COUNTRY COMPARATIVE GUIDES 2024

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

Ingrid Bandeira Santos

Associate | isantos@azevedosette.com.br

Stefania Mariotti Masetti

Senior Associate | smasetti@azevedosette.com.br

Carolina Simioni Perdomo

Associate | cperdomo@azevedosette.com.br

Camila Sabino Del Sasso

Associate | csasso@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 main principles of privacy and data protection are established in the Brazilian Federal Constitution ("CF/1988"), according to which privacy, private life, image and honor, as well as correspondence, telegraphic and telephone communications of individuals are inviolable. The Constitution also ensures the right to compensation for moral and economic damages resulting from noncompliance. Constitutional Amendment 115/2022 modified CF/1988 to expressly include data protection as a fundamental right in the list of article 5th.

Besides CF/1988, Law 13,709/2018 (the Brazilian General Data Protection Act or "LGPD") was enacted in August 2018, but most of its provisions only came into force in September 2020. Then in August 2021 the rules on administrative sanctions applicable to noncomplying agents came into force, through Law 14,010/2020.

LGPD can be considered a broad regulation for data protection, including, among the activities considered data processing: access, collection, classification, modification, monitoring, transmission, archiving, disclosure, and erasure of personal data. Under this Law, data processing must observe ten principles, which are: purpose limitation, adequacy, minimization, free access by the data subject, data quality, transparency, integrity, prevention of damages, non-discrimination, and accountability.

Alongside the Brazilian data protection framework, Internet matters are also regulated, mainly by the Brazilian Civil Rights Framework for the Internet (Law 12,965/2014, the "Internet Law"). This Law sets forth principles, rights, obligations, and guarantees for the use of the Internet in Brazil, and it is regulated by Decree 8,771/2016. The Decree sets forth rules on security and confidentiality of personal data, records, and private communication, as well as on the request of record data by public agents.

The following list contains some of the main sectorial laws and regulations that include rights related to privacy and data protection, grouped in sectors:

Civil and Consumer rights:

- Civil Code (Law 10,406/2002) protects the private life of individuals, and eventual violations are subject to judicial claims;
- Consumer Protection Code (Law 8,078/1990) is guided by the principles of transparency, information to suppliers and consumers, and data quality.

Internet and Telecommunication

- Telecommunications Act (Law 9,472/1997) assigns privacy rights to telecommunications services' consumers;
- Wiretap Act (Law 9,296/1996) establishes that interception of communications can only occur by court order in connection with criminal investigations or with discovery in criminal proceedings. The request may be made by police authorities in charge of the investigation or by the Public Prosecutor's Office;
- Resolution 3/2009 of the Internet Steering Committee in Brazil (CGI.br) establishes ten fundamental governance principles for the use of Internet in Brazil, mostly directed at Internet service providers, aimed at protecting individual rights and freedoms in a regulated innovative environment.

Banking and Finance

- Bank Secrecy Act (Complementary Law 105/2001) requires secrecy of financial data of individuals and entities by financial institutions and comparable entities, unless a judicial order is issued in connection with discovery in criminal proceedings or investigation of illegal acts;
- Positive Credit Registry Act (Law 12,414/2011) allows databases of 'positive' credit score (i.e., fulfillment of contracted obligations) but prohibits record of information considered excessive (i.e., data which is unnecessary for assessing consumer credit risk) and sensitive data (e.g., sexual preferences, ethnicity, health and genetic data, religious or political convictions). Moreover, as per amendment by Complementary Law 166/2019, the Positive Credit Registry Act started authorizing database managers to include individuals and legal entities in positive record databases, without their prior request;
- Resolution 1/2020 of the Brazilian Central Bank, which established the Pix payment arrangement (an instant payment system designed by the Brazilian Central Bank), requires formal consent by users for the registration of payment keys and for the use of Pix.
- Joint Resolution 5/2020 of the Brazilian Central Bank and the National Monetary Council provides for interoperability of Open Finance requires formal consent from users for data sharing in the Open Finance environment;
- PagTesouro, operated by the Ministry Finance, is a digital platform offering a method of collecting fees due to various governmental offices and bodies connected with the National Treasury. It was established by Decree 10,494/2020. This platform allows citizens other payment options (like Pix and credit card), in addition to the existing modality of Federal Revenue Collection Slip ("GRU").

Health protection

- Law 14,129/2021, which sets forth principles, rules, and tools for the Digital Government and for the increase of public efficiency requires compliance with LGPD, including personal data protection and privacy as a Digital Government and efficiency principle;
- Resolution 489/2022 of the National Supplementary Health Agency imposes a fine up to BRL 50,000 on health insurance companies for conditioning portability to certain health conditions of a patient;
- Resolution 657/2022 of the Brazilian Health Regulatory Agency ("ANVISA") establishes rules for regularization of Software as a Medical Device (SaMD). It requires manufacturers to indicate software cybersecurity measures such as protection against unauthorized use; and devices to be developed taking into account risk management, including data security, for the evaluation of data on safety and effectiveness of the product.

Brazil's ANPD is the National Data Protection Authority. Since its creation, it issued guidelines and booklets, which have no force of law, but serve as instruction based on ANPD's views. Among the guidelines, we highlight the following:

i. Guideline on Definitions of Processing Agents and Data Protection Officer, of May, 2021, with definitions, responsibilities, and illustrative examples;
ii. Booklets on Internet security, of July, 2021, with two volumes: one on data leaks and the other on data protection;
iii. Guide How to Protect Your Data, of September, 2021, targeting data subjects, and issued in Portuguese, English and Spanish;
iv. Guideline on Information Security for Small-Sized Processing Agents, of October, 2021, aimed at assisting the target public with general information security measures;
v. Guideline on Data Processing by Public Agents, of October 2021, setting objective parameters, establishing surveillance guidance and obligations for public entities;
vi. Guideline on Application of LGPD by Processing Agents in the electoral context, of January 2022, with aspects to be considered by candidates, coalitions, parties regarding the processing of personal data in the electoral context;
vii. Guideline on the use of Cookies, of October, 2022, with definitions of cookies and their types, as well as with legal hypotheses and requirements to be ideally observed in the use of cookies, especially for cookie banners on websites;
viii. Guideline on the Processing of personal data for academic purposes, studies, and research, of June, 2023, with good practices suggested for this subject.

In terms of recent regulations, in 2023 ANPD updated its rules on reporting security incidents and issued Resolution 4/2023, with the Regulation on How to Calculate and Apply Administrative Sanctions. In April, 2024, ANPD regulated its Compliance Program by publishing two Resolutions (Res. 12/2024 and 13/2024), the first creating the Compliance Program itself and, the second, establishing its Compliance and Transparency Committee.

More recently, on April 26, 2024, ANPD published Resolution 15/2024, with the long-awaited Regulation on Notification of Security Breach Incidents.

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2024–2025 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments (together, "data protection laws"))?

