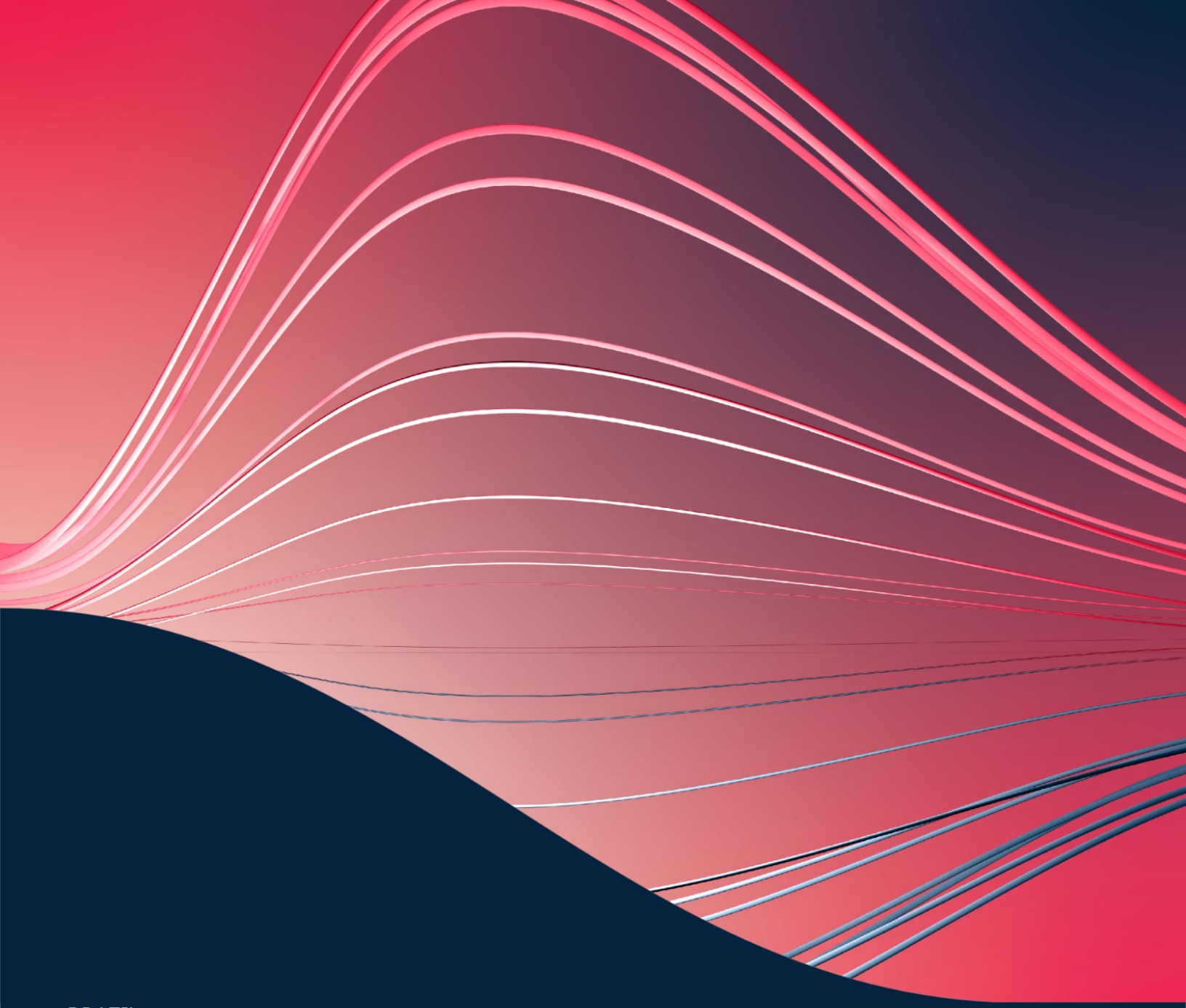


BRAZIL

Data Protection Laws of the World

DLA PIPER

Introduction

Welcome to the 2025 edition of DLA Piper's Data Protection Laws of the World Handbook. Since the launch of our first edition in 2012, this comprehensive guide has been a trusted resource for navigating the complex landscape of privacy and data protection laws worldwide. Now in its fourteenth edition, the Handbook has grown to provide an extensive overview of key privacy and data protection regulations across more than 160 jurisdictions. As we step into 2025, the global landscape of data protection and privacy law continues to evolve at an unprecedented pace. With new legislation emerging in jurisdictions around the world, businesses face a growing need to stay informed and agile in adapting to these changes. This year promises to bring new developments and challenges, making the Handbook an invaluable tool for staying ahead in this ever-changing field.

