



Data Protection 2025

12th Edition



Contributing Editors:

Tim Hickman & Dr. Detlev Gabel
White & Case LLP

glg Global Legal Group

Expert Analysis Chapters

- 1** The Rapid Evolution of Data Protection Laws
Tim Hickman & Dr. Detlev Gabel, White & Case LLP
- 8** AI Regulatory Landscape and Development Trends in China
Kate Yin, Gil Zhang, Sherman Deng & Huihui Li, Fangda Partners
- 17** The Increased Relevance for Companies of Data Collection of Racial and Ethnic Origins in the EU
Pierre Affagard & Laure Ekani, Clyde & Co LLP
- 24** Cloud Computing, Privacy Impact Assessments and Record-Keeping Regarding Data Protection in Japan
Yusaku Akasaki, Hiroki Minekawa & Ronald Kaloostian, Chuo Sogo LPC

Q&A Chapters

- 29** **Australia**
Darren Pham, Phillip Salakas & Harry Sultan,
Nyman Gibson Miralis
- 47** **Brazil**
Larissa Galimberti, Luiza Fonseca de Araujo &
Cecília Alberton Coutinho Silva,
Pinheiro Neto Advogados
- 64** **China**
Susan Ning & Han Wu, King & Wood Mallesons
- 81** **Egypt**
Ibrahim Shehata, Tasneem ElNaggar & Safa Rabea,
Shehata & Partners
- 96** **France**
Clara Hainsdorf & Bertrand Liard,
White & Case LLP
- 107** **Germany**
Martin Röleke & Dr. Evelyne Sørensen,
activeMind.legal Rechtsanwalts-gesellschaft mbH
- 120** **Greece**
Dr. Nikos Th. Nikolinakos, Dina Th. Kouvelou &
Alexis N. Spyropoulos, Nikolinakos & Partners Law Firm
- 135** **Hungary**
Adam Liber & Tamás Bereczki,
BLB Legal – Bagdi-Liber-Bereczki Attorneys-at-Law
- 145** **India**
Rachit Bahl, Rohan Bagai, Sumit Ghoshal &
Archana Iyer, AZB & Partners
- 156** **Indonesia**
Abadi Abi Tisnadisastra, Prayoga Mokoginta &
Aloysius Andrew Jonathan,
ATD Law in association with Mori Hamada
- 167** **Ireland**
Victor Timon, Zelda Deasy, Seán O'Donnell &
Jane O'Grady, Byrne Wallace Shields LLP
- 181** **Isle of Man**
Caitlin Gelder, Kathryn Sharman & Sinead O'Connor,
DQ Advocates Limited
- 192** **Israel**
Vered Zlaikha, Ariella May & Shahar Talmon,
Lipa Meir & Co.
- 205** **Japan**
Hiromi Hayashi & Masaki Yukawa,
Mori Hamada & Matsumoto
- 219** **Mexico**
Abraham Diaz, Gustavo Alcocer & Carla Huitron,
OLIVARES
- 229** **Nigeria**
Jumoke Lambo, Chisom Okolie, Opeyemi Adeshina &
Joel Adeyemi Adefidipe, Udo Udoma & Belo-Osagie
- 245** **Pakistan**
Saifullah Khan & Saeed Hasan Khan,
S. U. Khan Associates Corporate & Legal Consultants
- 254** **Poland**
Jakub Gładkowski, Barbara Kieltyka &
Malgorzata Kieltyka, Kieltyka Gladkowski KG Legal
- 271** **Saudi Arabia**
Saifullah Khan & Saeed Hasan Khan,
Droua Al-Amal Consultants
- 282** **Serbia**
Vladimir Djerić, Lena Petrovic, Katarina Radovic &
Kristina Petronijevic, Mikijelj Jankovic & Bogdanovic
- 295** **Singapore**
Lim Chong Kin & Anastasia Su-Anne Chen,
Drew & Napier LLC
- 312** **Switzerland**
Daniela Fábíán, FABIAN PRIVACY LEGAL GmbH
- 322** **Taiwan**
Yvonne Y.F. Lin, Jeffrey K.S. Hung & Jackie Yang,
Formosan Brothers Attorneys-at-Law
- 331** **Ukraine**
Vladyslav Podolyak & Tetiana Partsei, Arriba
- 345** **United Arab Emirates**
Saifullah Khan & Saeed Hasan Khan,
Bizilance Legal Consultants
- 357** **United Kingdom**
Tim Hickman & Aishwarya Jha, White & Case LLP
- 370** **USA**
F. Paul Pittman, Abdul Hafiz & Andrew Hamm,
White & Case LLP

Brazil

Pinheiro Neto Advogados



Larissa
Galimberti



Luiza Fonseca
de Araujo



Cecília Alberton
Coutinho Silva

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The General Data Protection Law (Law No. 13,709) (*Lei Geral de Proteção de Dados* – known as the “LGPD”) is the principal data protection legislation in Brazil. The LGPD was enacted in August 2018 and came into force on September 18, 2020 (except for the chapter on administrative penalties provided by the LGPD, which came into force in August 1, 2021).

1.2 Is there any other general legislation that impacts data protection?

Yes. Before the enactment of the LGPD, privacy was generally protected in Brazil through the Federal Constitution, the Civil Code (Law No. 10,406/2002), the Consumer Protection Code (Law No. 8,078/1990), the Brazilian Internet Law (Law No. 12,965/2014) and Decree No. 8,771/2016, which regulates the Brazilian Internet Law. In addition, the Access to Information Law (Law No. 12,527/2011) provides regulation on the access to public information in Brazil.

Constitutional Amendment No. 115/2022 added to Article 5, LXXIX, of the Brazilian Federal Constitution the right to the protection of personal data, including in digital media, as a fundamental right, in addition to the right to privacy and the private life of individuals provided in Article 5, X, of the Brazilian Federal Constitution.

The Brazilian Civil Code also assures individuals with the right to seek judicial relief to prevent the continuous infringement of their privacy rights and the right to claim indemnification for all damages arising thereof (Articles 20 and 21).

The Consumer Protection Code provides for specific rules in connection with the creation of consumer databases (Article 43). The creation of databases with consumer records must be informed to consumers whose information will be collected, and such records cannot contain any negative information that is more than five years old. Consumers must be granted access to information collected about them and they have the right to demand any correction deemed necessary.

The Brazilian Internet Law also establishes rules that apply to application providers; for instance, the Brazilian Internet Law provides for personal data retention obligations. Application providers must store log information (access date and time associated to an IP address) for, at least, six months (Article 15).

1.3 Is there any sector-specific legislation that impacts data protection?

Yes. Specific sectors also have regulations that impact data protection, for instance, the banking, health and electoral sectors.

Banking sector

Entities regulated by the Central Bank of Brazil (“BCB”) are subject to specific law and regulation, such as the Banking Secrecy Law (Supplementary Law No. 105/2001) and the Cybersecurity Regulation (Brazilian National Monetary Council (“CMN”) Resolution No. 4,893/2021, and the Central Bank Circular No. 85/2021), among others.

According to the Banking Secrecy Law, financial entities must keep confidential “all of their credit and debit transactions, as well as the services rendered”. The specific situations in which information may be disclosed without being considered a breach of the Banking Secrecy Law are listed in Article 1, paragraph 3; for example: (i) exchange of information between financial entities or ancillary entities for credit protection; (ii) disclosures determined by law or ordered by a competent authority; and (iii) disclosures expressly authorised by the interested parties (i.e., the client).

The Cybersecurity Regulation provides rules applicable to regulated financial institutions and payment institutions, in connection with certain local requirements for storing and processing data, such as: (i) internal cybersecurity governance requirements; (ii) requirements for hiring outsourced relevant services regarding cloud computing and data processing; (iii) establishing a cybersecurity policy; and (iv) storing data outside Brazil.

The Positive Data Law (Law No. 12.414/2011), Decree No. 9,936/19 and CMN Resolution No. 4,737/19 altogether regulate the creation and management of databases containing information on the payment record of individuals or legal entities, aimed at building a positive credit history.

On May 10, 2020, the CMN and the BCB issued Joint Resolution No. 1/2020 containing the main regulation for the Brazilian Open Finance framework. Open Finance consists of the sharing of customer data and comprises payment initiation services and the forwarding of credit transaction proposals by financial institutions, payment institutions and other BCB-authorised entities through the integration of platforms and infrastructure of information systems.

One of the goals of Open Finance is to facilitate the access to information and to enhance transparency among the institutions and their customers. To that end, the institutions are required to safeguard the security and privacy of data

and services shared within the Open Finance environment, keeping the quality of data and the interoperability among participants. The sharing of customer data is possible only upon the data subject's explicit consent.