Yes. ANPD's original Regulatory Agenda for 2023-2024 was modified by Resolution CD/ANPD 11/2023 of December, 2023. The subjects to be regulated by the authority until the end of 2024 have therefore been updated. The high-priority themes in Stages 1 and 2 have not been moved, but two items from Stage 2 have been repositioned as the last two items of Stage 4. The updated agenda for years 2023-2024 is the following:

STAGE 1 (initiated in 2021-2022)		
Subject	Description	Document
Regulation of Dosimetry and Imposition of Administrative Penalties	Regulate the administrative sanctions for LGPD violations and the methodologies that shall guide the calculation of the fine sanctions.	Regulation
Data subject rights	Clarify how to guarantee the rights of data subjects, such as review of automated decisions and publicity of data processing by public servants.	Regulation
Data breach notification	Regulate the deadlines, standard template and the adequate submission procedure to ANPD.	Regulation
International transfer of personal data	Regulate the articles of LGPD addressing international data transfers.	Regulation
Data Protection Impact Assessment (DPIA)	Issuance of regulations and procedures on the subject.	Regulation
Data Protection Officer (DPO)	Issuance of supplementary rules on the definition and duties of the DPO, as well as hypotheses of DPO designation 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"	Establishing of criteria for defining these expressions.	Regulation
Sensitive personal data for Religious Organizations	Definition of basic measures for LGPD compliance by religious organizations	Document
Use of personal data for academic purposes and for studies by research organizations	Providing recommendation and guidance aimed at encouraging the adoption of best practices and supporting 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 of LGPD	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 (expected to be initially finished by December, 2023)		
Subject	Description	Document
Data Sharing by Public Authorities	Operationalize Articles 26 and 27 of LGPD, concerning the sharing of data by the government to private entities. This should also cover the procedures to be adopted and the information to be sent to ANPD for compliance with legal provisions.	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 Internet-based digital platforms and games on the protection of children's and adolescents' data.	Technical Study

STAGE 3 (expected to be finished by mid-2024)		
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, modification, 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 (expected to be finished by December, 2024)		
Subject	Description	Document
Conduct Adjustment Commitment (TAC)	Regulate TAC. The Conduct Adjustment Commitment – TAC is an instrument that makes up the Inspection Process and the Sanctioning Administrative Process of ANPD, allowing the interested agent to submit a proposal for agreement as an alternative to the regular progress of the sanctioning process.	Regulation
Guidelines for the National Policy on Personal Data Protection and Privacy	Direct the actions of all subjects involved in the data protection ecosystem, including ANPD, also regarding other published policies, such as the Digital Strategy, the IoT National Plan, and others.	Guideline
Regulation of criteria for recognition and disclosure of good practices and governance rules	Regulate criteria for the recognition and dissemination of good practices and governance rules to be observed by processing agents	Regulation

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

When it comes to data processing activity itself, the Brazilian data protection legislation, LGPD included, does not require any prior licensing or registration. However, companies acting in regulated sectors (e.g., health, banking, electricity, transportation, telecommunication, oil & gas) are required to have licenses/authorizations issued by the corresponding regulatory bodies.

4. How do these data protection laws define "personal data," "personal information," "personally identifiable information" or any equivalent term in such legislation (collectively, "personal data") versus special category or sensitive personal data? What other key definitions are set forth in the data protection laws in your jurisdiction?

LGPD contains the following definitions:

- Personal data: information related to any identified or identifiable individual;
- Sensitive personal data: data that concerns racial or ethnic origin, religious belief, political opinion, affiliation to a trade union or to an organization of religious, philosophical or political nature, data relating to health or sexual life, genetic or biometric data, when linked to a natural person.

Some other relevant definitions are:

- Data subject: individual to whom refer the personal data object of processing activity;
- Data controller: an individual or legal entity, governed by public or private law, who is responsible for making decisions regarding the processing of personal data;
- Data processor: an individual or legal entity, governed by public or private law, which carries out the processing activity of personal data on behalf of the controller;
- Data protection officer: person appointed by the controller and data processor to act as a communication channel between the controller, the data subjects, and ANPD;
- Processing agents: data controller and data processor;

- Processing activity: any operation involving personal data, including, but not limited to, those concerning collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, elimination, evaluation or control of information, modification, communication, transfer, dissemination or extraction;
- ANPD: public administration body responsible for ensuring, implementing and overseeing compliance with LGPD in the Brazilian territory.

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

Under article 6 of LGPD, the processing of personal data shall abide by good faith and the following principles: (i) purpose limitation; (ii) adequacy; (iii) minimization; (iv) free access; (v) data quality; (vi) transparency; (vii) integrity; (viii) prevention; (ix) non-discrimination; and (x) accountability.

Additionally, article 7 of LGPD limits the processing of personal data to be carried out only under the following circumstances:

- Upon data subject's consent;
- For compliance with a legal or regulatory obligation by the controller;
- By the public administration, for the processing and shared use of data required for the implementation of public policies;
- For the performance of studies by a research body, ensuring anonymization of personal data whenever possible;
- When necessary for the performance of a contract or preliminary proceedings related to a contract to which the data subject is a party, upon request of the data subject;
- For the regular exercise of rights in judicial, administrative or arbitral proceedings;
- For the protection of the life or physical integrity of a data subject or of a third party;
- For the protection of health in a procedure performed by health professionals, health services or health authority;
- When necessary to meet the legitimate interests of the data controller or of a third party, except in the event that the data subject's fundamental rights and freedoms prevail, requiring the protection of personal data;
- For credit protection, including with respect to provisions of the relevant legislation.

Article 15 of LGPD establishes the circumstances that trigger termination of the data processing. Such events are: (i) when the purpose of the processing has been achieved or the data are no longer necessary or relevant to achieve the purpose sought; (ii) when the processing period ends; (iii) upon communication by the data subject based on a legal request, such as to revoke consent; (iv) when ANPD so determines in case of violation of LGPD. The law permits custody of personal data after their processing in the following circumstances under article 16 of LGPD:

- The controller must keep data to comply with a legal or regulatory obligation;
- Data are kept for study by a research body securing anonymization of the personal data whenever possible;
- Transfer to third parties, provided that data processing requirements set forth in LGPD are observed;
- Exclusive use by the controller, with no access to third parties, and provided the data are anonymized.

It is important to note that other fields of law in Brazil may provide their own thresholds on data storage. For instance, there are specific data storage rules in the consumer, labour and tax laws. Finally, the Internet Law (Law 12,965/2014) establishes that, in the provision of Internet connection, the autonomous system administrator shall keep connection records confidential, in a controlled and secure environment, for one year (article 13). It also determines that Internet application providers shall keep records of access to Internet applications (*i.e.*, information on date and time of use of a given Internet application from a certain IP address – article 5, VIII) confidential, in a controlled and secure environment, for a minimum term of six months (article 15).

6. Are there any circumstances for which consent is required or typically obtained in connection with the general processing of personal data?

Yes, there are situations in which LGPD requires consent by a data subject. For instance, as a general rule, the

processing of personal data of children and adolescents requires specific and highlighted consent granted by at least one of the parents or by the legal guardian.

Consent is also required for a mandatory data sharing by the controller, when the data was obtained by consent in the first place. Still, there may be a waiver of such consent for data transfer, like in the situation where data are clearly made public by the data subject.

Consent is one of the legal grounds for the processing of personal data under LGPD. Where personal data processing is based on consent, LGPD establishes that it can be revoked at any time by express manifestation of the data subject, in a free and facilitated procedure. LGPD also lets the data subject require deletion of personal data processed under the subject's consent, unless the processing occurs in one of the circumstances listed under article 16 of LGPD, referred to in the response to question 5 above.

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)?

LGPD defines consent as a free, informed and unequivocal manifestation by which the data subject agrees to the processing of his/her data for a specific purpose. Breaking down the elements of a valid consent, we have the following:

- Free – the data subject cannot be under pressure, duress or obligation to consent. Ideally, it should not be given through a pre-selected checkbox;
- Informed – the object of consent by the data subject must be clear, transparent, thorough, and simple to understand;
- Unequivocal – there can be no doubt on whether the data subject accepted the text of his/her consent.

LGPD provides some practical guidance on the form of a valid and enforceable consent, such as:

- Consent shall be given in writing or by other means that demonstrate the express will of the data subject;
- If consent is provided in writing, it shall be displayed in a separate contractual clause;
- Consent shall refer to specific purposes; generic authorizations for processing personal data shall not be valid;
- Consent given to the processing of sensitive personal data must be specific and highlighted.

