

Individuals affected by a violation of LGPD are entitled to compensation or monetary damages. Usually, actual damage is required and injury of feelings must be proved to justify compensation. Many court decisions are repelling the mere injury of feelings to generate monetary compensation to data subjects. In a recent decision (March, 2023), the Superior Court of Justice (Superior Tribunal de Justiça – STJ) understood that data breach does not have the capacity, by itself, to generate indemnifiable moral damage. Therefore, in an eventual claim for compensation, it is necessary that the data subject proves the actual damage generated by the exposure of this information. The decision was issued in a lawsuit for moral damages against an energy company for improper sharing personal data to third parties. According to the plaintiff, an elderly person, the energy company had improperly shared her personal data to third parties, which exposed her to potential danger of fraud and harassment. The data shared improperly were full name, ID, gender, date of birth, age, telephone number, cell phone and address, in addition to data related to consumption of electricity. STJ understood that the case was nothing more than an inconvenient exposure of common personal data, routinely informed in various situations of everyday life, besides not having been proven the effective damage by the leak.

This is one of the first decisions coming from the higher Courts in Brazil and will serve as a parameter, but there is still much to be debated in order to form a jurisprudence on the matter.

38. How are data protection, privacy and cybersecurity laws enforced?

According to article 55 – I of LGPD, the ANPD is competent to ensure the protection of personal data, supervise and impose sanctions in case of data processed in violation of the Brazilian laws, through an administrative process ensuring defense and right to appeal. In addition, the ANPD published Resolution N. 1 on October 28, 2021, which regulates the inspection process and the sanctioning administrative process within the scope of the ANPD’s performance.

The Resolution establishes that the administrative process can be initiated: (i) ex officio by the General Inspection Coordination; (ii) as a result of the monitoring process (also regulated by the Resolution); and (iii) upon request made by the General Inspection Coordination, after carrying out an admissibility analysis and deciding on the immediate opening of a sanctioning process.

Furthermore, the sanctioning administrative process must observe the following criteria:

1. serving purposes of general interest;
2. adequacy between means and ends, prohibited the imposition of obligations, restrictions, and sanctions to a greater extent than those strictly necessary to meet the

public interest;
3. observance of the essential formalities to guarantee the rights of interested parties;
4. adoption of simple forms, suitable to provide an adequate degree of certainty, security and, respect for the rights of interested parties;
5. ex officio imposition of the administrative process, without prejudice to the action of the interested parties; and
6. interpretation of the administrative rule in the way that best guarantees the fulfillment of the public purpose for which it is aimed, prohibited the retroactive application of a new interpretation.

Complementary issues such as the methodologies that will guide the calculation of the value of fines sanctions and the conditions for adopting a fine may be regulated subsequently by the ANPD.

In addition to the ANPD, other bodies already acted in the enforcement of privacy in Brazil and will continue to act, such as the Public Prosecutor's Office, the National Consumer Bureau (SENACON) and consumer protection authorities, such as Procon. These bodies opened several cases and investigations against companies that suffered security incidents and data breaches in Brazil or processed personal data and sensitive personal data in potentially or effectively harmful ways to the data subjects.

39. What is the range of sanctions (including fines and penalties) for violation of data protection, privacy and cybersecurity laws?

The LGPD provides that the ANPD will impose administrative sanctions on processing agents for violation of the rules, namely:

- Warning, with an indication of the period for the adoption of corrective measures;
- A simple fine of up to 2% (two percent) of a private legal entity, group, or, conglomerate's revenues in Brazil, for the prior fiscal year, excluding taxes, up to a total maximum of BRL 50,000,000.00 (fifty million reais) per infraction;
- A daily fine, observing the total limit referred above;
- Publication of the infraction after duly ascertained and confirming its occurrence;
- Blocking of the personal data to which the infraction refers until its regularization;
- Deletion of the personal data to which the infraction refers;
- Partial suspension of the operation of the database to which the violation refers for a maximum period of 6 (six) months, extendable for the same period until the controller's regularization of the processing activity;
- Suspension of the exercise of the processing activity of the personal data to which the infraction refers for a maximum period of 6 (six) months, extendable for the same period;
- Partial or total prohibition of the exercise of activities related to data processing.

