JONES DAY | One Firm Worldwide®

WHITE PAPER

September 2024

Brazil Amps Up Enforcement of Data Protection Law

Actions in the last six months of the Brazilian National Data Protection Authority ("ANPD") suggest that it intends to aggressively enforce the Brazilian Data Protection Law ("LGPD"). The LGPD applies to any entity that processes personal data of individuals in Brazil regardless of whether the entity has operations in the country. Such entities must, therefore, actively implement data privacy compliance policies.

Notable recent actions taken by the ANPD include: (i) promulgation of a regulation on the appointment of a data protection officer ("DPO") by data controllers, detailing a DPO's roles and responsibilities under the LGPD; (ii) enjoining the use by Meta Platforms Inc. of personal data from social media platforms for training artificial intelligence systems; (iii) promulgation of a regulation requiring disclosure of security incidents to affected individuals and the ANPD and a related order requiring public disclosure of data breaches by the National Social Security Institute; and (iv) promulgation of a regulation on international transfer of personal data, under the LGPD, and standard contractual clauses that can be implemented in connection with such transfers.

Companies and individuals doing business in Brazil have a new area of concern. As the LGPD (*Lei Geral de Proteção de Dados Pessoais*) and its enforcement agency, the ANPD (*Autoridade Nacional de Proteção de Dados*), mark their fourth anniversary of effectiveness, actions by the ANPD—requiring a data controller to appoint a DPO, prohibiting the use of social media posts for purposes of training artificial intelligence programs, ordering public disclosure of data breaches, and promulgating new rules on international transfer of data—make it clear that the ANPD intends to aggressively enforce Brazilian data privacy laws.

LGPD

Enacted on August 14, 2018, Law No. 13,709, the LGPD became effective on September 18, 2020. It was inspired by the European Union's General Data Protection Regulation ("GDPR") and aims to protect the fundamental rights of freedom and privacy of personal data for individuals.

The LGPD establishes detailed rules for the collection, use, processing, and storage of personal data and applies to any business or organization that processes the personal data of individuals in Brazil, regardless of where the entity is located.

The LGPD outlines the rights of data subjects, including their right to access, correct, and delete their data, as well as the right to be informed about the use of their data. It also imposes strict requirements on data processors and controllers regarding the handling of personal data, including the need for explicit consent for certain data processing activities, the implementation of security measures to protect data, and the notification of data breaches.

ANPD

The enforcement of the LGPD is carried out by the ANPD, which is an independent public authority linked to the Brazilian Ministry of Justice and Public Security. Although the ANPD was sanctioned by the LGPD, the structure and organization of the ANPD were detailed in Decree No. 10,474/20, which was signed on August 26, 2020. Its first five directors were appointed and approved in the latter half of October 2020. The responsibilities of the ANPD include:

- Monitoring and applying sanctions in cases of noncompliance with the LGPD;
- Issuing guidelines for the LGPD's implementation;
- Reviewing and approving data protection impact assessments; and
- Encouraging the adoption of standards for services and products that facilitate the protection of personal data.

The ANPD has the authority to impose penalties for noncompliance, which can include fines of up to 2% of a company's revenue in Brazil, limited to 50 million reais (approximately US$10 million) per violation.

In the last six months, the ANPD has made it clear that it will vigorously enforce the mandates of the LGPD.

DATA PROTECTION OFFICER REGULATION

On July 16, 2024, the ANPD enacted Resolution CD/ANPD No. 18, which detailed the role of the DPO contemplated by the LGPD. Some of its main provisions include the following.

Appointment by Formal Act

Every controller must appoint either an individual or a legal entity to act as a DPO through a written, dated, and signed document, which must be presented to the ANPD upon request.

Identity and Publicity

The controller's website must identify the DPO and its contact information in order to allow persons whose data is under the control of the Controller as well as the authorities to communicate with the DPO.

Deputy DPO

A deputy DPO must be formally appointed in case the DPO is absent or unable to perform or resigns or is terminated from its role.

DPOs for Processors

Processors are not required to appoint a DPO, but they are encouraged to do so as a best practice.

Qualifications

The controller must select the DPO, taking into account the entity's or person's knowledge about data protection legislation,

as well as the context, volume, and risk of the processing activities performed. No specific certification or registration with any specific body is required for the DPO.

Facilitation of Activities

The processing agent must: (i) provide the DPO with the necessary means to perform his/her duties; (ii) seek assistance and guidance from the DPO when carrying out activities and making strategic decisions related to data processing; (iii) ensure the DPO has the technical autonomy needed to fulfill its activities; (iv) ensure data subjects have swift, effective, and appropriate means to communicate with the DPO and exercise their rights; and (v) provide the DPO with direct access to the highest executives and decision-makers within the organization.

Communication

The DPO must be able to communicate clearly in the Portuguese language.