The data controller has the burden to prove that consent was obtained according to LGPD's provisions. Personal data cannot be processed with defective consent where it is required. A practical recommendation and also a good practice is to incorporate a highlighted consent into a document. This will contribute to knowledge and understanding by the data subject.

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

LGPD does not prohibit the processing of sensitive personal data, but there are rules in place for such processing. The general rule is that consent is required in a highlighted manner and for specific purposes, and it may be given by the data subjects or by their legal guardian. However, other situations in the law allow for health data processing without consent, such as:

- For the data controller to comply with a legal or regulatory obligation;
- For the public administration's execution of public policies with the shared processing and use of data;
- For the performance of studies by a research body, ensuring anonymization of sensitive personal data, whenever possible;
- For the regular exercise of rights in a contract or in judicial, administrative or arbitral proceedings;
- For the protection of the life or physical integrity of a third party or of the data subject;
- Exclusively for the protection of health, in a procedure performed by health professionals, health services or health authority;
- For the prevention of fraud and for ensuring safety of the data subject, in processes of identification and authentication of registration in electronic systems, observing the rights of the data subject, except where the data subject's fundamental rights and freedoms prevail, requiring the protection of personal data.

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

LGPD considers health data sensitive. Consequently, health data can only be processed under an adequate legal basis. Among the rules for processing sensitive data, LGPD prohibits the shared use of sensitive data pertaining to health among controllers, with the purpose of obtaining an economic advantage. LGPD also prohibits private health insurance providers from processing health data for doing risk selection in the contracting of any modality, as well as when contracting and excluding beneficiaries.

10. Do the data protection laws in your jurisdiction include any derogations, exclusions or limitations other than those already described? If so, please describe the relevant provisions.

LGPD lists the situations to which it does not apply. The types of personal data processing which fall out of LGPD's reach are those:

- Carried out by an individual exclusively for private and non-profit purposes;
- Carried out exclusively for journalistic, artistic, or academic purposes;
- Carried out exclusively for purposes of public safety; national defence; state security; or activities involving investigation and repression of crimes; or
- Originated outside the Brazilian territory and which are not the object of communication, shared use of data with Brazilian processing agents or object of international transfer of data with another country that is not the country of origin, provided that the country of origin maintains a level of personal data protection appropriate to the level established under LGPD.

11. Do the data protection laws in your jurisdiction address children's and teenagers' personal data? If so, please describe how.

Before entering this topic, it is relevant to bring the definition of children and of adolescents under the Brazilian legislation, since different countries may have divergent age ranges for this public. In Brazil, the Child and Adolescent Statute (Law 8,069/1990 – "ECA") establishes that a child is a person aged up to twelve years old, while an adolescent is a person aged between twelve and eighteen years old. Both receive full protection under this Statute.

Since children and adolescents have some level of vulnerability, LGPD grants them stricter rules for protection of their personal data. The law starts asserting that the processing of personal data of children and adolescents shall be carried out to their best interest, pursuant to the specific provisions of LGPD and the applicable law. LGPD rules for processing their data include the following:

- Specific and highlighted consent of at least one of the parents or of the legal guardian for processing personal data of children and adolescents;
- Controllers shall keep public the information on the types of data collected, the form of their use, and the procedures for exercising the rights under LGPD;
- Personal data of children and adolescents may be collected without consent when it is necessary to contact the parents or legal guardian, used only once and without storage, or for their protection. Moreover, the data shall not be transferred under no circumstances to third parties without adequate consent;
- Data controllers shall not associate participation of data subjects in games, Internet applications or other activities to the provision of personal information beyond those strictly necessary for the activity;
- The controller shall make use of all reasonable efforts to verify that consent was given by the person responsible for the child, considering the available technologies;
- Information on the processing of children's and adolescents' data shall be provided in a simple, clear and accessible manner, considering the physical and motor, perceptive, sensorial, intellectual and mental characteristics of the user, employing audiovisual resources when appropriate, to provide the necessary information to the parents or legal guardian and adequate for the child's understanding.

12. Do the data protection laws in your jurisdiction address online safety? Are there any additional legislative regimes that address online safety not captured above? If so, please describe.

The Child and Adolescent Statute ("ECA") contains

provisions aimed at online protection of its target public. For instance, ECA contains a whole section dedicated to regulating infiltration of police officers on the Internet for investigating crimes against the sexual dignity of children and adolescents, some of which are described in ECA itself, while others are in the Penal Code.

Additionally, in 2024, the Penal Code included the crimes of bullying (systematic intimidation) and cyberbullying (virtual systematic intimidation) in the list of crimes against personal freedom. Bullying is defined as the systematic intimidation, solely or in group, through psychological or physical violence, of one or more individuals, in a repetitive and intentional manner, with no evident reason, by means of intimidation, humiliation or discrimination acts or through verbal, moral, sexual, social, psychological, physical, material or virtual actions.

Cyberbullying is the same as bullying, adding the fact that it is perpetrated in a computers' network, social media, applications, online games or in any other digital means or environment, or in live broadcast. The base penalty for this crime is between two- and four-years imprisonment and fine, if the violation does not characterize a more serious crime.

13. Is there any regulator in your jurisdiction with oversight of children's and teenagers' personal data, or online safety in general? If so, please describe, including any enforcement powers. If this regulator is not the data protection regulator, how do those two regulatory bodies work together?

While ANPD is the main authority in charge of overseeing data protection matters in Brazil, online safety of children's and teenagers' is not exclusive of single governmental body or of the government alone. The Brazilian Constitution sets forth a broad duty of protecting children and adolescents, assigning this duty to the family, to society and to the State (government). All these actors are in charge of safekeeping children and adolescents from all kinds of negligence, discrimination, exploitation, violence, cruelty and oppression.

The list of governmental and private entities involved in the online protection of children and adolescents includes, although it is not limited to:

- Ministry of Human Rights and Citizenship: designs public policies for the protection, defence and warranty of rights;
- Federal Prosecutors Office ("MPF"): oversees compliance with the legislation on children's online safety and promotes public actions for the defence of children and adolescents;
- Federal Police: investigates cybercrimes involving children and adolescents;
- SaferNet Brasil: NGO acting in partnership with public bodies to promote online safety;
- CGI.br: publishes since 2012 researches on access and use of information technologies by children and adolescents, assessing not only digital capabilities, but also attitude and strategies for protection of privacy and use of the Internet;
- ANATEL: telecommunication regulator in Brazil, ANATEL has partnered with the UK Embassy and CGI.br to translate and make available several materials directed at instructing children and adolescents on how to protect themselves on the Internet. The materials are available free of charge on the online safety area of ANATEL's website.

The joint work of such actors is not necessarily provided for in the law or in regulations. It depends more on their initiative to partner in addition to their individual work directed at online safety.

14. Are there any expected changes to the online safety landscape in your jurisdiction in 2024–2025?

Yes. The National Council of the Children's and Adolescents' Rights ("CONANDA"), which is part of the Ministry of Human Rights and Citizenship, published on April 9, 2024 Resolution 245/2024, with provisions on the rights of children and adolescents in the digital environment, to take effect immediately. This Resolution reinforces the constitutional provision on joint responsibility of the family, society and public actors towards protection of minors; establishes guiding principles; and, among other things, sets forth rights related to navigation in the digital environment. The impacts of this new regulation are yet to be assessed, since it contains some provisions that may conflict with LGPD and with guidelines by ANPD on the processing of children's and adolescents' personal data.

Additionally, the country has been debating for a few years the need for a regulation on freedom, liability, and transparency on the Internet by means of Bill of Law 2,630/2020. This Bill has been called by some as Fake News Bill and, by others, as Censorship Bill and, after some years of debate in Congress, as well as in public hearings with society representatives, this Bill may have

reached its doom. The talk in Congress now is around the discussion and drafting of a new project on the subject, with support from the federal government.