BCB Resolution No. 342/2023 amended the BCB Resolution No. 1/2020, which governs the operation of the PIX payment arrangement, to include specific obligations related to the communication of security breaches involving personal data within the PIX infrastructure even when the security incident may not result in harm or damages to the data subjects.

In addition, BCB Resolution No. 304/2023 approves the regulation that governs, within the scope of the Brazilian Payment System, the operation of settlement systems, the performance of registration and centralised deposit activities for financial assets, and the establishment of encumbrances and liens on registered or deposited financial assets and consolidates rules on the matter. Such resolution is applicable not only to regulated entities but to all financial market system operating institutions.

According to Resolution No. 304/2023, the contracting of relevant data processing, data storage and cloud computing services provided outside Brazil must comply with the following requirements: (i) the existence of an information exchange agreement between the BCB and the supervisory authorities of the countries where the services may be provided; (ii) the contracting institution must ensure that the provision of the services does not impair its regular operation nor hinder the actions of the BCB; (iii) the contracting institution must define, prior to contracting, the countries and the regions within each country where the services may be provided and where the data may be stored, processed and managed; and (iv) the contracting institution must provide for alternatives for business continuity in the event of the impossibility of maintaining or the termination of the service contract.

Additionally, Joint Resolution No. 6/2023 establishes requirements for the sharing of data and information regarding indications of fraud among financial institutions and payment institutions regulated or authorised by BCB. The primary objective of this resolution is to enhance fraud prevention procedures and controls by mandating that relevant data – such as information about individuals or institutions involved in actual or attempted fraud, descriptions of fraudulent activities, and details about accounts receiving suspicious funds – be shared through a secure electronic system among covered institutions.

Health sector

Entities in the health industry are subject to the Medical Ethics Code (Resolution CFM No. 2.217/2018), which determines that health professionals must abstain from disclosing any information they become aware of as a result of their activities, unless such disclosure is made with cause, due to a legal obligation or with the previous and explicit authorisation, in writing, of the patient.

Electoral sector

The Superior Electoral Court approved 12 resolutions on rules and guidelines for the elections (for mayor and city councils) that took place in October 2024. Resolution No. 23,732/2024 amends Resolution No. 23,610/2019, which specifically regulates electoral campaigns. According to Resolution No. 23,732/2024, all application providers, political parties and candidates must comply with the LGPD whenever processing personal data and establishing additional obligations.

1.4 What authority(ies) are responsible for data protection?

The Brazilian authority responsible for data protection is the *Autoridade Nacional de Proteção de Dados* (“ANPD”), which was created on December 28, 2018, through the Executive Order (MP) 869/2018, and confirmed by the Federal Law No. 13,853/2019, enacted on July 8, 2019.

The ANPD is a special autonomous agency, endowed with technical and decision-making autonomy, with its own assets, composed of five commissioners appointed by the President.

The ANPD exercises roles of: (i) regulation, issuing regulations, guides and technical notes on the interpretation of the LGPD; (ii) investigation and sanctioning, in cases of non-compliance with the law, through administrative proceedings; and (iii) education, with the responsibility of promoting knowledge of the LGPD and security measures, promoting standards of services and products that facilitate data control and preparing studies on national and international practices for the protection of personal data and privacy, among others.

However, in practice, we have seen other authorities in Brazil enforcing privacy rights through administrative procedures or lawsuits, such as the Department of Consumer Protection and Defense and the Public Prosecutor Office. In addition, individual and collective lawsuits have been filed due to alleged violation of data privacy.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

■ “Personal Data”

In January 2024, the ANPD published a Personal Data Protection Glossary with key definitions related to data protection, which can be accessed at: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/glossario-anpd-protecao-de-dados-pessoais-e-privacidade.pdf>. Personal data is any information related to an identified or identifiable natural person (Article 5, I, LGPD). Name, address, phone number, tax ID number, etc. are all examples of personal data related to an identified person, by which you can easily identify the natural person it refers to. However, there is no criteria under the data protection legislation to define an “identifiable natural person”. While the ANPD does not provide for such criteria, personal data related to identifiable natural persons may be understood as data that, in conjunction with other data, permits you to identify a natural person, such as geolocation or profiles.

■ “Processing”

Processing of personal data includes any activity carried out with personal data. For instance, collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, elimination, information control, modification, communication, transfer, diffusion and extraction are all examples of data processing activities (Article 5, X, LGPD).

■ “Controller”

The controller is the natural person or legal entity, governed either by public or private law, that is in charge of making decisions about the processing of personal data (Article 5, VI, LGPD).

The controller is responsible for determining the purpose of the data processing activity and for appointing the appropriate legal basis for each process, among other obligations.

■ **“Processor”**

The processor is the natural person or legal entity, governed either by public or private law, that processes personal data on behalf of the controller and following the controller’s instructions (Article 5, VII, LGPD).

The processor, along with the controller, are the processing agents (Article 5, IX, LGPD).

■ **“Data Subject”**

The data subject is the natural person to whom the personal data refers to (Article 5, V, LGPD).

■ **“Sensitive Personal Data”/“Special Categories of Personal Data”**

The LGPD also determines sensitive personal data (Article 5, II, LGPD). This subgroup of personal data includes any information regarding a natural person’s race or ethnic origin, religion, political opinion, trade union or religious, philosophical or political organisation membership, health, sex life, genetics or biometrics.

■ **“Data Breach”**

Data breach is defined in the ANPD’s Resolution No. 15/2024, which regulates the data breach notification process (“Resolution CD/ANPD No. 15/2024”). According to Resolution CD/ANPD No. 15/2024, a data breach is any confirmed adverse event related to the violation of the confidentiality, integrity, availability and authenticity properties of personal data security.

For the purpose of clarification, Resolution CD/ANPD No. 15/2024 also defines the following:

- (i) Confidentiality as a quality ensuring that personal data is not available or disclosed to unauthorised individuals, companies, systems, agencies or entities.
- (ii) Integrity as a quality ensuring that personal data has not been modified or destroyed in an unauthorised or accidental manner.
- (iii) Availability as a quality ensuring that personal data is accessible and usable, on demand, by an individual or a specific system, organisation or entity duly authorised.
- (iv) Authenticity as a quality ensuring that information has been produced, sent, modified or destroyed by a specific individual, equipment, system, organisation or entity.

■ **“Anonymised Data”**

Anonymised data refers to data related to a natural person that cannot be identified considering the use of reasonable technical means available at the time of the data processing (Article 5, III, LGPD). Anonymised data are not subject to the LGPD.

■ **“Data Protection Officer”**

The LGPD defines the Data Protection Officer (“DPO”) as a person appointed by the controller and the processor to act as a communication channel between the controller, the data subjects and the ANPD (Article 5, VIII, LGPD).

■ **“Consent”**

Consent is a demonstration of the data subjects that they agree to the processing of their personal data for a specific purpose (Article 5, XII, LGPD). Consent must be free, informed and unequivocal, otherwise the consent would be deemed null and void.

■ **“Data Protection Impact Assessment”**

Data protection impact assessment refers to the documentation drafted by the controller that contains a

description of the personal data processing activities that could result in risks to the civil liberties and to the fundamental rights, as well as measures, safeguards and mechanisms to mitigate risks (Article 5, XVII, LGPD).

■ **“Balancing Test”**

A proportionality assessment carried out by the controller whenever the controller uses the legal bases of “legitimate interest” or “prevention of fraud and security for the data subject in the processes of identification and authentication of registration in electronic systems”, based on the context and specific circumstances of the data processing, taking into account the impacts and risks to the rights and freedoms of data subjects (ANPD’s Guidelines on the lawful bases: Legitimate Interest).

■ **“Joint Controllership”**

The joint, common or convergent determination by two or more data controllers of the purposes and essential elements for carrying out the processing of personal data, through an agreement establishing their respective responsibilities for compliance with the LGPD (ANPD’s Guidelines on Processing Agents Definition and Data Protection Officer).

■ **“Serious Infraction”**

An infraction shall be considered “serious” when: (i) the hypothesis of a medium infraction is verified, and cumulatively, at least one of the following: (a) it involves processing personal data on a large scale; (b) the infringer derives or intends to derive economic advantage from the committed infraction; (c) the infraction poses a risk to the life of the data subjects; (d) the infraction involves processing sensitive data or personal data of children, adolescents or the elderly; (e) the infringer processes personal data without justification under one of the lawful bases provided for in the LGPD; (f) the infringer carries out processing with illicit or abusive discriminatory effects; or (g) the systematic adoption of irregular practices by the infringer is verified; or (ii) it constitutes obstruction to inspection activities (ANPD’s Resolution No. 4/2023 on the dosimetry and application of administrative sanctions (“Resolution CD/ANPD No. 4/2023”).