Europe

Established data protection laws in Europe continue to evolve through active regulatory guidance and enforcement action. In the United Kingdom, the UK government has proposed reforms to data protection and e-privacy laws through the new Data (Use and Access) Bill ("**DUAB**"). The DUAB follows the previous government's unsuccessful attempts to reform these laws post-Brexit, which led to the abandonment of the Data Protection and Digital Information (No.2) Bill ("**DPDI Bill**"), in the run-up to the general election. Although the DUAB comes with some bold statements from the government that it will *"unlock the power of data to grow the economy and improve people's lives"*, the proposals represent incremental reform, rather than radical change.

United States

In the United States, legislation on the federal and in particular state level continues to evolve at a rapid pace. Currently, the US has fourteen states with comprehensive data privacy laws in effect and six state laws will take effect in 2025 and early 2026. Additionally, at the federal level, the new administration has signaled a shift in enforcement priorities concerning data privacy. Notably, there is a renewed focus on the regulation of artificial intelligence (AI), with an emphasis on steering away from regulation and promoting innovation. This includes the revocation of previous executive orders related to AI and the implementation of new directives to guide AI development and use.

In the realm of children's privacy, many of the new administration's supporters in Congress have indicated a desire to make the protection of children on social media a top priority, and new leadership at the Federal Trade Commission (FTC) appears aligned on this goal, albeit with a willingness to take another look at the recently adopted amendments to the Children's Online Privacy Protection Act (COPPA) Rule. Health data

privacy remains a critical concern, with a handful of states following Washington state's lead in enhancing or adopting health data privacy laws. On the international data transfer front, Executive Order (E.O.) 14117 " Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" as supplemented by the DOJ's final Rule will impact companies transferring data into certain jurisdictions, such as China, Iran and Russia. Another area of focus for companies with an EU presence will be the Trump administration's approach to the Privacy and Civil Liberties Oversight Board, as it is a critical pillar of the EU/UK/Swiss-US Data Privacy Framework.

Asia, the Middle East, and Africa

Nowhere is the data protection landscape changing faster – and more fundamentally – than in Asia, with new laws in India, Indonesia, Australia and Saudi Arabia, as well continued new data laws and regulations in China and Vietnam. The ever-evolving data laws, as well as the trend towards regulating broader data categories (beyond personal data), in these regions continue to raise compliance challenges for multi-national businesses.

Emerging trends in data governance

Unlocking data, regulating the relentless advance of AI, creating fairer digital markets and safeguarding critical infrastructure against the ever growing cyber threat, continue to impact and overlap with the world of data protection and privacy. Perhaps most notably, the EU have introduced a raft of new laws forming part of its ambitious digital decade, which will bring huge change to businesses operating within the EU. With the rapid adoption of artificial intelligence enabled solutions and functionality, data protection supervisory authorities have been closely scrutinising the operation of AI technologies and their alignment with privacy and data protection laws. For businesses, this highlights the need to integrate date protection compliance into the core design and functionality of their AI systems. In the midst of this, the privacy community found itself at the centre of an emerging debate about the concept of 'AI governance'. This is not a surprising development – AI systems are creatures of data and the principle-based framework for the lawful use of personal data that sits at the heart of data protection law offers a strong starting point for considering how to approach the safe and ethical use of AI. As AI technologies advance, so will regulatory expectations. It is expected that regulatory scrutiny and activity will continue to escalate and accelerate in tandem with the increase in integration of powerful AI models into existing services to enrich data. Whilst privacy professionals cannot tackle the AI challenge alone, expect them to continue to be on the front lines throughout 2025 and beyond.

Disclaimer

This handbook is not a substitute for legal advice. Nor does it cover all aspects of the legal regimes surveyed, such as specific sectorial requirements. Enforcement climates and legal requirements in this area continue to evolve. Most fundamentally, knowing high-level principles of law is just one of the components required to shape and to implement a successful global data protection compliance program.