Also, the Internet Law states that, without prejudice to any other civil, criminal or administrative sanction, the non-compliance with data protection rules can result in the following sanctions that may be applied on an individual or cumulative basis:

- A warning, with a deadline for the adoption of corrective measures;
- A fine up to 10% of the gross income of the economic group in Brazil in the last fiscal year, taxes excluded;
- Temporary suspension of the activities that entail the events set forth in any operation related to the processing of data;
- Prohibition to execute activities that entail the processing of data.

The Consumer Code determines a penalty of six months to one-year imprisonment or fine, or both, to those who block or hinder access by the consumer to respective information contained in files, databases or, records, or those who are expected of knowing that information relating to the consumer as contained in any file, database, record or registration is incorrect and, nevertheless, fail to immediately rectify it. The same statute sets forth administrative penalties imposed by the authorities in charge of protecting consumer rights, and such penalties include fines, intervention and, counter-advertising.

The Bank Secrecy Law (Complementary Law 105/2001) establishes a penalty of one to four years imprisonment and a fine for financial institutions (and similar entities) that breach the secrecy of the financial operations of, and the financial services provided to its users.

The Brazilian Criminal Code (Decree-Law 2.848/1940), as amended by Law 12.737/2012, sets forth the penalty of three months to one-year imprisonment and a fine for those who invade another computer device connected or not to the internet through improper breach of security mechanism and for the purpose of obtaining, tamper or destroying data or information without the explicit or

tacit authorization of the device owner or installing vulnerabilities to gain an illicit advantage.

40. Are there any guidelines or rules published regarding the calculation of fines or thresholds for the imposition of sanctions?

LGPD defines parameters applicable when calculating the amount of the monetary sanctions. The rules defined are as follows:

i. Severity and nature of the infringements and personal rights affected;
ii. Good faith of the offender;
iii. Advantage received or intended by the offender;
iv. Offender's economic standing;
v. Recurrence;
vi. Extent of damage;
vii. Cooperation of the offender;
viii. Repeated and substantiated adoption of internal mechanisms and procedures capable of minimizing the damage with a view towards safe and adequate processing of data, per the provisions of LGPG;
ix. Adoption of best practices and governance policies;
x. Prompt adoption of corrective measures; and
xi. Proportionality between severity of the infringement and nature of the sanction.

LGPD does not limit the sanctions to administrative sanctions imposed by the ANPD. Data subjects and their representatives may seek the court for compensation, in which case the limitation of the monetary amount imposed by LGPD will not be applicable.

Also, in February 2023, ANPD published the Regulation on How to Proceed with Aplication of Sanctions (Resolution CD/ANPD No. 4, of February 24, 2023). According to the Regulation, violations will be ranked according to severity, nature, and personal rights affected.

Minor infractions will be considered when they are not medium and serious.

Violations will be considered medium when they impact the interests and fundamental rights of the data subjects, as well as cause material or moral damage.

A violation will be considered serious when it constitutes obstruction of the supervisory activity or affects the data subjects in the same way as a medium breach and, at the same time (i) it involves large-scale processing; or (ii) the infringer obtains or intends to obtain an economic advantage; or (iii) it entails a risk to the lives of the data subjects; or (iv) it involves processing of sensitive data or of children, adolescents or the elderly; or (v) the processing was carried out without a legal basis; or (vi) the processing has unlawful or abusive discriminatory effects; or (vii) the systematic adoption of irregular practices is verified.

The regulation establishes a points table that must be used to define the parameters of the amount of the fine to be imposed. Thus, the calculation methodology takes into consideration the nature of the violation, the size of the company, and the turnover in the year prior to the violation:

- For minor infractions, the rates vary from 0.08% to 0.15% of revenue.
- For medium infractions, the rates vary between 0.13% and 0.5%.
- For serious violations, the rates range from 0.45% to 1.5%.