■ **“Medium Infraction”**

Infraction that significantly affects the interests and fundamental rights of data subjects, characterised in situations where the processing activity could significantly prevent or limit the exercise of rights or the use of a service, as well as cause material or moral harm to the data subjects, such as: discrimination; violation of physical integrity; right to image and reputation; financial fraud; or misuse of identity, provided it is not classified as serious (Resolution CD/ANPD No. 4/2023).

■ **“Minor Infraction”**

Infraction that does not fall within any of the hypotheses related to medium or serious violations (Resolution CD/ANPD No. 4/2023).

■ **“International Transfer”**

Transfer of personal data to a foreign country or international organisation of which the country is a member (Resolution CD/ANPD No. 19/24).

■ **“International Personal Data Collection”**

Collection of the data subject’s personal data carried out directly by the processing agent located abroad (Resolution CD/ANPD No. 19/24).

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Yes. The LGPD may apply to businesses established in other jurisdictions as it provides for extraterritorial reach. The LGPD applies to any data processing activity carried out by natural person or by a public or private legal person, regardless of the country where they are established or the country where the data is hosted, provided one of the following requirements are met: (i) the data processing takes place within the Brazilian territory; (ii) the processing activity is intended to offer or supply goods or services or to process data of individuals located in the Brazilian territory; or (iii) the collection of personal data subject to processing has taken place in the Brazilian territory (Article 3, LGPD).

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

Yes. The LGPD is not applicable when the processing of personal data: (i) is carried out by a natural person for exclusively personal and non-economic purposes; (ii) is carried out for exclusively (a) journalistic and artistic purposes, or (b) academic purposes; (iii) is carried out for exclusive purposes of (a) public security, (b) national defence, (c) state security, or (d) investigation and repression of criminal offences; or (iv) is related to personal data originated from outside the national territory and which are not the subject of communication, shared use with Brazilian processing agents, or international transfer of data to another country other than the country of origin, provided that the country of origin provides a level of personal data protection appropriate to that provided for in the LGPD (Article 4, LGPD).

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
The transparency principle assures data subjects of clear, accurate and easily accessible information on processing activities and on the respective processing agents, with due regard for trade and industrial secrets (Article 6, VI, LGPD).
- **Lawful basis for processing**
Processing of personal data may only occur if in accordance with one of the lawful bases provided by Article 7 (for regular personal data) or Article 11 (for sensitive personal data) of the LGPD.
- **Purpose limitation**
The purpose principle requires personal data to be processed for legitimate, specific and explicit purposes duly informed to the data subject, without any subsequent processing in a manner incompatible with such purposes (Article 6, I, LGPD).
- **Data minimisation**
Data minimisation is linked to the necessity principle. Personal data must be processed to the minimum

extent necessary for achievement of the respective data processing purposes (Article 6, III, LGPD).

- **Proportionality**

The proportionality principle relates to the necessity principle and thus also to data minimisation. Personal data must be processed using pertinent, proportional, non-excessive data. The type and amount of data processed must be in accordance with the intended purpose (Article 6, II and III, LGPD).

- **Retention**

Personal data shall be eliminated at the end of their processing, within the scope and technical limits of the activities, but may be retained for the following purposes: (i) fulfilment of statutory or regulatory obligations by the controller; (ii) studies by research bodies, ensuring, whenever possible, the anonymisation of personal data; (iii) transfer to a third party, to the extent that the data processing requirements set forth in the LGPD are fulfilled; or (iv) exclusive use by the controller, provided they may not be accessed by a third party, and to the extent that the data are anonymised (Article 16, LGPD).

- **Accuracy**

Data subjects shall be assured of accurate, clear, relevant and up-to-date data, to the extent necessary and for achievement of the purposes for which they are processed (Article 6, V, LGPD).

- **Adequacy**

Personal data shall be processed in a manner consistent with the purposes informed to the data subject, taking into consideration the context of such processing (Article 6, II, LGPD).

- **Free Access**

Data subjects shall be assured of the right to make easy and free-of-charge inquiries into processing mechanisms and duration, as well as the integrity of their personal data (Article 6, IV, LGPD).

- **Security**

Technical and administrative measures shall be adopted to protect personal data from unauthorised access and from accidental or unlawful events of destruction, loss, change, communication or dissemination of such data (Article 6, VII, LGPD).

- **Prevention**

Preventive measures shall be adopted to avoid damage from processing of personal data (Article 6, VIII, LGPD).

- **Non-discrimination**

Personal data cannot be processed for discriminatory purposes, i.e., in an unlawful or abusive manner (Article 6, IX, LGPD).

- **Liability and accountability**

The processing agents shall evidence the adoption of effective measures capable of demonstrating unnecessary compliance with personal data protection rules, as well as the effectiveness of such measures (Article 6, X, LGPD).

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to (copies of) data/information about processing**
The right of access to personal data consists of making available or providing to the data subject copies of his or

her personal data processed by the controller (Articles 18, II, and 19, LGPD). The response for the access request can be made online or in writing by delivering the data to the data subject in hard copy.

There are two ways of responding to data access requests, depending on the request submitted by the data subject: (i) by means of a simplified statement, including a summary of the main personal data processed by the controller, provided immediately; and (ii) by means of a complete statement, which must also include the summary referred above, the origin of the data, the lack of records, the criteria adopted for data processing and its purpose, with due regard for trade and industrial secrets, provided within 15 days from the date of the request.

- **Right to rectification of errors**

The right to rectification of incomplete, inaccurate or outdated data consists of correcting any errors concerning personal data of the data subject (Article 18, III, LGPD).

- **Right to deletion/right to be forgotten**

There are two hypotheses of a data subject's right to deletion in the LGPD, as follows:

- (i) The LGPD provides in Article 18, IV, the data subject's right to anonymisation, blocking or erasure whenever the controller is processing his or her personal data in an unnecessary or excessive manner or in violation of the LGPD. Anonymising refers to the use of reasonable and available techniques by which the personal data can no longer be directly or indirectly associated with the data subject. Blocking refers to the temporary suspension of any processing operation carried out with the personal data, keeping the data stored on the controller's database or systems, including an indication that they cannot be used for any other purposes. Erasing refers to removing from the controller's database or systems the personal data, regardless of the procedure being adopted.
- (ii) The LGPD provides in Article 18, VI, that when withdrawing his or her consent for the processing of personal data, the data subject may also request their erasure, with some exceptions as established by Article 16 (e.g., in case of the need to retain the information for compliance with legal or regulatory obligations).

There is no rule on the general right to be forgotten in the LGPD.

- **Right to object to processing**

Article 18, paragraph 2, of the LGPD provides that the data subject has the right to object to the processing of his or her personal data when based on one of the consent waiver events, in the event of non-compliance with the law.

The right to objection consists of ceasing the processing of personal data and suspending further processing activities, i.e., ceasing any further use of the personal data of this data subject.

Additionally, ANPD issued a guide on the practical use of the legitimate interest lawful basis, in which it is stated that the data subject has the right to oppose to the processing of his or her personal data based on the legitimate interest if the data subject believes his legitimate expectations have not been met.

- **Right to restrict processing**

Please see right to deletion above.

- **Right to data portability**

The right to data portability to another service or product supplier consists of providing a copy of the personal

data concerning a data subject to another company, excluding, however, information deemed as business secrets (Article 18, V, LGPD).

The ANPD is expected to regulate the portability right in the near future.

- **Right to withdraw consent**

The right to withdraw consent consists of ceasing data processing carried out on the basis of prior consent, and suspending further processing activities (Article 18, IX, LGPD), i.e., ceasing any further use of the personal data being processed on the basis of the data subject's consent. In most cases, withdrawal of consent will result in the agreement with the data subject being terminated. The consent may be withdrawn at any time upon express notice of the data subject, via free-of-charge and easily accessible procedures.

The withdrawal of consent, however, does not affect processing activities carried out before withdrawal, and in many cases the personal data will continue to be processed if there is another applicable legal basis – for example, events in which personal data should be maintained for compliance with legal obligations.

- **Right to object to marketing**

The right to object to marketing is not explicitly provided by the LGPD. Please refer to the “right to object to processing” right above.

- **Right protecting against solely automated decision-making and profiling**

The data subject has the right to request a review of decisions based solely on automated processing of personal data that affect his or her interests, including decisions intended to define his or her personal, professional, consumption and credit profile or the traits of his or her personality (Article 20, LGPD).

Fulfilment of a request for a review of decisions based on automated processing consists of providing clear and appropriate information concerning the criteria and procedures used for the automated decision, with due regard for trade and industrial secrets.

Differently from data protection laws from other jurisdictions, the LGPD does not explicitly require that the review of decisions based on automated processing include human participation.

- **Right to complain to the relevant data protection authority(ies)**

The data subject has the right to file a petition to the ANPD (Article 18, paragraph 1, LGPD).

- **Right to confirmation**

The right to confirmation of processing consists of informing the data subject on whether the company processes his or her personal data (Article 18, I, LGPD).