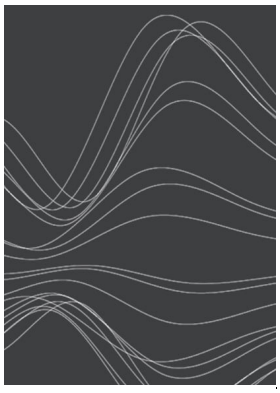
Africa key contact

Monique Jefferson
Director
monique.jefferson@dlapiper.com
Full bio

Americas key contact

Andrew Serwin
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
andrew.serwin@us.dlapiper.com
Full bio

Asia Pacific key contact



Carolyn Bigg
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
carolyn.bigg@dlapiper.com
Full bio

Europe key contacts

Andrew Dyson
Partner
andrew.dyson@dlapiper.com
Full bio

Ewa Kurowska-Tober
Partner
Head of Intellectual Property and Technology, Poland
ewa.kurowska-tober@dlapiper.com
Full bio

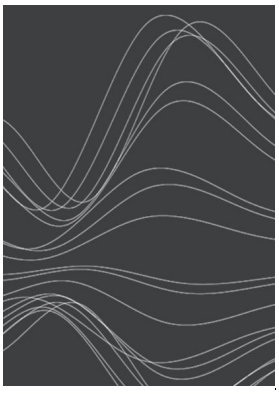
John Magee
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
john.magee@dlapiper.com
Full bio

Middle East key contact

Rami Zayat
Partner
rami.zayat@dlapiper.com
Full bio

Editors

Kate Lucente
Partner
kate.lucente@us.dlapiper.com
Full bio



Lea Lurquin
Associate
lea.lurquin@us.dlapiper.com
Full bio

Brazil

LAST MODIFIED 28 JANUARY 2024

Data protection laws

In force since September 18, 2020, the Brazilian General Data Protection Law (LGPD) is Brazil's first comprehensive data protection regulation, and it broadly aligns with the EU General Data Protection Act (GDPR).

The LGPD applies to any processing operation carried out by a natural person or a legal entity (of public or private law), irrespective of (1) the means used for the processing, (2) the country in which its headquarter is located, or (3) the country where the data are located, provided that:

- The processing operation is carried out in Brazil;
- The purpose of the processing activity is to offer or provide goods or services, or the processing of data of individuals located in Brazil; or
- The personal data was collected in Brazil.

On the other hand, the law does not apply to the processing of personal data that is:

- Carried out by a natural person exclusively for private and non-economic purposes;
- Performed for journalistic, artistic, or academic purposes;
- Carried out for purposes of public safety, national security, and defense or activities of investigation and prosecution of criminal offenses (which will be the subject of a specific law);
- Originated outside the Brazilian territory and are not the object of communication; or
- Shared data use with Brazilian processing agents or the object of international transfer of data with another country that is not the country of origin, provided that the country of origin offers a level of personal data protection adequate to that established in the Brazilian law.

In addition, on October 20, 2021, the Brazilian Senate unanimously approved the Proposed Amendment to the Constitution ("PEC") no. 17/2019, which includes in the

Federal Constitution the protection of personal data, including in digital media, as a fundamental right, and to refer privately to the Union (federal government) the responsibility to legislate on this subject. As of February 10, 2022, data protection is now encompassed by the Federal Constitution as a fundamental right.

Definitions

Definition of personal data

The LGPD defines personal data as any information related to an identified or identifiable natural person.

Anonymized data is not considered personal data, except when the process of anonymization has been reversed or if it can be reversed applying reasonable efforts.

Definition of sensitive personal data

The LGPD defines sensitive personal data as any personal data concerning:

- Racial or ethnic origin
- Religious belief
- Political opinion
- Trade union
- Religious, philosophical or political organization membership
- Health or sex life
- Genetic or biometric data

National data protection authority

The LGPD established the National Data Protection Authority (ANPD). On October 25, 2022, Law 14,460/2022 was published, altering ANPD's role into a special and independent autarchic regime with administrative and budgetary autonomy as opposed to linking the ANPD to the Presidency of the Republic. The ANPD is also given technical and decision-making autonomy with jurisdiction over the Brazilian territory. In addition, the ANPD will have its own appointed public attorneys, which enables the National Authority to independently take judicial measures that it deems appropriate.

The ANPD is now in operation and it is headquartered in the Federal District. Its structuring process started on August 27, 2020, with the publication of Decree No. 10,474/2020, which approved and regulated the regulatory structure of the ANPD, and its board of commissioned positions and nominated trust functions. On November 6, 2020, this Decree entered into force with the appointment of the Director-President and the members of the Board of Directors of the ANPD, after having been approved by the plenary of the Federal Senate. On March 9, 2021, the ANPD's Internal Regulations were published, establishing the competencies and organization of the National Authority.