15. Does your jurisdiction impose 'data protection by design' or 'data protection by default' requirements or similar? If so, please describe the requirement(s) and how businesses typically meet such requirement(s).

LGPD requires that processing agents use security, technical and administrative measures that can protect personal data from unauthorized access and accidental or unlawful situations from the design stage of the product or service until its execution. The idea of privacy by default is implied in LGPD, since companies must follow, among others, these principles:

- Purpose limitation: processing shall be performed for legitimate, specific, and explicit purposes, duly informed to the data subject, without possibility of further processing in a way inconsistent with these purposes;
- Minimization: restriction of the processing to the minimum required to achieve its purposes, encompassing relevant and proportional data, not excessive as to the purpose of such processing;
- Accountability: the agent shall demonstrate adoption of effective measures capable of proving compliance with personal data protection rules, and also the effectiveness of such measures.

Businesses usually comply with these requirements by means of a suitability program, whereby they: (i) maintain records of personal data processing operations; (ii) elaborate a Data Protection Impact Assessment ("DPIA"), with a description of the kinds of data collected, the methodology used for collection and for ensuring the security of information and the analysis by the controller regarding the technical and administrative measures adopted, safeguards and mechanisms of risk reduction; and (iii) adopt good practices of privacy and transparency.

ANPD may establish minimum technical standards, considering the nature of the information processed, specific data processing features and the available technology, in the case of sensitive personal data.

16. Are controllers and/or processors of personal data required to maintain any internal records of their data processing activities or establish internal processes or written documentation? If so, please describe how businesses typically meet such requirement(s).

The controller and the processor shall maintain records of the personal data processing operations they perform (article 37 of LGPD), especially when based on legitimate interest. It is also advisable for controllers and processors to maintain a current data mapping, to provide a Data Protection Impact Assessment (DPIA) when necessary, observing the principle of accountability.

ANPD addressed this matter in the Guideline on Definitions of Personal Data Processing Agents and Data Protection Officer, confirming the obligation of both agents (controller and processor) to keep records of personal data processing activities.

17. Do the data protection laws in your jurisdiction require or recommend data retention and/or data disposal policies and procedures? If so, please describe such requirement(s).

According to article 15 of LGPD, the processing of personal data must end when (i) the processing purpose is fulfilled or the data are no longer needed or relevant for that purpose; (ii) the processing period expires; (iii) the data subject requests to exercise his/her rights, including the right to withdraw consent; or (iv) ANPD so determines in case of LGPD violations.

LGPD also determines that personal data shall be eliminated after the processing ends, unless (i) they are required for the data controller to comply with legal or regulatory obligations; (ii) they are used for research purposes by a research body, and the personal data are anonymized whenever possible; (iii) they are transferred to third parties, in line with the data processing requirements, or; (iv) they are exclusively used by the data controller, without access by third parties and with anonymization of the data.

It is possible that ANPD will further regulate these issues. Until then, companies may implement good practices and ensure compliance with the principles under article 6 of LGPD.

18. Under what circumstances is a controller operating in your jurisdiction required or recommended to consult with the applicable data protection regulator(s)?

The law does not require or recommend consultation with regulators to process personal data. Nonetheless, ANPD keeps a "contact us" tab on its website, with an open channel to dialogue in cases of (i) Submitting a request from the data subject to the data controller; (ii) Complaining about an LGPD violation; (iii) Asking questions about LGPD; (iv) Personal Data Breaches; (v) Submitting invitations or files to ANPD; (vi) Press; (vii) Ombudsman; (viii) Requests for access to information under the relevant law. These options can be found at: https://www.gov.br/anpd/pt-br/canais_atendimento.

19. Do the data protection laws in your jurisdiction require or recommend risk assessments in connection with data processing activities and, if so, under what circumstances? How are these risk assessments typically carried out?

According to article 38 of LGPD, ANPD may require the preparation of a data protection impact assessment (DPIA) by the controller, including reference to sensitive data, data processing operations, preserving trade and industrial secrets. The DPIA shall contain the description of all personal data processes that could lead to risks to fundamental rights and civil freedoms of data subjects, as well as procedures, safeguards and instruments to mitigate such risks.

Also, when processing is based on legitimate interest, it must be carried out under the processing of data strictly necessary for the intended purpose, with grounds on specific situations. Under LGPD, article 10, paragraph 3, ANPD may request from the controller a data protection impact assessment (DPIA).

ANPD maintains a Questions & Answers section on its website about DPIA. The page is available at: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd

ANPD recommends drawing up the DPIA before the controller starts processing personal data for the desired purpose, precisely so that it can assess the possible risks associated with this processing beforehand. However, if it is not possible to draw up the DPIA before the processing begins, it is recommended that it be drawn up as soon as a processing operation is identified that could generate a high risk to the guarantee of the general principles of personal data protection provided for in LGPD and to the civil freedoms and fundamental rights of the data subject.

20. Do the data protection laws in your jurisdiction require a controller's appointment of a data protection officer, chief information security officer, or other person responsible for data protection, and what are their legal responsibilities?

LGPD requires the controller to appoint a Data Protection Officer – DPO. The DPO's identity and contact information must be made public, in a clear and simple way, preferably on the controller's website. Although LGPD does not mandate the appointment of a DPO for processors, they may assign a DPO as well, as per article 5, VIII of LGPD.

The DPO's tasks include: (i) taking complaints and messages from data subjects, giving explanations and implementing measures; (ii) receiving communications from ANPD and following measures; (iii) instructing employees and contractors on the practices to follow in connection with privacy and data protection processes; (iv) Carrying out other duties set forth by the controller or in additional rules.

Moreover, ANPD issued the Guideline on Definitions of Personal Data Processing Agents and Data Protection Officer, which states the following:

- LGPD does not specify conditions under which an organization should have a DPO, using as a rule that every organization should have a DPO;
- LGPD does not indicate whether the DPO should be an individual or a legal entity, a company's employee or an external agent. Nonetheless, the guide suggests that the DPO should be appointed by a formal act;
- As a good practice, the DPO should have autonomy in performing his or her duties, as well as knowledge of information security and data protection;
- LGPD does not prevent DPOs from having the support of a multidisciplinary data protection team.

ANPD may establish additional rules on the definition and duties of the DPO, including cases of exemption of appointment, depending on the nature and size of the entity, or volume of data processing operations.

ANPD Resolution 2/2022 has addressed this topic by regulating the application of LGPD to Small-Sized Processing Agents. Processing agents that meet the criteria of the Resolution may opt out of appointing a DPO, but if they do appoint one, this will be regarded as a good practice.

21. Do the data protection laws in your jurisdiction require or recommend employee training related to data protection? If so, please describe such training requirement(s).

Under LGPD, the DPO must train the company's workers and contractors on governance and data protection best practices. Even though LGPD does not specify the controller's duty to inform and educate its employees, it is a necessary step for companies to comply with LGPD.

22. Do the data protection laws in your jurisdiction require controllers to provide notice to data subjects of their processing activities? If so, please describe such notice requirement(s) (e.g., posting an online privacy notice).

Yes. Data subjects are entitled to easy access to information on how their data is processed. Such information must be presented in a clear, adequate, and ostensive manner, among other characteristics required for in regulation, to comply with the principle of free access (LGPD, article 9), such as:

- Specific purpose of the processing;
- Form and duration of the processing, observing trade and industrial secrets;
- Identification of the data controller;
- Contact information of the data controller;
- Information on data sharing by the controller and its purpose;
- Liabilities of the agents that will perform the processing; and
- Rights of the data subject, clearly mentioning the rights provided for under LGPD.