There are rare cases where the request is limited solely to confirmation as the data subject usually wishes to have access to his or her personal data as well.

- **Right to be informed about the consequences in case of refusal to consent**

When the controller uses consent as a lawful basis for processing personal data, the data subject has the right to be informed about: (i) the possibility of refusing consent, where feasible; and (ii) the consequences of refusal, which will typically mean the impossibility of using a certain product or service (Article 18, VIII, LGPD).

- **Right to anonymisation or blocking data processing**

Please see “right to deletion” above.

- **Right to request information about data sharing**
Article 18, VII of the LGPD ensures the data subject the right to know with which public and private entities the controller has shared his or her personal data.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

Yes. Article 22 of the LGPD provides that data subjects have the right to exercise their rights in court, whether individually or collectively, which could be made through not-for-profit organisations, to the extent all the requirements provided by Brazilian laws are met.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

The LGPD establishes that children and teenagers' data must be processed in their best interest. Children are individuals from zero to 12 years old (incomplete) and teenagers are individuals from 12 to 18 years old (incomplete).

In May 2023, the ANPD published the Statement CD/ANPD No. 1/2023, which provides that the processing of personal data of children and teenagers can be relied on any lawful basis, provided for in Articles 7 and 11 of the LGPD, and it does not require the consent in every case.

However, if the controller relies on consent to process children's data, the LGPD provides that such consent must be given by a parent or legal guardian in a specific and conspicuous way.

Although not provided in the LGPD, the ANPD sees children, teenagers and elderly people as vulnerable data subjects and therefore requires additional caution from controllers and processors when processing their personal data.

Additionally, it is important to note that other governmental bodies intend to regulate the processing of minors' personal data. This is the case of the National Council for the Rights of Children and Adolescents ("CONANDA"), which published Resolution No. 245/2024 that addresses children and adolescents' rights in virtual environments. For the purpose of Resolution No. 245/2024, "virtual environments" means any information or communication technology, such as: digital networks, content, services and applications available on the Internet; devices and connected environments; virtual and augmented reality; artificial intelligence ("AI"); robotics; and automated systems, biometrics, algorithmic systems and data analysis.

Although there are discussions on whether the CONANDA are purely guidelines or should be interpreted as law, as well as on the unconstitutionality and violation and conflict of laws, Resolution No. 245/2024 establishes specific data protection requirements, such as the prohibition of processing minors' personal data for commercial purposes, such as profiling in connection with consumption, behaviour, and market segmentation and targeted advertisement.

Irrespective of CONANDA's resolutions, the ANPD has ongoing investigation proceedings regarding processing of children and teenagers' personal data.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

No, currently there is no obligation on businesses to register with or notify the ANPD in respect of processing activities.

The LGPD simply provides that controllers and processors must keep records of processing activities (Article 37, LGPD); however, it does not impose obligations on registry of such records.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable; please see above.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable; please see above.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable; please see above.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable; please see above.

7.6 What are the sanctions for failure to register/notify where required?

This is not applicable; please see above.

7.7 What is the fee per registration/notification (if applicable)?

This is not applicable; please see above.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable; please see above.

7.9 Is any prior approval required from the data protection regulator?

This is not applicable; please see above.

7.10 Can the registration/notification be completed online?

This is not applicable; please see above.

7.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable; please see above.

7.12 How long does a typical registration/notification process take?

This is not applicable; please see above.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

According to Article 41 of the LGPD, the controller has the obligation to appoint a DPO; and, on the other hand, according to Resolution CD/ANPD No. 18/2024 issued by ANPD (which approves the regulation on the role of DPO), the data processor does not have the obligation to appoint a DPO, although the appointment could be considered as a good practice.

- **Small Processing Agents.** In the Resolution CD/ANPD No. 2/2022 on small processing agents, the ANPD determined that small processing agents are not obligated to appoint a DPO; however, the appointment of a DPO by a small processing agent would be considered as good practice, which is likely to be considered as a mitigating factor in case of a sanctioning proceeding (Article 11, Resolution CD/ANPD No. 2/2022).

Resolution CD/ANPD No. 18/2024 also provided for the obligation to appoint a substitute for the DPO, for cases in which the DPO is absent for any reason.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

As the appointment of a DPO is mandatory in some circumstances, if a DPO is not appointed, the failure to appoint can be interpreted as a violation of the LGPD.

A violation of the LGPD may result in the following administrative penalties (in addition to civil liabilities): (i) warnings; (ii) fines up to 2% of the revenues earned by the legal entity, group or conglomerate in Brazil in the preceding year, net of taxes, capped at R\$50 million per offence; (iii) daily fines; (iv) disclosure of the offence; (v) blocking of the personal database to which the offence refers, until the processing activity is corrected; (vi) elimination of the personal data to which the offence refers; (vii) partial or total suspension of the operation of the database to which the offence refers for a maximum

period of six months, extendable for the same period; (viii) suspension of the processing of personal data to which the infringement refers for a maximum period of six months, extendable for the same period; and (ix) partial or total prohibition of the performance of any activities relating to data processing.

According to Resolution CD/ANPD No. 4/2023, the definition of which administrative sanctions will be applicable in cases of violation of the LGPD will depend on: (i) the classification of the infraction as “minor”, “medium” or “serious”; and (ii) the ANPD’s understanding of the proportionality of the sanction in relation to the infraction committed.

On November 2024, the ANPD initiated an investigatory proceeding against 20 companies for not appointing a DPO, not disclosing the DPO information or not providing a communication channel to data subjects. ANPD notified the companies to adequate the information of the DPO. On April 2025, the investigatory proceeding was concluded since all the 20 companies complies with the ANPD’s requirements and were deemed to be in compliance with the LGPD.

In view of these precedents, in the specific case of failure to appoint a DPO, ANPD may impose a warning or require the company to nominate a DPO within a certain deadline.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

Neither the LGPD nor the Resolution CD/ANPD No. 18/2024 provides for specific clauses regarding disciplinary measures or other employment consequences for the DPO. The absence of an express civil liability regime regarding the DPO in the LGPD does not exempt the DPO from the fulfilment of legal obligation, such as labour, contractual and civil.

The liability of the DPO will vary according to the DPO’s role in the company’s organisation. For example, in case the DPO is a statutory director, its liabilities would be similar to those of the statutory directors of limited liability companies; in case the DPO is a non-statutory director, its liabilities would be limited to specific liabilities of employees; and in case the DPO is a third party hired to act as DPO, its liabilities would be those specified in the agreement.

However, Resolution CD/ANPD No. 18/2024 made it clear that the DPO role does not attract personal liability to the DPO for companies’ non-compliance with the LGPD.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

Resolution CD/ANPD No. 18/2024 allows the DPO to perform multiple roles and carry out their activities for more than one data controller, provided that they are able to fully meet their responsibilities related to each controller and that no conflict of interest exists.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

The LGPD does not require specific requirements or certifications for the DPO role. Resolution CD/ANPD No. 18/2024 provides that the DPO may be: (i) a natural person, a member of the organisational framework of the processing agent or external to it; or (ii) a legal entity.

However, Resolution CD/ANPD No. 18/2024 provides that the DPO must be able to communicate in Portuguese with the ANPD and data subjects.

Article 7 of the regulation approved by Resolution CD/ANPD No. 18/2024 states that the company that appoints the DPO is responsible for determining the required qualifications for the DPO.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

According to the LGPD, the DPO has the following duties: (i) intermediate the communication between the company and data subjects; (ii) intermediate the communication between the company and the ANPD, and implement any relevant measures arising from such communication; (iii) educate the company's employees and contractors regarding data protection practices; and (iv) perform other attributions determined by the company or by complementary rules, not yet provided by the ANPD.

In addition to such provisions, Resolution CD/ANPD No. 18/2024 provides that supplementary duties of the DPO include assisting the processing agent in relation to: (i) drafting communication regarding personal data security incidents; (ii) drafting the record of personal data processing operations; (iii) drafting the data protection impact assessment; (iv) identification and analysis of risks related to personal data processing; (v) definition of technical and administrative security measures to protect personal data from unauthorised access and from accidental or unlawful situations of destruction, loss, alteration, communication, or any form of improper or unlawful processing; (vi) implementation of internal policies and procedures to ensure compliance with the LGPD and ANPD regulations; (vii) analysis of contractual clauses with third parties regarding personal data protection; (viii) international data transfers; (ix) creation and implementation of good practices and governance rules, and a privacy governance programme; (x) carrying out privacy by design analysis in products and services; and (xi) other activities and strategic decision-making regarding processing of personal data.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

The DPO must be appointed through a formal document, i.e., through a written, dated and signed document. However, such appointment does not need to be registered or notified to the relevant authorities; the full name and contact details of the DPO must, on the other hand, be made publicly available, as described in question 8.8 below.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

Article 41, paragraph 1 of the LGPD provides that the identity and contact information of the DPO must be publicly, clearly and objectively disclosed, preferably on the company's website.