The ANPD is composed of:

- A Board of Directors
- A national council for Personal Data and Privacy Protection (Council)
- Bodies of direct and immediate assistance to the Board of Directors (General Secretariat, General Coordination of Administration, General Coordination of Institutional and International Relations)
- An Internal Affairs Office (inspection body)
- An ombudsman
- The Prosecution
- Its own legal advisory body, and
- Administrative and specialized units for the enforcement of the LGPD (*ie*, General Coordination of Standardization; General Coordination of Supervision; and General Coordination of Technology and Research)

The ANPD has the authority to issue sanctions for violations of the LGPD. This sanctions authority came into force on August 1, 2021. On October 29, 2021, the ANPD issued Regulation CD/ANPD 01/2021 for the Regulation of the Inspection Process and the Sanctioning Administrative Process, establishing the procedures regarding the supervision and enforcement of the LGPD. However, the Regulation is still pending further instructions relating to the parameters of calculation of such penalties, which are expected to be regulated by the end of 2023.

In August 2021, the President of the Republic appointed representatives of the National Council for Personal Data and Privacy Protection (Council). The Council contributes to the performance of the ANPD and has the authority to, among other things:

- Oversee the protection of personal data
- Issue regulations and procedures related to personal data protection
- Deliberate, at an administrative level, upon the interpretation of the LGPD and matters omitted in its redaction
- Supervise and apply sanctions in the event of data processing performed in violation of the legislation
- Implement simplified mechanisms for recording complaints about the processing of personal data in violation of the LGPD

In addition, the ANPD Council is responsible for, among other functions:

- Proposing strategic guidelines and allowance for the creation of the National Policy for the Protection of Personal Data and the operation of ANPD
- Suggesting actions to be carried out by the ANPD
- Preparing studies and conducting public debates and hearings about the protection of personal data

Since the ANPD started its operations, several actions have already been implemented to protect personal data, including:

- Determining the procedures regarding the inspection and application of administrative sanctions
- Providing specific regulation regarding small-sized data processing agents
- Publishing guidelines regarding cookie policy and banner
- Opening public consultation regarding international transfers
- Publishing guidance on reporting a security incident with personal data and its assessment to the ANPD
- Explaining availability of a claim by the data subject against controller
- Providing educational materials on data protection, such as (1) guidelines for defining personal data processing agents and the DPO, (2) how consumers should protect their personal data, and (3) information security for small processing agents.

However, there are still several provisions of the LGPD requiring further regulation and interpretation by the ANPD, which stakeholders should monitor for future compliance.

Registration

There is currently no requirement to register with the National Data Protection Authority under Brazilian law.

Data protection officers

The LGPD creates the position of Chief of Data Processing, which is the data protection officer (DPO) in charge of data processing operations. The DPO is responsible for the following:

- Accepting complaints and communications from data subjects and the National Authority
- Providing guidance to employees about good practices and carrying out other duties as determined by the controller or set forth in complementary rules

On July 16, 2024, the National Data Protection Authority (ANPD) published Regulation CD/ANPD 18/2024, which provides that data processors are not required to appoint a DPO, but it shall be considered as good practice by the ANPD. The appointment of a DPO is also not required for small businesses, startups, and innovative companies, as defined by the law, except for those performing data processing activities which incur in high risks for data subjects[1] , pursuant to ANPD Regulation CD/ANPD 02/2022.

Regulation no. 18/2024 also provides that the appointment of the DPO must be made through a formal act, *ie*, a written document, dated and executed, which clearly and unequivocally demonstrates the data processing agent's intention to appoint a natural person or a legal organization as DPO, including the DPO's roles and activities.

According to the mentioned Regulation, the DPO may be (i) a natural person, either internal or external to the data processing agent (controller or processor), or (ii) a legal organization. The DPO is required to be able to communicate with data subjects and with the ANPD in a clear and precise manner and in Portuguese.

In addition, the DPO's identity and contact information shall be publicly available, in a clear and objective manner, in highlighted and easily accessible place on the organization's website. If the DPO is a natural person, their full name must be disclosed, and if the DPO is a legal organization, it must be disclosed the company's name and fantasy name, as well as the full name of the natural person responsible for the company.

Even though the DPO may carry out more than one activity within an organization, the DPO may not be responsible for functions within the same organization that could result in a conflict of interest, such as carrying out activities that involve making strategic decisions related to the processing of personal data by the controller, which does not include making decisions related to the processing of personal data which is inherent to the exercise of the DPO's duties.

Due to the absence of legal or regulatory requirements, there is no need to communicate or record the identity and contact information of the DPO with the ANPD.

[1] The following entities are considered Small-Sized Processing Agents:

- micro-enterprises and small size businesses, as defined by Art. 41, Law No 14,195 /2021
- entrepreneur, as defined by the Civil Code No 10,406/2002
- start-ups, as defined by Law No 182/2021
- non-profits organizations
- natural persons and depersonalized private entities who carry out treatment of personal data, assuming typical controller or operator obligations.