41. Can personal data or PII owners/controllers appeal to the courts against orders of the regulators?

There is no express provision about this possibility in the LGPD or any other legislation that refers to data protection in Brazil. However, taking into consideration that the Federal Constitution establishes that the law may not exclude from the Judiciary's assessment injury or threat to rights, data subjects could appeal to the courts against orders of the ANPD, provided that the data subject proves his/her right of action (interest and legitimacy).

42. Are there any identifiable trends in enforcement activity in your jurisdiction?

The ANPD has not yet imposed any fines, however, with the publication of the Regulation on How to Proceed with Application of Sanctions, it is expected that fines will begin to be applied. Also, in March 2023, the ANPD published administrative proceedings open for the application of sanctions for violation of the LGPD. Six public agencies and one private company are under investigation. The list drew attention by the fact that public agencies dominate the list and demonstrated the rigidity that the ANPD will act, showing that it will adopt an active position in the enforcement of LGPD and related rules.

43. Are there any proposals for reforming data protection, privacy and/or cybersecurity laws currently under review? Please provide an overview of any proposed changes and how far such proposals are through the legislative process.

Yes, there are many proposals for changes and additions to the Brazilian legislation, such as:

- The use of Artificial Intelligence (AI) is currently being discussed in Brazil through a single Bill No. 5,691/2019 that establishes the "National Policy for Artificial Intelligence", with the goal of stimulating the formation of a favorable environment for the development of technologies in AI. This bill is the result of a union of other previous bills that discussed the topic: (i) Bill No. 5.501/2019 – established the principles for the use of AI and regulated its use; (ii) Bill No. 872/2019 – provided for the ethical frameworks and guidelines that underlie the development and use of AI; (iii) Bill No. 21/2020 – intended to create the legal framework for the development and use of artificial intelligence by public authorities, companies and individuals. The text established principles, rights, duties and governance instruments for AI. The National AI Policy establishes as its core principles (i) inclusive and sustainable development; (ii) respect for ethics, human rights, democratic values, and diversity; (iii) protection of privacy and personal data; and (iv) transparency, security, and reliability. The bill also states that AI should respect people's autonomy; preserve people's intimacy and privacy; preserve the bonds of solidarity between people and different generations; be intelligible, justifiable, and accessible; be open to democratic scrutiny and allow for debate and control by the population; be compatible with maintaining social and cultural diversity and not restrict personal lifestyle choices; contain safety and security tools that allow human intervention where necessary; provide traceable decisions without discriminatory or prejudiced bias; and follow governance standards that ensure ongoing management and mitigation of potential technological risks. In March 2023 two other new bills were introduced: Bill No. 753/2023, which intends to regulate IA systems and Bill No. 1153/2023, which provides general rules for research, development and application of IA at the Federal, State and Municipal levels in Brazil.
- Bill No. 2392/2022 intends to prohibit the use of facial recognition technologies for identification purposes in the public and private sectors without a prior data protection impact assessment (DPIA).
- Bill N. 490/22 makes it mandatory to share the location and date of automated vehicle identification made by surveillance equipment for public safety purposes. The text under analysis by the House of Representatives inserts the device in the Brazilian Traffic Code. The project will be analyzed by the committees of Public Security and Combating Organized Crime; Transportation; and Constitution and Justice and Citizenship.
- Bill N. 2630/20, known as "The Fake News Law", establishes rules regarding the transparency of social networks and private messaging services, especially regarding the responsibility of providers to combat disinformation and to increase transparency on the internet, transparency regarding sponsored content and the actions of public authorities, as well as establishes sanctions for non-compliance with the Brazilian law. This project is still in progress in the House of Representatives.

Contributors

Ricardo Barretto Ferreira da Silva
Senior Partner
barretto@azevedosette.com.br

Lorena Pretti Serraglio
Coordinator
lserraglio@azevedosette.com.br

Bruna Evellyn Pereira Bigas
Associate
bbigas@azevedosette.com.br

Carolina Simioni Perdomo
Associate
cperdomo@azevedosette.com.br

Ingrid Bandeira Santos
Associate
isantos@azevedosette.com.br