Resolution CD/ANPD No. 18/2024 reinforces such provision and provides that the identity information must cover, at least: (i) the full name of the DPO, if the DPO is a natural person; or (ii) the corporate name or title of the establishment, as well as the full name of the natural person responsible for the entity, if the DPO is a legal entity.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

The LGPD does not have any requirements for businesses to enter into any form of agreement with their processors and the ANPD has not yet issued any requirements or regulated this topic.

Notwithstanding the lack of specific legal requirement, it is highly recommended for businesses to enter into agreements with their processors in order to establish the parties' compliance with the LGPD and any other data protection rules, the extent of the parties' responsibilities and liabilities within the scope of their activities under contract, the measures to be taken in case of a data breach, collaboration in relation to the fulfilment of the data subject's rights, mechanisms applicable in case of cross-border data transfer, the obligation to retain or delete information stored by data processors, and effects of the contract termination, among other obligations.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The LGPD does not provide for any requirements for businesses to enter into any form of agreement with their processors, as explained above.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Currently, there is no specific general regulation on the sending of electronic direct marketing; however, there are laws and regulations applicable to the matter: (i) the Brazilian Consumer Protection Code; (ii) the LGPD; (iii) regulation issued by the National Telecommunications Agency ("Anatel"); and (iv) state laws for "do-not-spam".

The Brazilian Consumer Protection Code does not contain any specific provision regarding direct marketing actions; however, it establishes several obligations to the advertisers and suppliers that are applicable to such actions. Among other obligations, messages should have an opt-out option to give the consumer the option to stop receiving direct marketing messages.

The LGPD requires a lawful basis to process data. There are discussions regarding the lawful bases that would be applicable to such practices, mainly consent or legitimate interest would apply.

Anatel has issued regulation related to the delivery of marketing via short message service ("SMS") and massive phone calls. Anatel's rules apply in principle to mobile carriers only. Among other requirements, an opt-in must be obtained, an opt-out option must be offered, and information must be clear and detailed.

Under the state laws for "do-not-spam", consumers are given the option to add their contact details to a "do-not-spam" list.

The data subjects with contact details in that list must not be contacted with marketing content, be it phone calls, SMS and, in some cases, even email. The scope may vary with each state.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

There is no specific general regulation on the sending of electronic direct marketing in a business-to-business context. In any case, state laws for “do-not-spam” as provided above shall apply for business-to-consumer marketing.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Currently, there is no specific general regulation on the sending of electronic direct marketing. Please refer to question 10.1 above for a general overview of the Brazilian regulatory system.

Restrictions may apply in other specific scenarios. The Brazilian Bank Federation and the Brazilian Bank Association developed a self-regulation system for payroll-linked loans. In this system, bank clients may opt to not be contacted about payroll-linked loans.

Anatel decided for the creation of a “non-disturbance” national list for consumers who do not wish to receive calls offering specific products and services (such as telecommunication services and payroll-deductible loan or credit card offering).

In 2021, Anatel issued Act No. 1,0413/2021, now replaced by Act No. 13,762/2022, which approved the Operating Procedures for the Assignment of Numbering Resources, by which it became mandatory for the companies that perform telemarketing activities to adopt the allocation of the non-geographic code (CNG) 0303, prohibiting, for this purpose, the use of any other codes. This way, consumers can identify the originator of the call and decide whether to attend the call.

On September 4, 2024, through Act No. 12.712, Anatel expanded the use of 0303, determining that companies that make more than 10,000 daily calls must adopt the prefix, effective from March 2025. According to the Act, companies that make more than 10,000 calls per day and that do not comply with the new rules will have their calls blocked.

Additionally, mechanisms such as opt-outs are recommended as good practice for businesses whenever the company relies on legitimate interest and not on consent in relation to marketing activities.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The above-mentioned provisions are applicable to any marketing communication made in the Brazilian territory or whenever there is a consumer relationship regulated by Brazilian law. In relation to the LGPD, it clearly establishes an extraterritorial reach as provided in the answer to question 3.1 above.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Considering there is no specific restriction on marketing established by the ANPD, the ANPD may verify if marketing activities are carried out in accordance with the LGPD.

The first enforcement decision issued by the ANPD was directed to a telemarketing company that processed personal data without a proper lawful basis. The penalty for such violation of the LGPD was a fine in the total amount of 2% of the company’s revenue per offence.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Although there is no prohibition in the law on the purchase of marketing lists from third parties, the ANPD’s first enforcement decision was related to the provision of marketing lists for electoral candidates. In view of this, if a company is willing to receive marketing lists from third parties, it is recommended that the company ensures the third party complies with data protection laws and regulation, as well as the company itself assessing whether such data processing, in that specific case, is lawful.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Non-compliance with the applicable laws may result in sanctions and penalties that will depend on the type of violation. In case of violation of the LGPD, specific administrative penalties are provided in Articles 52 to 54 (as detailed in the answer to question 8.2); in case of violation of the Brazilian Consumer Protection Code, penalties therein provided shall apply. Notwithstanding the foregoing, individual and collective lawsuits could be filed due to alleged violation of data privacy or consumer rights, seeking for indemnification for material and moral rights.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

Differently from the European Union, cookies or similar tracking technologies are not regulated in Brazil by a specific rule/regulation.

On October 18, 2022, the ANPD published on its website a Guide on Cookies and Personal Data Protection (“Cookies Guidelines”), which aim to provide processing agents with good practices related to the subject. The Cookies Guidelines present conceptual issues about cookies and similar tracking technologies, dividing them into categories (e.g., first-party cookies, third-party cookies, necessary cookies and non-necessary cookies, among other classifications).

The Cookies Guidelines also discuss the recommended legal bases for the processing of personal data through cookies and similar tracking technologies, which should be defined according to the categories of cookies. The guidelines further recommend that processing agents develop a cookie policy, which may be presented: (i) as a specific section in the privacy

policy; (ii) in a specific and separate location; or (iii) in the cookie banner itself, provided that the cookie policy contains clear, precise and easily accessible information on the data processing.

Finally, the Cookies Guidelines provide instructions on how to design cookie banners, including indications of: (i) how the data subjects' rights should be presented; (ii) what information should be present; (iii) how the data subjects can manage cookies; and (iv) what should be avoided when designing the banners.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

As explained above, there are no specific restrictions applicable to cookies, but only specific guidance issued by the ANPD.

The Cookies Guidelines provide for the following types of cookies:

- (i) First-party or primary cookies: are cookies directly defined by the website or app that the data subject is visiting. Generally, primary cookies cannot be used to track activity in a website other than the original website in which they were put. This type of cookie can include information such as login credentials, shopping cart items or preferred language.
- (ii) Third-party cookies: are cookies created by a domain other than the one that the data subject is visiting. They derive from functionalities of other domains that are embedded on a website, as in the display of adverts.
- (iii) Necessary cookies: are those used for the website or app to carry out basic functions or correctly operate. For this reason, the collection of information is essential to ensure functioning of the website or for proper provision of services. Therefore, the activities addressed as strictly necessary include those related to a specific functionality of the service.
- (iv) Non-necessary cookies: are cookies that do not fall within the definition of necessary cookies and disabling these cookies will not impair functioning of the website or app or use of services by users. Within this context, non-necessary cookies are related to non-essential functionalities of the service, app or website.
- (v) Analytical or performance cookies: collect data and information about how users use the website, which pages they more frequently visit on that website, the occurrence of errors, or information about the performance of the website or app.
- (vi) Functionality cookies: are used to provide basic services requested by users and allow to remember preferences of the website or app, such as the user name, region or language.
- (vii) Marketing cookies: are used to collect the data subject information with the purpose of displaying adverts. More specifically, from the collection of information about the user's browsing habits, the marketing cookies allow their identification, the building of profiles and the display of personalised adverts.
- (viii) Session or temporary cookies: are designed to collect and store information while data subjects access a website. They are usually deleted after the end of a session.
- (ix) Persistent cookies: the data collected by cookies are stored and may be accessed and processed by the controller for a definite period, which may vary from some minutes to multiple years.

According to the ANPD's examples set forth in the Cookies Guidelines, the "consent" lawful basis is the appropriate lawful basis for non-necessary cookies. On the other hand, the "legitimate interest" lawful basis is the appropriate lawful basis for necessary cookies.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

The ANPD has not yet taken any enforcement action in relation to cookies.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

As provided above, there is no specific regulation on cookies or similar technologies and therefore there are no specific penalties for breaches of restrictions. However, it is expected that all processing of personal data through cookies complies with the LGPD.