Small-Sized Processing Agents must not earn gross revenue higher than BRL 4.800.000,00, or, in the case of start-ups BRL 16.000.000,00, nor belong to an economic group whose global revenue exceeds the limits, as defined by the corresponding laws or perform high-risk processing. According to the Regulation, a high-risk data processing activity meets at least one general and one specific criteria among those listed in the Regulation. General criteria are: (i) processing of personal data in large scale; and (ii) processing of personal data which may significantly affect the data subjects' interests and fundamental rights, while specific criteria is (i) use of emerging or innovative technologies; (ii) vigilance or control of public accessible areas; (iii) decisions made exclusively with basis on automated data processing; and (iv) use of sensitive data or personal data belonging to children, adolescents and elderly people.

Collection and processing

Under the LGPD, collecting and processing are referred to as "data treatment", and defined as all operations carried out with personal data, such as:

- Collection
- Production
- Reception
- Classification
- Utilization
- Access
- Reproduction
- Transmission
- Distribution
- Processing
- Filing
- Storage
- Elimination
- Evaluation
- Control
- Modification
- Communication
- Transfer
- Diffusion, or
- Extraction

The processing of personal data may only be carried out based on one of the following legal bases:

- With data subject consent
- To comply with a legal or regulatory obligation by the controller
- By the public administration, for the processing and shared use of data which are necessary for the execution of public policies provided in laws or regulations or contracts, agreements or similar instruments
- For carrying out studies by research entities, ensuring, whenever possible, the anonymization of personal data
- For the execution of a contract or preliminary procedures related to a contract to which the data subject is a party
- For the regular exercise of rights in judicial, administrative or arbitration procedures

- As necessary for the protection of life or physical safety of the data subject or a third party
- For the protection of health, exclusively, in a procedure carried out by health professionals, health services or sanitary authorities
- To fulfill the legitimate interests of the controller or a third party, except in the case of prevailing the fundamental rights and freedoms of the data subject, and
- For the protection of credit

Notwithstanding the above, personal data processing must be carried out in good faith and based on the following principles:

- Purpose
- Suitability
- Necessity
- Free access
- Quality of the data
- Transparency
- Security
- Prevention
- Nondiscrimination, and
- Accountability

As for the processing of sensitive personal data, the processing can only occur when the data subject or their legal representative consents specifically and in highlight, for specific purposes; or, without consent, under the following situations:

- As necessary for the controller's compliance with a legal or regulatory obligation
- Shared data processed as necessary for the execution of public policies provided in laws or regulations by the public administration
- For carrying out studies by research entities, ensuring, whenever possible, the anonymization of personal data
- For the regular exercise of rights, including in a contract or in a judicial, administrative or arbitration procedure
- Where necessary for the protection of life or physical safety of the data subject or a third party
- The protection of health, exclusively, in a procedure performed by health professionals, health services or sanitary authorities, or
- To prevent fraud and protect the safety of the data subject

The controller and operator must keep records of the data processing operations they carry out, mainly when the processing is based on a legitimate interest.

In this sense, the ANPD may determine that the controller must prepare an Impact Report on Protection of Personal Data, including sensitive data, referring to its data processing operations, pursuant to regulations, subject to commercial and industrial secrecy. The report must contain at least a description of the types of data collected, the methodology used for collection and for ensuring the security of the information, and the analysis of the controller regarding the adopted measures, safeguards and mechanisms of risk mitigation.

On January 28, 2022, the ANPD published Regulation CD/ANPD 02/2022, which provides special rules on the application of the LGPD to small businesses, startups, and innovative companies, as defined by the law, except to those performing data processing activities which incur in high risks for data subjects.[1] This Regulation includes certain exemptions and flexibilities, reducing obligations under the law. For example a simplified template of records of data processing activities, which will be made available by the ANPD.

Footnotes

FN 1:

The following entities are considered Small-Sized Processing Agents:

- micro-enterprises and small size businesses, as defined by Art. 41, Law No 14,195/2021
- entrepreneur, as defined by the Civil Code No 10,406/2002
- start-ups, as defined by Law No 182/2021
- non-profits organizations
- natural persons and depersonalized private entities who carry out treatment of personal data, assuming typical controller or operator obligations.