If the specific goals of the processing, type or duration of the processing, identification of the controller or information about the joint use of data are changed, the controller shall inform the data subject, with a special emphasis on the content of the changes.

Where consent is the legal basis of the processing activity and if there are changes in the reasons for the processing of personal data that make it incompatible with the original consent, the controller shall inform the data subject beforehand of the changes. In this case, the data subject may withdraw the consent whenever he or she disagrees with the changes.

If the processing of personal data is a condition for the delivery of a product, the offering of a service or the exercise of a right, the data subject shall be informed of this fact and of how the rights outlined in LGDP can be exercised.

23. Do the data protection laws in your jurisdiction draw any distinction between the controllers and the processors of personal data, and, if so, what are they?

LGPD defines controllers and processors as "processing agents" and differentiates them in article 5, items VI, VII and IX. A data controller is an individual or legal entity, governed by public or private law, who can decide on how personal data is processed. By its turn, a data processor is an individual or an entity, governed by public or private law, who processes personal data on behalf of the controller.

Under LGPD, article 39, the data processor shall follow the controller's instructions, and the controller must check that the processor follows the instructions and the rules applicable to the matter.

According to articles 42 to 45 of LGPD, the controller or the processor who, by processing personal data, causes pecuniary, moral, individual or collective damage to others, in violation of data protection laws, must compensate for it.

The data processor is jointly liable with the controller for damages caused by the processing if the processor fails to comply with the law or to observe the controller's lawful instructions, in which case the processor is considered equivalent to the controller Processing agents shall not be liable in case there is evidence that:

- They did not process the personal data attributed to them;
- Even though they did the personal data attributed to them, there was no violation of data protection laws;
- The damage arises exclusively from the fault of a third party or of the data subject.

The controller or the processor who does who fails to adopt the security measures required under LGPD will be liable for the damages caused.

24. Do the data protection laws in your jurisdiction place obligations on processors by operation of law? Do the data protection laws in your jurisdiction require minimum contract terms with processors of personal data?

There is no legal requirement for minimum contract terms or other limitations on hiring service providers. Companies can negotiate the contract terms and limitations among themselves. However, LGPD draws some general directions for data processors and data controllers on security matters.

ANPD also deals with this issue in the Guideline on Definitions of Personal Data Processing Agents and Data Protection Officer. It includes the processor's obligation to sign contracts that set, among other things, the provisions of activities and responsibilities with the controller. LGPD states, moreover, that ANPD can further regulate this matter.

Under article 50 of LGPD, controllers and processors can design rules for good practice and governance. These rules may set conditions of organization, operating regime, procedures, complaints, and petitions for data subjects, security and technical standards, and specific obligations for the parties involved, in addition to other possible initiatives. When making these rules, the processing agents should consider factors related to the processing of the subject's data, such as nature, scope, purpose, likelihood, and severity of risks and benefits that will result from the data processing.

25. Are there any other restrictions relating to the appointment of processors (e.g., due diligence, privacy and security assessments)?

No.

26. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction, including through the use of tracking technologies such as cookies. How are these terms defined, and what restrictions on their use are imposed, if any?

In attention to the principle of transparency, provided for in article 6, item VI of 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. This includes decisions intended to define their personal, consumer, and credit profiles or aspects of their personality.

As regards cookies, ANPD published a Guideline on the use of Cookies and the protection of personal data. This document brings important recommendations on how cookies should be used. Based on the principles of LGPD, especially on purpose limitation, minimization, adequacy, free access, and transparency, the document lists useful parameters: (i) ensuring a high level of transparency to data subjects, with clear and complete policies and privacy notices; (ii) provision of information on how the user can manage cookies, demonstrating that the websites contain tools for changing preferences on cookies in a practical and easy manner; (iii) 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), being possible to insert the same cookie in more than one category.

The Guideline also provides information on the appropriate legal basis for processing of each type of data collected. The cookies' classification will directly reflect the purpose of the data being processed and the legal basis authorizing the data processing carried out through the cookies.

When it comes to data collection by advertising cookies, the Guideline suggests that the most appropriate legal basis is "consent." Such recommendation implies measures that must be taken by those responsible for the websites, so that the collection of consent be carried out properly and in compliance with LGPD. Generic authorizations commonly collected through "agree", "accept" or "aware" buttons are not interpreted as representing valid consent.

Finally, the Guideline displays the possibility of applying the legal basis of legitimate interest of the controller, considering the use of necessary cookies. Another point of great relevance concerns the layout and configuration of the cookie management tool. The Guideline suggests 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.

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

Behavioral advertising is advertising delivered using the data subject's data and information. This can include demographic data, economic status, gender, age, employment, lifestyle, interests, purchase history. Customization of ads is possible because of online monitoring. LGPD does not prohibit behavioral advertising, but it devises mechanisms and principles that allow it not to become unlawful. Therefore, the principles established under LGPD will guide processing agents on how to perform behavioral advertising.

The practice of behavioral advertising cannot go against the guarantees provided in article 2 of LGPD, which are: (i) respect for privacy; (ii) informative self-determination; (iii) freedom of information and communication; (iv) inviolability of intimacy, honor and image; and (v) free development of personality.

In that sense, article 18 of LGPD establishes the need for security and transparency in data processing, guaranteeing rights that the data subject can exercise. Once ANPD releases further definitions on the subject, it will be possible to apply it more objectively and with clearer recommendations.

Other laws are applicable to this subject. For instance, the Internet Law, in its article 7, determines a need to provide clear and complete information for the processing of personal data. The Consumer Protection 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 there is no express regulation in Brazil about behavioral advertising, the requirements outlined in Brazilian laws and regulations must be observed.

Also in this regard, ANPD's Guideline on the use of Cookies must be taken into account. It advises the user on how to manage cookies, offering the data subject the possibility to refuse cookies not necessary for navigation. Informing data subjects 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 else detailed in privacy policies or notices.

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

Brazil has no specific rules on the sale of personal data. LGPD must be followed in any case, and a valid legal basis for the processing must exist. Some public entities have punished companies that sold personal data without clear permission from the data owners. In this case, consent was the required legal basis, and, in the case of such violations, it had not been obtained.

29. Please describe any data protection 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") issued Act 10,413/2021, requiring phone operators to start any marketing call with the code 0303. This standardization aims to help the data subject identify telemarketing calls and avoid unwanted calls. The procedure came into effect in March, 2022.

Additionally, there are public opposition lists created by state laws in Brazil where the individual/data subject can indicate that he/she does not want to receive marketing messages via phone calls or SMS. These lists are supervised by the Procon (Consumer Protection Office) in each state. The controllers and processors must respect this rule when using these means to send ads of their products and services to individuals with area codes from states that have official opposition lists.

In any case, all communications with the data subject for marketing purposes must follow the principles and best practices established by LGPD, as well as the Consumer Protection Code that has provisions that protect consumers in general against, among other things, abusive marketing and advertising of products and services.

Lastly, LGPD does not specify the term "direct marketing," nor does it bring specific obligations in its text for this kind of advertising. Therefore, to do direct marketing, the controller must consider the peculiarities of the processing activity and ensure compliance with LGPD's provisions, especially regarding the data subject's rights and their legitimate expectation of receiving certain advertisements content.

30. Please describe any data protection

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

Biometric data, including facial recognition, is sensitive personal data under LGPD. LGPD has specific rules and legal bases for processing this data, because it can affect data subjects' fundamental rights.

There is no specific law for facial recognition in Brazil yet, but some Bills are being discussed in the House of Representatives. Bill 2,537/2019 requires businesses that use facial recognition to notify customers with signs or stickers at their entrances. It needs to be approved by the House and the Senate. Other Bills (4,612/2019, 4,901/2019, both attached to Bill 12/2015) aim to regulate the development, application, and use of facial and emotional recognition and other digital technologies for identification and behavior analysis. They are still in progress in the House.