In case a processing activity related to the use of cookies is in violation of the LGPD, the administrative penalties described in question 8.2 may apply, in addition to complaints or lawsuits filed by other authorities or the data subject itself.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The transfer of personal data to other jurisdictions is only permitted in accordance with the instances set forth by the LGPD, such as: (i) for cross-border transfers to third countries or international organisms with adequate protection on the same level as established by the LGPD (a list of countries will be issued by ANPD); (ii) transfers that are necessary for international legal cooperation among intelligence, investigation and prosecution bodies; (iii) transfers that are necessary to protect the life or physical integrity of the data subject(s) or others; (iv) transfers authorised by the ANPD; (v) transfers under international cooperation agreements; (vi) transfers that are necessary for executing or enforcing public policies or public services; (vii) transfers with the specific consent of the data subject; (viii) transfers that are necessary for the fulfilment of a legal or regulatory obligation, for the execution of a contract or preliminary procedures relating to a contract to which the data subject is a party, on the request of the data subject, or for the regular exercise of rights in the course of judicial, administrative or arbitration proceedings; and (ix) when the controller ensures safeguards through the use of specific contractual clauses, standard contractual clauses ("SCCs"), global corporate clauses, seals, certificates or codes of conduct.

On August 23, 2024, the ANPD enacted Resolution CD/ANPD No. 19/2023, which establishes the Regulation on International Data Transfers, pursuant to Articles 33–36 of the LGPD. The Regulation on International Data Transfers outlines the rules and procedures for recognising the adequacy of foreign countries or international organisations and sets forth contractual mechanisms for the international transfer of personal data.

Among the mechanisms regulated are the SCCs, which define the minimum safeguards and conditions required for

international data transfers. Data controllers and processors relying on SCCs must incorporate the ANPD-approved clauses into their contractual instruments by August 23, 2025. The template (Portuguese and English versions) of the SCCs is available on ANPD's website.

The regulation also provides for the possibility of using specific contractual clauses and global corporate rules ("BCRs"). BCRs apply to intra-group international data transfers and require prior approval from the ANPD. These rules must include, among other elements, a commitment to implement a privacy governance programme, a description of the international transfers covered by the BCRs, the identification of the destination countries, and a list of the entities within the corporate group to which the rules apply.

Specific clauses may be adopted in exceptional cases where it is demonstrably unfeasible to use the SCCs. These must ensure an equivalent level of data protection to that provided by the SCCs and must be tailored to the particularities of the transfer operation. Such clauses must be approved by ANPD.

Please note that in case of federal administrative public entities, restrictions to the storage of data outside Brazil may apply.

Sectorial rules may impose requirements to the storage of data outside Brazil in the financial market, such as BCB Resolution No. 304/2023, applicable to all financial market system operating institutions (as detailed in question 1.3 above) and the cybersecurity regulation that applies to entities regulated or authorised by the BCB (Resolution No. 4,893/2021 and Resolution No. 85/2021).

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Please refer to the response to question 12.1. above. The most-used mechanism is SCCs.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

International transfers do not require registration/notification or prior approval from the national authority. However, approval from the ANPD is one of the legal instances set forth by the LGPD that allows international transfers.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

There is no legal requirement to draft a transfer impact assessment for international transfer of personal data. Regardless, whenever the international transfer is deemed as a high-risk activity, the controller must fill out a data protection impact assessment (applicable to any and all high-risk data processing activity).

According to Resolution CD/ANPD No. 2/2022, a processing activity will be considered as a high-risk activity when it cumulatively meets at least: (i) general criteria; and (ii) specific criteria.

General criteria are: (i) processing on a large scale (i.e., when processing involves a significant number of data subjects, also considering the volume of data involved, as well as the duration, frequency and geographical scope of the processing); or (ii) processing that may significantly affect data subjects' interests and rights (i.e., when the processing may prevent the exercise of rights or the use of a service, as well as cause property or moral damage to the data subjects, such as discrimination, violation of physical integrity, of the right to image, and reputation, financial fraud or identity theft).

A processing activity will meet a specific criterion whenever the processing involves: (i) monitoring or control of public accessible areas; (ii) automated processing; (iii) emerging or innovative technologies; or (iv) sensitive data or children's, adolescents' and elderly's data.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

No official guidance has been issued by the authorities in Brazil.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

As mentioned above, the Regulation on International Data Transfers includes the official SCCs for international data transfers under the LGPD, available here in English: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/regulation-on-international-transfer-of-personal-data.pdf>

These SCCs, detailed in Annex II of the Regulation on International Data Transfers, establish minimum safeguards and conditions for lawful cross-border transfers of personal data. To be valid, the SCCs must be adopted in full, without modification, either as standalone agreements or as annexes to broader contracts, provided that no other provisions contradict or alter their content.

The Regulation on International Data Transfers mandates that data controllers and processors utilising SCCs must incorporate the ANPD-approved clauses into their contractual instruments by August 23, 2025. Additionally, the regulation requires controllers to provide data subjects with access to the full text of the SCCs upon request within 15 days and to publish clear, accessible information about international data transfers on their websites.

Furthermore, the ANPD's regulation allows for the recognition of foreign SCCs as equivalent to the Brazilian SCCs, subject to a formal approval process before ANPD. Interested parties may request such recognition by submitting the foreign clauses, translated into Portuguese, along with relevant legislation and a compatibility analysis with the LGPD. The ANPD will assess whether the foreign clauses ensure a level of data protection equivalent to that guaranteed by the national SCCs and consider the potential impacts on international data flows and diplomatic relations. Once approved, these equivalent

clauses will be published on the ANPD's website and can be used as valid mechanisms for international data transfers.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The Anticorruption Law in Brazil (Law No. 12,846/2013) and its related Decree No. 8,420/2015 include the existence of a whistle-blower hotline as a parameter for the integrity programme of a company. The whistle-blower hotline must be open to all employees and third parties, be widely advertised, and must have protection mechanisms for the whistle-blowers in good faith. The current legislation does not specify or limit the permitted scope for the hotline.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is encouraged as one of the protection mechanisms, as mentioned in guidelines issued by the *Controladoria Geral da União*.¹

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

No. The use of CCTV currently does not require registration, notification and/or prior approval from the ANPD. However, as the use of CCTV involves the processing of personal data, the controller must comply with the LGPD's principles and obligations and ensure all reasonable technical and administrative security measures are taken to guarantee the protection of the data, including the implementation of a privacy governance.

As provided in question 12.4 above, monitoring or control of public accessible areas is one of the specific criterion to identify a high-risk activity. In view of this, whenever using CCTV, companies must verify if any general criteria is met to evaluate if the processing activity is deemed as a high-risk activity and therefore requires a data protection impact assessment.

In addition, there are local and regional laws to guide and determine the adoption of additional procedures, such as those referring to the affixing of signs indicating the filming procedures; for example, São Paulo's Municipal Law No. 13,541/2003, which provides for the placement of a visible sign about filming environments and Decree No. 43,236/2003, which regulates such Municipal Law.

14.2 Are there limits on the purposes for which CCTV data may be used?

Neither the LGPD nor the ANPD have specifically regulated limits on the purposes for which CCTV data may be used. However, as any other processing activity, the use of CCTV

data must follow the LGPD's principles and obligations. Therefore, the process must be: (i) for legitimate, specific and explicit purposes, of which the data subject is informed; (ii) compatible with the purpose notified to the data subject; (iii) limited to the minimum necessary for the achievement of the purpose of which the data subject is informed; (iv) clearly notified to the data subject; (v) protected against unauthorised use or access by technical and administrative measures; and (vi) conducted in such a way that prevents discrimination.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

The LGPD does not regulate employee monitoring and the ANPD has not yet provided any specific guidance or regulation regarding this subject. However, under Brazilian labour legislation, employers have the ability to determine how employees should render their services as well as behave in the workplace. This ability, which is commonly referred to as "employers' directive power", may include: (i) monitoring the company's email address provided to the employee; (ii) supervising the type of information and/or content that employees should not have access to while using company's devices (e.g., private or improper material); (iii) creating and implementing general rules on how the company's devices should be used if owned and granted by the company to employees for the rendering of services (e.g., must not be taken home, should not be used for personal purposes, etc.); and (iv) placement of a CCTV system.

Therefore, if the monitoring activity can be justified by a lawful basis provided by the LGPD and is not in violation of the law (specifically privacy rights), it may be performed by the employers. It is important to note that controllers (employers) must keep records of all personal data processing in a manner that it is able to demonstrate compliance with the LGPD, adopt technical and organisational security measures to protect personal data from unauthorised access and from accidental events or unlawful destruction, loss, modification, communication, dissemination or any other occurrence arising from improper or unlawful processing, and provide data subjects with sufficient information regarding the processing activities.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

The consent of the employee is not always required since there are other legal bases that could justify the processing activities related to employee monitoring, such as the regular exercise of rights in case of judicial, administrative or arbitral proceedings, execution of the employment agreement and legitimate interest, depending on the purposes of the processing. If the processing involves sensitive data, the adequate legal bases could be the regular exercise of rights in contracts and in case of judicial, administrative or arbitral proceedings, or ensuring fraud prevention and safety of data subjects in identification and record authentication proceedings in electronic systems, depending on the purposes of the data processing.