Small-Sized Processing Agents must not earn gross revenue higher than BRL 4.800.000,00, or, in the case of start-ups BRL 16.000.000,00, nor belong to an economic group whose global revenue exceeds the limits, as defined by the corresponding laws or perform high-risk processing. According to the Regulation, a high-risk data processing activity meets at least one general and one specific criteria among those listed in the Regulation. A general criteria is (i) processing of personal data in large scale; and (ii) processing of personal data which may significantly affect the data subjects' interests and fundamental rights, while specific criteria is (i) use of emerging or innovative technologies; (ii) vigilance or control of public accessible areas; (iii) decisions made exclusively with basis on automated data processing; and (iv) use of sensitive data or personal data belonging to children, adolescents and elderly people.

Transfer

The transfer of personal data to other jurisdictions is allowed only subject to compliance with the requirements of the LGPD. Prior specific and informed consent is needed for such transfer, unless:

- The transfer is to countries or international organizations with an adequate level of protection of personal data
- There are adequate guarantees of compliance with the principles and rights of data subject provided by LGPD, in the form of
  - Specific contractual clauses for a given transfer
  - Standard contractual clauses
  - Global corporate norms, or
  - Regularly issued stamps, certificates and codes of conduct
- The transfer is necessary for international legal cooperation between public intelligence, investigative and prosecutorial agencies
- The transfer is necessary to protect the life or physical safety of the data subject or a third party
- The ANPD has provided authorization
- The transfer is subject to a commitment undertaken through international cooperation
- The transfer is necessary for the execution of a public policy or legal attribution of public service
- The transfer is necessary for compliance with a legal or regulatory obligation, execution of a contract or preliminary procedures related to a contract, or the regular exercise of rights in judicial, administrative or arbitration procedures

On August 23, 2024, ANPD published Regulation CD/ANPD 19/2024, which provides for the rules for international transfer of personal data, including the ANPD approved form of standard contractual clauses, and the proceeding for approval of specific contractual clauses and binding corporate rules. Said regulation also provides for the criteria that shall be observed by the ANPD for issuing adequacy decisions and for recognizing the equivalence of standard contractual clauses issued by other jurisdictions with the ANPD clauses.

If standard contractual clauses are the elected transfer mechanism within an organization, it is important to note that ANPD clauses must be implemented by August 2025.

On May 05, 2022, ANPD opened a public consultation regarding international transfers regulation. However, such regulation is pending but expected to be published sometime in 2023.

Security

Controllers and processors must adopt technical and administrative security measures designed to protect personal data from:

- Unauthorized accesses, and
- Accidental or unlawful situations of:
  - Destruction
  - Loss
  - Alteration
  - Communication, or
  - Any improper or unlawful processing

The LGPD grants the ANPD authority to establish minimum technical standards for companies to implement.

On 4 October 2021, the ANPD launched information security guidelines aimed at small data processing agents (such as microenterprises, small businesses, and startups) to assist them with good practices in implementing technical and administrative information security measures for the protection of personal data. The guidelines also contain a checklist to facilitate the visualization of suggestions, such as awareness and training programs, agreements management, access controls, data storage guidelines, and vulnerability management.

On December 09, 2024, the ANPD published its Regulatory Agenda for 2025/2026 and made the regulation of technical and administrative security measures a priority for the period, determining the start of the regulation procedures within 2025.

The Brazilian Internet Act further establishes that service providers, networks and applications providers should keep access records (such as IP addresses and logins) confidential and in a secured and controlled environment. Guidelines issued under the Internet Act established guidelines on appropriate security controls, including:

- Strict control on data access by defining the liability of persons who will have the possibility of access and exclusive access privileges to certain users
- Prospective of authentication mechanisms for records access, using, for example, dual authentication systems to ensure individualization of the controller records
- Creation of detailed inventory of access to connection records and access to applications containing the time, duration, the identity of the employee or the responsible person for the access designated by the company and the accessed file
- Use of records management techniques that ensure the inviolability of data, such as encryption or equivalent protective measures

Breach notification

According to the LGPD, any unauthorized accesses and from accidental or unlawful situations of destruction, loss, alteration, communication or diffusion is considered a breach.

The controller is responsible for reporting to ANPD and the data subject within three (3) working days after becoming aware of the breach if it is likely to result in risk or harm to data subjects.

On April 24, 2024, the ANPD published Regulation CD/ANPD 15/2024, which provides for the rules for communication of data breaches. According to such regulation, a breach is considered to pose relevant risks or damages to data subjects if it significantly affects their interests and fundamental rights and involves at least one of the following criteria:

- Sensitive personal data
- Data relating to children, adolescents, or the elderly
- Financial data
- Data used for system authentication (e.g., login credentials, tokens, or passwords)
- Data protected by legal, judicial, or professional confidentiality obligations, or
- Large-scale data.