The latest Bill (2,392/2022), presented in August, 2022, bans the use of facial recognition for identification in public and private sectors without a prior privacy impact report – DPIA. This Bill is currently being processed in the House.

31. Please describe any data protection laws in your jurisdiction addressing artificial intelligence or machine learning ("AI").

There are no laws currently addressing AI in Brazil. However, some existing laws may impact the way AI is used, such as the existing rules on data privacy, Internet, and consumer protection. Congress has been discussing some Bills on the subject.

ANPD has contributed to one of the legislative discussions by submitting a Technical Note (16/2023/CGTP/ANPD) on Bill 2,338/2023, which aims at regulating the use of Artificial Intelligence in Brazil. As mentioned above in the response to question 2, ANPD's Regulatory Agenda includes the issuance of guidelines in its Stage 3.

32. Is the transfer of personal data outside your 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 or notification to or authorization from a regulator?)

The transfer of data outside the jurisdiction is regulated by Brazilian legislation in articles 33 to 36 of LGPD. The law establishes that the international transfer of personal data is only permitted in the following situations:

- When the country or international organization of destination provides a level of personal data protection that is adequate to the provisions of LGPD, in the form of: (i) specific contractual clauses for a given transfer; (ii) standard contractual clauses; (iii) global corporate standards; (iv) regularly issued seals, certificates and codes of conduct;
- When the controller offers and proves guarantees of compliance with the principles, the rights of the data subject and the data protection regime provided for in LGPD;
- When the transfer is necessary for international legal cooperation between public intelligence, investigation, and prosecution bodies;
- When ANPD authorizes the transfer;
- When the transfer is necessary for the fulfilment of a legal obligation, the execution of a public policy, the performance of a contract, the regular exercise of rights in judicial, administrative or arbitration proceedings, among other cases.

It is important to highlight that the efficacy of some rules on international data transfers described above still requires regulation by the National Data Protection Authority (ANPD).

33. What security obligations are imposed on data controllers and processors, if any, in your jurisdiction?

The Internet Law provides security requirements for Internet service providers, as well as LGPD, which establishes the need for processing agents to protect personal data from unauthorized access and accidental or unlawful cases of destruction, modification, loss, communication or improper or unlawful processing, adopting security, technical and administrative measures.

The software/systems used for processing personal data shall be structured to comply with the security

requirements, general data protection principles, standards of good practice and governance, and other sectorial regulatory rules. Furthermore, the security of the information should be ensured by the controllers and processors, even when processing has ended, as established by LGPD.

In addition, Article 13 of Decree 8,771/2016 establishes the security standards and confidentiality of records, personal data and private communications, as follows: (i) definition of responsibilities of people who will be able to access the data and exclusive access privileges for certain users; (ii) provision of authentication mechanisms for access to records to ensure individualization of the people who will have access to data; (iii) creation of a detailed inventory of access to connection records and access to applications, containing time, duration, identity of the designated employee/individual responsible for the access; and (iv) use of management solutions of records using techniques which guarantee data inviolability, such as encryption or equivalent protection measures.

34. Do the data protection laws in your jurisdiction address security breaches and, if so, how do such laws define a "security breach"?

Security breaches were defined by ANPD as any confirmed adverse event related to a breach in the security of personal data, such as unauthorized, accidental or unlawful access resulting in the destruction, loss, modification, leakage or any form of inappropriate or unlawful processing of data, which may result in a risk to the rights and freedoms of the data subject.

With the enactment of Resolution 15/2024, ANPD changed the above definition to now call security breach incident "any confirmed adverse event related to the violation of the personal data security attributes of confidentiality, integrity, availability, and authenticity". Confidentiality relates to assuring that data will not be made available or revealed to unauthorized people, systems or entities. Integrity pertains to assuring that data were not destroyed or modified in unauthorized or accidental ways. Availability is linked to ensuring that data are accessible and useable on demand. Finally, authenticity relates to the information being produced, issued, modified or destroyed by a certain individual, equipment, system, body or entity (article 3, items XII, V, XIII, XI, and II).

It is important to highlight that incidents involving personal data must be reported by the controller to ANPD upon meeting the reporting criteria explained under item 36 of this Guide. However, incidents involving anonymized data or which are not related to identifiable natural persons do not need to be reported to ANPD.

35. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecom, infrastructure, AI)?

In Brazil, there are specific security requirements on certain regulated sectors and industries, as described below:

Internet Service Providers:

- The Internet Law provides security requirements for Internet service providers, and Decree 8,771/2016 provides security standards for handling personal data and private communications for Internet service providers;

Telecommunications Sector:

- Cybersecurity Regulation Applied to the Telecommunications Sector of the National Agency for Telecommunications (ANATEL) aims to establish conduct and procedures for promoting security in telecommunications networks and services, including cybersecurity and the protection of critical telecommunications infrastructures. Following the publication of the Regulation, ANATEL approved the Cybersecurity Requirements for Telecommunications Equipment. It is important to note that the certification and approval of telecommunications equipment is the responsibility of ANATEL, which must aim to protect the safety of users of these products, now also taking cybersecurity into account;
- ANATEL's Resolution 740/2020 establishes the regulation on cybersecurity applied to the telecommunications sector;
- Decree 9,637/2018 creates the National Information Security Policy and provides for the governance of information security;
- Normative Ruling 4/2020 of the Institutional Security Office provides the minimum cybersecurity requirements to be adopted when establishing 5G networks.

Financial Institutions:

- Central Bank of Brazil's Resolution 85/2021 (amended by Resolution 368/2024) provides for the cybersecurity policy and requirements for contracting data processing, data storage and cloud computing services to be complied by payment institutions, securities brokerage companies, securities distribution companies and foreign exchange brokerage companies authorized to operate by the Central Bank;
- National Monetary Council's Resolution 4,893/2021 provides for the cybersecurity policies and requirements for contracting data processing and storage, as well as cloud computing services, requirements which must be observed by institutions authorized to operate by the Central Bank.

Insurance Companies:

- Superintendence of Private Insurances (SUSEP) Circular 638/2021 issued provisions on cybersecurity to be applied to insurance companies, open supplementary pension entities, capitalization companies and local reinsurers. The Circular aims to align the insurance market with existing legal provisions and should be interpreted in conjunction with LGPD, the rules to be issued by ANPD and consumer legislation, where applicable.

Energy Sector:

- Brazilian National Energy Agency (ANEEL)'s Resolution 964/2021 provides for the cybersecurity policies to be adopted by agents in the energy sector.

36. Under what circumstances must a business report security breaches to regulators, impacted individuals, law enforcement, or other persons or entities? If breach notification is not required by law, is it recommended by the applicable regulator in your jurisdiction, and what is customary in this regard in your jurisdiction?

The controller must report the occurrence of security breaches that may cause risk or relevant damage to data subjects. Under ANPD's Resolution 15/2024, the incident causes risk or relevant damage to data subjects when it significantly affects interests and fundamental rights of subjects and, cumulatively, it involves one of the following criteria:

- Sensitive personal data;
- Data of children, adolescents or elders;
- Financial data;
- Data for authentication in systems;
- Data protected by legal, judicial or professional secrecy; or
- Data in large scale

The data breach significantly affects interests and fundamental rights of subjects when, among other circumstances, the processing activity may cause material or moral damages to subjects, discriminate, violate the physical integrity, the right to image and reputation, financial fraud or identity theft. The incident must be reported to ANPD through a statement available in the authority's website and to data subjects, according to article 48 of LGPD.