However, to comply with the LGPD principles, the data controllers (employers) must give transparency to the data subjects (employees) on the processing of their personal data. This means that the controller must inform the data subject of the personal data being processed and the purposes of such processing among other things, such as the data subjects' rights regarding these personal data.

This can be carried out through a general privacy notice providing all processing activities with employees' personal data, or through specific privacy notices according to the monitoring activity being performed; for instance, when providing employees with a company phone or computer devices.

15.3 To what extent do works councils/trade unions/ employee representatives need to be notified or consulted?

Currently, there is no regulation indicating that work councils, trade unions and/or employee representatives should be notified or consulted for the employer to perform employee monitoring.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

Yes. At the time of writing, there is no restriction on the monitoring of employees' attendance in office, provided the processing activity is carried out in accordance with the LGPD.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes. The security of personal data is not only an obligation, but also a principle in the LGPD (Articles 6, VII, 46 and 50 of the LGPD). It is necessary for all parties involved in the processing of personal data (controllers and/or processors) to ensure and adopt technical and administrative measures to protect personal data from unauthorised access and from accidental or unlawful events of destruction, loss, change, communication or dissemination of such data.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes. Article 48 of the LGPD establishes that the data controller must notify the ANPD and the data subjects about the occurrence of a security incident that may result in risks or relevant damages to the data subjects.

In line with LGPD obligation, Resolution CD/ANPD No. 15/2024 (on the security incident notification proceeding) states that the controller has the obligation to notify the ANPD about the occurrence of a security incident that may result in risks or relevant damages to the data subjects within three business days from the date the controller became aware that the security incident involved personal data. Resolution CD/ANPD No. 15/2024 provides in Articles 4 and 5 the interpretation of the requirements to an incident to configure an event that may result in risks or relevant damages to the data subjects.

Communication to the ANPD must be carried out through a specific system of the ANPD (known as SUPER/ANPD) and must include all the information required in a specific form

available by ANPD, including: (i) the description of the nature and category of personal data affected; (ii) the number of affected data subjects, breaking down, where applicable, the number of children, adolescents or elderly people; (iii) the technical and security measures used to protect personal data, implemented before and after the incident, observing commercial and industrial secrets; (iv) the risks related to the incident with identification of possible impacts on data subjects; (v) the reasons for the delay, in case the communication was not carried out within the expected deadline; (vi) the measures that have been or will be adopted to reverse or mitigate the effects of the incident on the data subjects; (vii) the date of occurrence of the incident, when possible to determine, and the date of its knowledge by the controller; (viii) information on the DPO or whoever represents the controller; (ix) identification of the controller and, if applicable, a statement that it is a small processing agent; (x) processor identification, when applicable; (xi) description of the incident, including the main cause, if it is possible to identify it; and (xii) the total number of data subjects whose data is processed in the processing activities affected by the incident.

If controller does not have all the information, it can submit a preliminary communication on the data breach within the three business days, and a complementary version of the communication within 20 business days.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes. As provided above, Article 48 of the LGPD provides for the controller obligation to notify the data subjects of the occurrence of a security incident that may result in risks or relevant damages to the data subjects. Resolution CD/ANPD No. 15/2024 provides in Articles 4 and 5 the interpretation of the requirements to an incident to configure an event that may result in risks or relevant damages to the data subjects. Whenever the controller communicates the ANPD, it will have to communicate the data subjects, as the same requirements will apply to both cases (obligation to notify ANPD and data subjects).

Resolution CD/ANPD No. 15/2024 states that data subjects must also be notified of the security incident within three business days from the date the controller became aware that the security incident involved personal data.

Communication to the data subject must include, at least: (i) the description of the nature and category of personal data affected; (ii) the technical and security measures used to protect data, observing commercial and industrial secrets; (iii) the risks related to the incident with identification of possible impacts on data subjects; (iv) the reasons for the delay, if the communication was not made within the deadline; (v) the measures that have been or will be implemented to reverse or mitigate the effects of the incident, when applicable; (vi) the date of knowledge of the security incident; and (vii) a contact for obtaining information and, when applicable, the contact details of the DPO.

16.4 What are the maximum penalties for personal data security breaches?

The LGPD does not provide for specific penalties applicable to a data breach. The ANPD reviews the circumstances of

the data breach in order to confirm if a violation to LGPD has occurred or not in the specific event. In any case of violation of the LGPD, specific administrative penalties are provided in Articles 52 to 54 (as detailed in the answer to question 8.2). In addition, other competent authorities may investigate the incident (such as the Public Prosecutor Office) and/or individuals/entities representing individuals that suffered damages may file claims before Courts.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

- (a) **Investigative powers:** The ANPD has administrative powers to apply sanctions and thus requires a proper prior investigation. The sanctions shall be applied after conclusion of an investigative proceeding and commencement of an administrative sanctioning proceeding that gives the offender the opportunity of full defence, in a gradual, isolated or cumulative form, according to the features of the concrete case, and considering the lawful parameters and criteria. The ANPD may apply precautionary measures in the beginning of the investigation.
- (b) **Corrective powers:** The ANPD has administrative powers to apply sanctions determined by the LGPD, such as: (i) warning, with indication of a deadline for the adoption of corrective actions; (ii) blocking of the personal data to which the offence refers, until the processing activity is regularised; (iii) erasure of the personal data to which the offence refers; (iv) partial suspension of the database to which the infringement refers for a maximum period of six months, extendable for the same period, until the processing is regularised by the controller; (v) suspension of the processing of personal data to which the infringement refers for a maximum period of six months, extendable for the same period; (vi) partial or total prohibition on data processing activities; and (vii) disclosure of the offence after the occurrence thereof has been duly investigated and confirmed.
- (c) **Authorisation and advisory powers:** The ANPD is responsible for the issuance of technical opinions and recommendation.
- (d) **Imposition of administrative fines for infringements of specified legal provisions:** Among the possible applicable sanctions by the ANPD in case of violation of the LGPD, there are administrative fees such as: (i) a one-off fine of up to 2% of the revenues earned by the legal person, group or conglomerate in Brazil in the preceding year, net of taxes, capped at R\$50 million per offence; and (ii) a daily fine, subject to the cap referred to above.
- (e) **Non-compliance with a data protection authority:** In case of non-compliance with the ANPD's binding rules, the offender could be subject to the same sanctions described above. In addition, in case of non-compliance with the ANPD's decision, daily fines could be applicable as established by the LGPD.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

Some of the administrative sanctions to be applied by the ANPD stated in the LGPD provide for the suspension of the

processing of personal data and partial or total prohibition on data processing activities. The application of these sanctions does not require a court order and can be imposed by ANPD.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The ANPD is still focusing on its educational powers, by way of issuing public consultations and calls for contribution for the issuance of guidelines and regulations.

However, the ANPD has initiated its sanctioning processing in July 2023. The ANPD has disclosed a list of nine sanctioning proceedings that are currently in place. Only one sanctioning procedure relates to a private legal entity, as described below.

On July 6, 2023, the ANPD issued its first decision in the context of an administrative proceeding against a private entity, regarding violation of the LGPD by a telemarketing company, which allegedly sold phone numbers of electors in the context of electoral campaigns. The company's infraction allegedly consisted in the lack of: (i) applicable lawful basis for its processing activities; (ii) appointment of the DPO; and (iii) collaboration with the ANPD's requests. The ANPD's decision resulted in the imposition of administrative sanctions (warning and fines up to 2% of the company's revenue).

In addition, the ANPD is currently conducting several high-profile enforcement actions under the LGPD. These include supervisory procedures against:

- a social media network company for alleged violations related to the processing of children's and adolescents' personal data – specifically regarding the platform's failure to implement adequate age verification mechanisms; and
- a messaging company to evaluate whether its data-sharing practices comply with transparency and consent requirements under the LGPD.

The ANPD has also initiated sector-wide investigations, including:

- Data protection practices in the pharmaceutical industry, particularly focusing on loyalty programmes and personal data use.
- LGPD compliance in the use of facial recognition technologies by 23 football clubs for ticketing and stadium access.

Most recently, the ANPD ordered a company to suspend alleged incentives linked to the processing of data, citing risks to fundamental rights.