If a notification is required, it must be submitted by the controller's DPO or the legal representative with the corresponding nomination documentation or power of attorney, through a breach reporting form provided by the ANPD.

The notice to the ANPD must contain, at least, the following key information:

- Description of the nature of the affected personal data
- Information regarding the data subjects involved, including the amount of data subjects, detailing, when applicable, the amount of children, adolescents or elderly involved
- Indication of the security measures used to protect the personal data before and after the incident
- The risks generated by the incident with identification of possible impacts for data subjects
- The reasons for a delay in communication (if any)
- The measures that were or will be adopted to reverse or mitigate the effects of the incident
- The date in which the incident occurred, if possible to identify, and the date in which the controller became aware of the data incident
- Information on the data protection officer or of the controller's legal representative
- The controller's identification
- The processor's identification, if applicable
- A description of the incident, including the main cause, if possible to identify
- The total amount of data subjects involved in the data processing activities affected by the incident

- Information regarding the communication to the affected data subjects

As to the notification to affected data subjects, the following information is required:

- A description of the nature and categories of personal data affected
- The technical and security measures taken to protect the personal data
- Risks related to the data incident and identification of the possible impacts on data subjects
- The reasons for the delay (if any)
- The measures that have been or will be taken to reverse or mitigate the effects of the data incident, when applicable
- The date in which the controller became aware of the data incident
- Contact for obtaining information and, if applicable, contact data of the of the controller's data protection officer

It is important to highlight that notification to the affected data subjects must be made (i) in simple and easy-to-understand language, and (ii) individually, directly to the data subjects, also within three (3) working days counted from the date when the controller became aware of the security incident. The notification may be carried out by any means such as e-mail, SMS, letter, or electronic message and, preferably, through the channel normally used by the controller to communicate with the data subject. If the controller is unable to identify each individual data subject affected by the incident, it shall notify the occurrence of the data incident through the available means of dissemination, such as its website, applications, social media and customer service channels, so that the communication allows broad knowledge, with direct and easy visualization, for a period of at least three (3) months.

Controller is required to submit to the ANPD a declaration stating that data subjects were duly informed of the breach, containing the communication or broadcast means used, within three (3) working days after filing the notification before the ANPD. If direct and individualized communication to data subjects is not feasible, controller shall notify the data subjects through broadcast means available, such as its website, apps, social media and customer service, to ensure that the notification allows broad knowledge with direct and easy visualization for at least three (3) months.

Additionally, the ANPD must verify the seriousness of the incident and may, if necessary to safeguard the data subject's rights, order the controller to adopt measures, such as the broad disclosure of the event in communications media, as well as measures to reverse or mitigate the effects of the incident.

The failure to report a data breach that could cause significant risk or damage to data subjects may subject agents to the administrative sanctions provided under the LGPD. In case the Controller is unable to provide a complete breach notification within the three (3) working days period, the Controller must submit a preliminary notice with the corresponding justification. The preliminary notice must be supplemented as soon as possible and, at the latest, within twenty (20) working days.

It is also important to note that all security incidents must be recorded and kept on file for five (5) years as part of a Security Incident Record, which must include, at a minimum:

- The date the controller became aware of the incident
- A general description of the circumstances surrounding the incident
- The nature and categories of the affected personal data
- The number of affected data subjects
- A risk assessment and potential damages to data subjects
- Measures taken to mitigate the incident (if applicable)
- Details of any notifications made to the ANPD or data subjects
- The reasons for not notifying the incident (if applicable)

An additional recommendation, which is not legally required, is to implement contractual clauses establishing the obligations regarding notification of breaches between controllers and processors, seeking to expedite the assessment and minimize the risks to the data subjects.

On January 28, 2022, the ANPD published Regulation CD/ANPD 02/2022 which grants to small businesses, startups, and innovative companies, as defined by the law, except to those performing data processing activities which incur in high risks for data subjects the double deadline extension in the communication of security incidents, as well responding to data subjects' requests, for communicating severe security incidents to the ANPD and affected data subjects, and for responding to ANPD's requests.

Enforcement

The LGPD provides for penalties in case of violations its provisions. Data processing agents that commit infractions can be subject to administrative sanctions, in a gradual, single or cumulative manner, including a fine, simple or daily, of up to 2% of the revenues of a private legal entity, group or conglomerate in Brazil, up to a total maximum of R$50 million per infraction.