LGPD and ANPD determine that the communication must contain, at a minimum (without prejudice to additional information), the following information:

- description of the nature of the affected personal data;
- number of data subjects involved, including the number of vulnerable subjects like children, adolescents or elders, where applicable;
- the technical and security measures used for data protection, respecting industrial and commercial secrets;
- the risks related to the security breach, identifying possible impact to the subjects;
- in case the communication was not made in up to three business days from knowledge or within another legal deadline, the reasons for the delay;
- the measures that were/will be adopted to revert or mitigate the effects of the damage;
- date of occurrence and the date on which the controller became aware of it;
- information about the DPO or of whoever represents the controller;
- identification of the controller and, if it is the case, statement about being a small-size processing agent;
- identification of the processor, where applicable;
- description of the incident, including its main cause, in case it is identifiable;
- the total of subjects the data of which are processed in the processing activities affected by the breach incident.

Before reporting the security breach, the controller must carry out a risk assessment to decide whether the

incident can be reported to ANPD and/or to the data subjects. This type of assessment should consider some aspects, such as: (i) the context of the data processing activity, (ii) the categories and quantities of data subjects involved, as well as the potential damages caused to data subjects (material, moral and reputational); (iii) the types of data breached; (iv) if the data breached has been protected in such a way as to make it impossible to identify the data subjects; (v) the mitigation measures adopted by the controller after the security breach.

Regarding the deadline for communication of an incident, LGPD determines that the Communication of security breaches ("CIS") must be performed within a reasonable period of time, as defined by ANPD. According to ANPD's Resolution 15/2024, up to three business days after the security breaches is known, unless there is a different deadline established by specific law. For small-sized companies, the deadline is doubled.

In addition, ANPD indicates the deadline of twenty business days for submission of additional information, counted from the notification. Unjustified delays in reporting a security breach can subject processing agents to the administrative sanctions provided for under LGPD.

37. Does your jurisdiction have any specific legal requirements or guidance for dealing with cybercrime, such as in the context of ransom payments following a ransomware attack?

Regarding the payment of ransoms in ransomware attacks and other cybercrimes related to money laundering, financial pyramids and crimes related to cryptocurrencies, for example, it is important to note that they can be dealt with by the Judiciary in the cases of infractions provided for in the Brazilian Penal Code or in specific regulations.

On April 2023, the Government promulgated the Convention on Cybercrime. Brazil became one of the countries that joined this multilateral international instrument, thus strengthening cooperation ties with strategic cooperation in combating cybercrime.

Some other normative instruments can also be nominated, such as:

- Law 11,829/2008, which institutes the crime of child pornography on the Internet;
- Law 14,811/2024, which amended the penal code to create the crime of cyberbullying;
- Law 12,735/2012, providing for the creation of specialized police stations to combat cybercrime in the Federal Police and in the Civil Police;
- Law 12,737/2012 on cybercrimes.

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

There is not a separate cybersecurity regulator in Brazil. Cybersecurity matters usually are dealt with by public authorities, such as the Public Prosecutor's Office or by the Judiciary in cases which the demand is brought to its attention. In addition, there is the Computer Network Security Incident Processing Center of the Federal Public Administration ("CTIR"), which should be contacted in cases of cybersecurity incidents involving Brazilian Public Administration.

39. Do the data protection 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 such rights, how they are exercised, any exceptions and any other relevant details.

LGPD ensures that all natural persons have the right to own their personal data and are ensured the protection of fundamental rights such as freedom, intimacy, and privacy. This legislation also provides that data subjects have the right to request from the data controller, at any time and upon request, in accordance with articles 17 to 22 of LGPD:

- Confirmation of whether their data is being processed;
- Access to their data;
- Correction of incomplete, inaccurate, or outdated data;
- Anonymization, blocking, or deletion of unnecessary, excessive, or non-compliant data as per LGPD;
- Portability of their data to another service or product provider, upon explicit request and following ANPD regulations, while respecting commercial and industrial secrets;
- Deletion of personal data processed with the consent of the data subject, except under specific conditions such as compliance with legal obligations, research purposes, transfer to third parties under legal compliance, or

exclusive use by the controller with anonymized data;
- Information about public and private entities with whom the controller has shared data;
- The ability to refuse consent and understand the consequences of such refusal;
- Withdrawal of consent;
- The right to object to processing based on consent exemptions if it does not comply with LGPD provisions;
- The right to review decisions made solely on automated data processing that impacts the data subject's interests, including profiling related to personal, professional, consumer, or credit aspects.

These rights must be exercised through an express request by the data subject or their legal representative to the controller, free of charge. If immediate action is not possible, the controller must provide a response indicating either that they are not the data processor or the legal and factual reasons for the delay.

Data subjects also have the right to lodge complaints regarding their data with the controller before ANPD and may seek legal action to defend their interests and rights, either individually or collectively.

The rights to confirm data processing and access data will be fulfilled immediately in a simplified manner, or within fifteen days in a detailed format that respects commercial and industrial secrecy. Data can be provided electronically or in print. Additionally, when processing is based on consent or on a contract, data subjects may request a comprehensive electronic copy of their personal data in a usable format.

ANPD's Resolution 2/2022 extends the deadlines for small-sized processing agents to comply with LGPD, including providing a simplified data processing declaration within fifteen days. Moreover, the Consumer Protection Code grants individuals the right to access, modify, or delete their data in consumer databases, which can also be enforced through consumer protection agencies.

The Internet Law allows users, at the end of their contract with Internet application providers, to request the permanent deletion of their personal data, subject to mandatory data retention laws. Lastly, the Brazilian Constitution now recognizes the protection of personal data as a fundamental right.

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

The Brazilian Federal Constitution declares that the law shall not prevent the Judiciary's evaluation of any harm or threat to rights. Thus, it upholds the principle that the defence of data subjects' interests and rights can be pursued in court, individually or collectively, as outlined in applicable legislation, including mechanisms for both individual and collective protection.

Additionally, LGPD provides data subjects with the right to address grievances regarding their data directly with the controller and to petition before the National Data Protection Authority (ANPD). This right of petition extends to seeking recourse from consumer protection entities, enhancing the avenues available for individuals to assert their rights concerning personal data management.

In essence, these provisions emphasize the importance of legal recourse and regulatory oversight in safeguarding personal data, ensuring individuals have the means to seek redress and protect their privacy rights effectively.

41. Do the data protection laws in your jurisdiction provide for a private right of action and, if so, under what circumstances?

Yes, under the Brazilian Federal Constitution, any person is entitled to initiate legal proceedings to seek reparations for economic and moral harm caused by violations of their privacy or personal intimacy. Moreover, the Brazilian Code of Civil Procedure stipulates that initiating a lawsuit requires the plaintiff to demonstrate a legitimate interest and standing in the matter.

The Internet Law further establishes the right of users to demand the permanent deletion of their personal data from Internet application providers once the service relationship ends. Similarly, LGPD empowers data subjects to defend their rights and interests in court on an individual basis, providing a comprehensive legal basis for the protection of personal and data privacy rights in Brazil. This ensemble of laws underscores a robust commitment to safeguarding personal data and privacy in the digital age, ensuring individuals have substantial recourse to rectify, access, or remove their personal information across various platforms and contexts.

42. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require actual damage to have been sustained, or is injury to feelings, emotional distress or similar sufficient for such purposes?

Under articles 42 to 45 of LGPD, controllers or processors who, through their data processing activities, cause material, moral, individual, or collective harm to others in violation of data protection legislation, are required to compensate for these damages. Additionally, processing agents who fail to implement measures to prevent security incidents are liable for damages resulting from breaches of data security.

The entitlement to compensation or monetary damages for individuals affected by a breach of LGPD typically requires the demonstration of actual harm. Proving emotional distress alone often does not suffice for compensation claims. Many judicial decisions have dismissed claims based solely on emotional distress as insufficient grounds for monetary compensation to data subjects.