These cases demonstrate the ANPD's expanding oversight across both private and public sectors, demonstrating its focus on supervisory actions before initiating sanctioning procedures.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

Yes, the ANPD has already filed investigations against business established in other jurisdictions that provides products and services to Brazilian users, and collects data from Brazilian users. In one of the cases, the ANPD has imposed a precautionary measure to make it to cease part of its activities.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

The Brazilian Code of Civil Procedure does not provide for a broad discovery phase, as it occurs, for example, in the U.S. Therefore, the scope and depth of disclosure will mostly rely on a case-by-case analysis, that will take into account the facts and concrete elements of the case and the fulfilment of the basic legal requirements for the discovery.

Brazil has declared, under Article 23 of the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, that it will not execute letters of request (letters rogatory) issued for the purpose of obtaining pre-trial discovery of documents. In spite of that, the Superior Court of Justice has executed certain letters rogatory on pre-trial discovery under the understanding that the aforementioned declaration “is not to block the search for evidence abroad, but to prevent abuse” (CR 13559-US). Once again, a case-by-case analysis will be necessary.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

Currently, there is no guidance from the ANPD regarding e-discovery requests or requests for disclosure from foreign law enforcement agencies.

19 Artificial Intelligence

19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?

Under Brazilian law, particularly Article 20 of the LGPD, data subjects have the right to request a review of decisions made solely through automated processing of personal data (using AI or not), that affect their interests. This includes decisions related to creditworthiness, professional profile, consumer behaviour, or other aspects of their personality. Additionally, controllers shall provide, if requested by the data subject, clear and adequate information on the criteria and procedures used in automated decision-making processes, while preserving commercial and industrial secrecy.

To clarify the scope and practical implementation of these safeguards, the ANPD conducted a public consultation between November 2024 and January 2025, focusing on the automated processing of personal data and the use of AI. Following this initiative, the ANPD consolidated the contributions and published Technical Note No. 12/2025/CON1/CGN/ANPD, which sets out preliminary interpretations and regulatory considerations.

19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?

In addition to Technical Note No. 12/2025/CON1/CGN/ANPD mentioned above, ANPD released the third volume of

its “Technology Radar” series, titled “Generative Artificial Intelligence”,² providing an in-depth analysis of generative AI models and their implications for data protection.

Also, in August 2024, the ANPD lifted the preventive suspension previously imposed on a social network platform regarding the use of personal data for training its generative AI systems. This decision followed the social network platform’s submission of a Compliance Plan, which includes several commitments to align its data processing activities with the LGPD. Key measures outlined in the plan involve enhancing transparency through clear notifications to users about data processing for AI training and providing simplified mechanisms for users and non-users to opt-out.

20 Trends and Developments

20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

Over the past 12 months, enforcement activity under the LGPD has increased. While the ANPD began imposing administrative penalties in 2023 – primarily targeting public entities, which are not subject to monetary fines under Resolution CD/ANPD No. 4/2023 – a growing trend involves closer scrutiny of the private sector and the tech industry. Notably, on July 6, 2023, the ANPD issued its first sanction against a private entity: a very small telemarketing company found to have processed voter data without legal basis. The company was sanctioned for failing to appoint a DPO (Article 41), lacking an appropriate legal basis (Article 7), and not cooperating with the ANPD (Article 5 of Resolution No. 1/2021). Sanctions included a warning and two monetary fines.

In 2024, enforcement actions became increasingly focused on high-profile cases involving complex data processing practices. For example, the ANPD investigated social media network platform’s use of personal data for training generative AI systems. Following a preventive suspension, the social media network was only permitted to resume data use after submitting a compliance plan.

In 2025, additional enforcement initiatives targeted facial recognition practices by football clubs, data practices in the pharmaceutical retail sector, and loyalty programmes, as well as alleged incentives tied to data processing activity.

These cases indicate a probable enforcement trend: the ANPD is moving beyond foundational compliance to scrutinise emerging technologies, especially in contexts involving children, biometric data and AI.

20.2 In your opinion, what “hot topics” are currently a focus for the data protection regulator?

The ANPD has identified several key focus areas for 2025–2026, as outlined in its Regulatory Agenda, reflecting a growing effort to address emerging technologies and high-impact data processing practices.

One of the central topics is the regulation of AI and automated decision-making. The ANPD aims to clarify the scope and application of Article 20 of the LGPD – particularly concerning data subjects’ rights in the context of automated decisions – and to develop rules on the governance and legal bases applicable to AI-driven data processing.

Another major area of focus is the protection of children’s and adolescents’ personal data. The ANPD intends to issue

specific rules on parental consent and age verification in digital environments, aligned with international standards such as the OECD Recommendation on Children in the Digital Environment.

Additionally, the ANPD plans to address the legal basis for credit protection activities. The regulatory agenda includes the development of specific guidance on the interpretation and operationalisation of Article 7, section X, of the LGPD, which provides for data processing when necessary to ensure the protection of credit.

Other hot topics include detailed regulations on data subject rights (such as access, correction, deletion and portability), the implementation of Data Protection Impact Assessments for high-risk processing, technical and administrative security measures, biometric data processing, and data sharing by public authorities.

As of 2025, Brazil is actively advancing a regulatory framework for AI through Law Bill No. 2,338/2023 (“AI Bill”), introduced by Senator Rodrigo Pacheco. The AI Bill was approved by the Federal Senate in December 2024, following significant input from multiple sectors and the Internal Temporary Committee on Artificial Intelligence, and is currently under review in the House of Representatives.

Endnotes

- 1 Available at: <https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/integridade/arquivos/programa-de-integridade-diretrizes-para-empresas-privadas.pdf>
- 2 Available here in English: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-inteligencia-artificial-generativa-versao-em-lingua-inglesa.pdf>



Larissa Galimberti specialises in technology, licensing, data protection and intellectual property law. With a focus on cutting-edge technologies, digital platforms and the sharing economy, Larissa brings a wealth of expertise in navigating complex legal matters in the rapidly evolving tech landscape. Her proficiency in software, data analytics, IoT, cybersecurity, media and entertainment, as well as her adeptness in handling agreements involving intellectual property rights, make her an invaluable asset in safeguarding the interests of Brazilian and international clients.

Pinheiro Neto Advogados

Rua Hungria, 1100, Jardim Europa
São Paulo, SP
Brazil

Tel: +55 11 3247 6265

Email: lgalimberti@pn.com.br

LinkedIn: www.linkedin.com/in/larissagalimbertiafonso



Luiza Fonseca de Araujo assists national and international clients in the advisory sphere, focusing on topics related to technology, data protection, AI and intellectual property. She has experience in structuring digital platforms, product development, adapting activities to data protection legislation, administrative proceedings with the National Data Protection Authority, and regulatory analysis related to AI.

Pinheiro Neto Advogados

Rua Hungria, 1100, Jardim Europa
São Paulo, SP
Brazil

Tel: +55 11 3247 6331

Email: laraujo@pn.com.br

LinkedIn: www.linkedin.com/in/luiza-araujo



Cecília Alberton Coutinho Silva is a lawyer specialised in technology, with a focus on the global regulatory and transactional spheres such as data protection, crypto assets, blockchain, AI and cybersecurity. She holds a Master's degree in Law and Technology from Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS), with research on facial recognition and regulatory modalities by private entities. Currently, she assists companies in leveraging technology across its various aspects, providing innovative legal solutions to drive business growth while ensuring compliance with regulations in Brazil and Latin America.

Pinheiro Neto Advogados

Rua Hungria, 1100, Jardim Europa
São Paulo, SP
Brazil

Tel: +55 11 3247 8553

Email: ccoutinho@pn.com.br

LinkedIn: www.linkedin.com/in/cec%C3%ADlia-coutinho-781a2a15a

Pinheiro Neto Advogados has rendered counsel in virtually all areas of legal practice since 1942 and is structured to offer its clients comprehensive assistance with all legal aspects of their business activities. It currently has over 840 members, including more than 100 partners, approximately 380 associates, in addition to a team of paralegals and professionals in other support areas. Pinheiro Neto Advogados provides services to approximately 2,000 local and international groups and has full-service offices in São Paulo, Rio de Janeiro and Brasília, as well as representative offices in Palo Alto and Tokyo.

www.pinheironeto.com

PINHEIRONETO
ADVOCADOS

The **International Comparative Legal Guides**

(ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 58 practice areas.

Data Protection 2025 features four expert analysis chapters and 27 Q&A jurisdiction chapters covering key issues, including:

- Relevant Legislation and Competent Authorities
- Territorial and Material Scope
- Key Principles
- Individual Rights
- Children's Personal Data
- Registration Formalities and Prior Approval
- Appointment of a Data Protection Officer
- Appointment of Processors
- Marketing
- Cookies
- Restrictions on International Data Transfers
- Whistle-blower Hotlines
- CCTV
- Employee Monitoring
- Data Security and Data Breach
- Enforcement and Sanctions
- E-discovery/Disclosure to Foreign Law Enforcement Agencies
- Artificial Intelligence