Other sanctions can include:

- Warning
- Publicizing of the violation
- Blocking the personal data to which the infraction refers to until its regularization
- Deletion of the personal data to which the infraction refers
- Partial suspension of the database operation to which the infringement refers for a maximum period of six (6) months, extendable for the same period, until the processing activity is corrected by the controller;

- Suspension of the personal data processing activity to which the infringement refers for a maximum period of six (6) months, extendable for the same period;
- Partial or total prohibition of activities related to data processing.

Although the LGPD became effective September 18, 2020, the penalties provided by the law were only enforceable from August 1, 2021. On October 29, 2021, the ANPD published the Regulation of the Inspection Process and the Sanctioning Administrative Process, which establishes the procedures applicable to ANPD's inspection process and the rules to be observed during the administrative sanctioning process. On February 24, 2023, the ANPD published the Regulation of Dosimetry and Application of Administrative Sanctions, which provides for the parameters of calculation of the above penalties. Until the present moment, the ANPD has only imposed one administrative sanction regarding violations to the LGPD by a private entity. Therefore, the level of enforcement activity is still uncertain.

Public authorities (such as consumer protection bodies and public prosecutors) are also entitled to monitoring data protection matters and to applying penalties based on the LGPD obligations and other applicable laws. Additionally, data subjects may file lawsuits if any of the rights provided by the LGPD are violated. Under the law, a controller or processor that causes material, moral, individual, or collective damage to others is liable to individuals for such damages, including through a class action.

Exceptions to the obligation to remedy a violation exist only if:

- The agent (*ie*, controller or the processor) did not carry out the data processing
- There was no violation of the data protection legislation in the processing, or
- The damage arises due to exclusive fault of the data subject or a third party

Electronic marketing

Brazil has no specific law regulating electronic marketing communications. However, it is important to point out that, according to the LGPD, all processing of consumers' personal data (which includes the collection, storage, and sending of marketing communications) can only occur upon the appropriate legal basis for such purpose. Under this scenario, two available legal bases could be used, depending on the analysis of the concrete case:

- the data subject's consent, or
- the controller's legitimate interest.

Despite the lack of a specific statute, general provisions on privacy and intimacy rights, as well as consumer protection rights, also apply to electronic marketing. Therefore, the sender should immediately cease sending any electronic marketing if the consumer requests (i.e., offering an opt-out option to electronic marketing).

Online privacy

The Brazilian Internet Act has several provisions concerning the storage, use, disclosure, and other processing of data collected on the Internet. The established

rights of privacy, intimacy, and consumer rights apply equally to electronic media, such as mobile devices and the Internet. Violations of these rights may also be subject to civil enforcement.

Furthermore, as explained in prior sections, identifiable data are also encompassed under the scope of protection of the LGPD. Thus, if cookies and location data are associated with a natural person, their collection should also observe the same obligations provided by the Brazilian data protection law. However, the obligation does not apply to anonymized data, which is not considered personal data under the LGPD unless the process of anonymization has been reversed or can be reversed using reasonable efforts.

That said, a proper legal basis is needed when using cookies and similar technologies that involve the processing of a user's personal data from (e.g., the information is linked or linkable to a particular user, IP address, a device, or other particular identifier). Under this scenario, two available legal bases could be used, depending on the analysis of the concrete case: the data subject's consent or the controller's legitimate interest (in the case of essential cookies, for example).

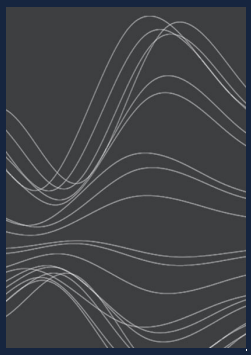
On October, 2022, the ANPD published Cookie Guidelines establishing recommendations for cookie policy disclosures, such as to inform the categories of relevant cookies, their purposes, retention periods and whether the data collected through cookies is shared. Such disclosures must be provided to the data subject in a simplified and understandable format and manner. Further, the guidelines require collection of affirmative opt-in consent, for example through cookie banners, and provide the data subject with the possibility to reject the cookies at that time and revoke consent at any time later on.

Data protection lawyers

Paula Mena Barreto
Partner
Campos Mello Advogados
paula.menabarreto
@cmalaw.com
View bio

For more information

To learn more about DLA Piper, visit dlapiper.com or contact:



Carolyn Bigg
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
carolyn.bigg@dlapiper.com
Full bio

John Magee
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
john.magee@dlapiper.com
Full bio

Andrew Serwin
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
andrew.serwin@us.dlapiper.com
Full bio

About us

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa and Asia Pacific, positioning us to help companies with their legal needs around the world.

dlapiper.com