43. How are data protection laws in your jurisdiction enforced?

Under Article 55, I of LGPD, ANPD holds the authority to ensure personal data protection, oversee compliance, and enforce sanctions in cases where data processing contravenes Brazilian legislation, via an administrative procedure that safeguards the rights to defence and appeal.

The administrative sanctioning process is guided by several key principles:

- Advancing the public interest;
- Ensuring the proportionality of measures, obligations, restrictions, and sanctions to the minimum necessary to protect public interest;
- Maintaining essential procedural formalities to protect the rights of the involved parties;
- Employing straightforward procedures that provide sufficient certainty, security, and respect for the rights of those involved;
- Allowing for the autonomous initiation of processes by the authority, without hindering the participation of interested parties; and
- Interpreting administrative rules in a manner that best fulfills the intended public objective, avoiding the retroactive application of new interpretations.

ANPD may further detail methodologies for calculating fines and conditions for imposing penalties. Besides ANPD, several other entities have been active in enforcing privacy regulations in Brazil, such as the Public Prosecutor's Office, the National Consumer Secretariat (SENACON), and consumer protection agencies like Procon. These organizations have launched numerous cases and investigations against companies involved in security incidents, data breaches, or the potentially harmful processing of personal and sensitive data, underscoring a comprehensive approach to data protection enforcement within the country.

44. What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction?

LGPD mandates that the National Data Protection Authority (ANPD) enforce administrative penalties on entities that fail to comply with data processing regulations. These sanctions include:

- **Warnings**, specifying a timeframe for implementing corrective actions;
- **Monetary fines**, capped at 2% of the entity's annual revenue in Brazil for the preceding fiscal year, excluding taxes, with a maximum penalty of BRL 50,000,000.00 per violation;
- **Daily fines**, within the aforementioned maximum limit;
- **Public disclosure** of the violation, once its occurrence is confirmed;
- **Data blocking**, concerning the specific data involved in the violation until compliance is achieved;
- **Data deletion**, targeting the specific data implicated in the infraction;
- **Database operation suspension**, either partially or entirely, for up to six months, extendable by the same period, pending regularization of data processing activities;
- **Suspension** of the personal data processing activities related to the infraction for up to six months, extendable for an additional six months;
- **Partial or total prohibition** of data processing activities.

Moreover, the Internet Law outlines additional consequences for non-compliance with data protection rules, potentially applied individually or cumulatively:

- **Warnings**, with a deadline to undertake

corrective measures;
- **Fines**, up to 10% of the entity's gross revenue in Brazil for the last fiscal year, excluding taxes;
- **Temporary suspension** of activities associated with data processing;
- **Prohibition** of data processing activities.

The Consumer Protection Code prescribes a punishment ranging from six months to one year of imprisonment, a fine, or both, for individuals who deny consumers access to their information in databases or fail to correct known inaccuracies immediately. Additionally, it establishes various administrative penalties, such as fines and mandatory corrective advertising, enforceable by consumer protection authorities.

The Bank Secrecy Law imposes a one- to four-year prison sentence and a fine on financial institutions that disclose client financial operations or services without authorization.

Finally, the Brazilian Criminal Code, updated by Law 12,737/2012, penalizes unauthorized access to computer devices, with or without Internet connection, by bypassing security measures to obtain, modify, or destroy data or to install vulnerabilities for illicit gain, with three months to one year of imprisonment and a fine.

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

The General Data Protection Act (LGPD) establishes specific criteria for determining the amount of monetary penalties for data protection violations. These criteria are designed to ensure fairness and proportionality in sanctions, taking into account various factors such as:

- **Severity and nature of the infringements** and the personal rights that were affected;
- **Good faith** of the offender;
- The **advantage gained or sought** by the offender;
- The **economic status** of the offender;
- **Recurrence** of the violation;
- **Extent of the damage** caused;
- The **level of cooperation** by the offender with the authorities;
- **Evidence of internal mechanisms and procedures** previously implemented to mitigate damage and ensure the safe processing of data, in line with LGPD requirements;
- **Implementation of best practices** and governance policies;
- **Timely corrective actions** taken by the offender;
- **Proportionality** between the severity of the infringement and the nature of the sanction.

LGPD clarifies that penalties are not confined to administrative actions by ANPD. Data subjects and their legal representatives have the right to pursue judicial remedies for compensation, where the limits on monetary penalties specified by LGPD do not apply.

This structured approach aims to provide clarity and consistency in the enforcement of data protection laws, ensuring that penalties are properly aligned with the nature and impact of the infringement.

46. Can controllers operating in your jurisdiction appeal to the courts against orders of the regulators?

Although LGPD or other specific Brazilian data protection laws do not explicitly address the right to challenge in court decisions made by ANPD, the Brazilian Federal Constitution lays a foundational principle that may fill this gap. According to the Constitution, the law cannot preclude the Judiciary from reviewing cases involving harm or threats to rights. Consequently, this constitutional guarantee suggests that data subjects may have recourse to judicial appeals against ANPD decisions, assuming they can adequately demonstrate their standing and interest in the matter (i.e., their right of action). This interpretation hinges on the broad protective scope of the Constitution regarding access to justice, implying that individuals can seek judicial review of administrative decisions that affect their rights, including those related to data protection.

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

While ANPD has not yet levied many sanctions for violation of LGPD, the authority started using its Regulation of Dosimetry and Imposition of Administrative Penalties in the five proceedings made public on the authority's website. The proceedings finished or under analysis by ANPD can be found here: https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/processos-administrativos-sancionadores. Out of nine proceedings made public, only five currently have public documents available.

In March 2023, ANPD had initiated administrative

proceedings to apply sanctions for LGPD breaches, involving six public agencies and one private entity. This action is notable not only for the predominance of public agencies but also for signaling ANPD's commitment to enforce data protection standards rigorously. The list underscores the authority's readiness to hold both governmental and private sector entities accountable, reflecting its proactive stance in safeguarding personal data rights under LGPD. This move is a clear indication that ANPD intends to uphold the principles of LGPD and related regulations, ensuring that entities across all sectors adhere to the required data protection and privacy standards.

48. Are there any proposals for reforming data protection laws in your jurisdiction currently under review? Please provide an overview of any proposed changes and the legislative status of such proposals.

There are a few very important proposals for changes to the Brazilian legislation in connection with data privacy, some of which we highlight below:

- The use of Artificial Intelligence has been discussed through several legislative initiatives underway, but the most advanced of them is Bill 2,338/2023, which is currently being discussed in the Senate. Subsequently, it will be examined by the Chamber of Deputies (reviewing house) and, after the legislative procedures, it will be forwarded to presidential sanction. The aforementioned Bill aims to create the Legal Framework for Artificial Intelligence to establish rights for the protection of citizens and create governance tools, operated by AI supervisory and oversight institutions.
- Bill 2,392/2022, which provides for the use of facial recognition technologies in the public and private sectors. The intention is 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). This Bill was presented in August, 2022 and it is still under analysis in the House of Representatives.
- Bill 490/2022, which amends the Brazilian Traffic Code to oblige the sharing of information on the location and date of automated vehicle identification carried out by inspection equipment for public security purposes. The text was already analyzed by the committees of Public Security and Combating Organized Crime and Transportation, and now is under analysis by the committee of Constitution and Justice and Citizenship.

Contributors

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

Ingrid Bandeira Santos
Associate
isantos@azevedosette.com.br

Stefania Mariotti Masetti
Senior Associate
smasetti@azevedosette.com.br

Carolina Simioni Perdomo
Associate
cperdomo@azevedosette.com.br

Camila Sabino Del Sasso
Associate
csasso@azevedosette.com.br