DPO Functions

DPO responsibilities include: (i) accepting complaints and communications from data subjects, providing clarifications, and taking appropriate actions; (ii) receiving, responding to, and implementing communications from the ANPD; (iii) instructing employees and contractors of the processing agent on good data protection practices; (iv) performing other duties defined by the processing agent or supplementary regulations; (v) assisting and guiding the processing agent in the development, definition, and implementation, as appropriate, of:

- Communication of incidents;
- Record of processing activities;
- Data protection impact assessments, when necessary;
- Risk mitigation measures considering potential processing risks;
- Necessary security measures for data protection;
- Internal policies, regulations, and guidelines compliant with the LGPD and ANPD;
- Drafting and implementing contractual clauses related to data protection;
- International data transfers;
- Governance rules and best practices on data processing;
- Products and services that adopt privacy by design and by default; and
- Other strategic decisions related to data processing.

Legal Responsibility

The DPO does not have personal liability for the compliance of data processing activities carried out by the data controller.

Cumulative Roles

The DPO may hold multiple roles and perform duties for more than one processing agent, provided it can fulfill its responsibilities owed to each processing agent and no conflict of interest exists.

Conflict of Interest

If a conflict of interest should arise, the DPO and the processing agent must, respectively, declare and take care to avoid such situations, whether they involve conflicting internal duties or duties at different processing agents, as well as the accumulation of DPO activities with other activities involving strategic decision-making on data processing. The existence of a conflict of interest must be verified on a case-by-case basis and might subject the controller to penalties. If a conflict of interest is identified, the controller must: (i) take measures to eliminate the risk of conflict of interest; or (ii) replace the designated person or entity.

The above requirement extends to foreign companies processing data in Brazil regardless of their actual presence in Brazil. Given the newness of the regulation, it is unclear whether, on its basis, companies will appoint internal employees as DPOs or will choose to appoint third-party consultants. Boutique law firms and consultants are actively offering the service, but for now it looks like companies are using internal employees, especially since the role requires an understanding and appreciation of internal operations and how data is stored and used.

ENJOINING AI DATA USE BY META

On July 1, 2024, the ANPD handed down a preventive measure suspending the implementation of a new privacy policy by Meta Platforms Inc.–Facebook Online Services of Brazil.

The policy related to the use of personal data processed within Meta's platforms, such as Facebook, Messenger, and Instagram, for training generative artificial intelligence systems. The penalty to be imposed for any breach of the preventive measure was 50,000 reais (approximately US$10,000) per day. On August 30, 2024, the ANPD suspended the preventive measure after Meta submitted an acceptable Adjustment Plan resolving the issues noted by the ANPD.

The original decision imposing the preventive measure noted four aspects of noncompliance with the LGPD: (i) inadequate identification of a legitimate interest to process sensitive personal data, including the necessity and purpose of processing such personal data and the failure to observe the legitimate expectations of the data subjects; (ii) lack of transparency in the disclosure of the new information to the data subjects, as well as the complexity and obscurity of the mechanisms for exercising their rights, especially the right to object to and opt out of the processing of their information (the decision notes that in Brazil, users were required to opt out by making eight clicks and filling out a lengthy form, whereas in Europe only three clicks and brief information were required for those opting out); (iii) limitation on data subjects' exercise of their rights, especially those who are not users of the company's platforms; and (iv) processing of children's and adolescents' personal data without necessary safeguards and without considering their best interest.

The Adjustment Plan submitted by Meta resolved these issues by providing for certain notices and disclosures to users of Meta's platforms on the use of their information for AI training, and the right of such users to oppose such use by Meta in a "facilitated" manner. Meta also committed not to process personal data of minors under the age of 18 (i.e., children and adolescents) for this specific purpose until a definitive settlement is executed with the ANPD.

It appears that the ANPD was piggybacking on actions by EU regulators in June that caused Meta to suspend the use of information from Facebook and Instagram posts to train its AI tools (currently occurring in the United States, which does not have strict data privacy rules). The EU action likely prompted the Institute for Consumer Defense to file a complaint with the ANPD. Brazil is one of the top four countries in terms of the highest number of Facebook users.

The investigation and orders against Meta are not unique. Earlier, on March 31, 2024, the ANPD published Technical Note No. 2/2024/FIS/CGF/ANPD opening an investigation of four banks for using personal data from the Brazilian National Social Security Institute or *Instituto Nacional do Seguro Social* ("INSS"). According to the Technical Note, the banks were being investigated for making offers of credit to individuals, based on complaints that the individuals were being contacted by financial institutions with offers for credit in relation to their Social Security benefits. The ANPD therefore launched an investigation into the sharing of personal data between the INSS and financial institutions.

For now, what evidence exists suggests that absent action by the authorities of other jurisdictions or the filing of a formal complaint, it is unlikely that the ANPD has the resources to identify other such instances of noncompliance, but that will certainly change over time. As was the case relating to the Meta proceeding, the ANPD appears to be taking a particular interest in the processing of personal data of children and adolescents without necessary safeguards (for example, obtaining the consent of their parents or guardians by verified means) and without considering their best interest

DISCLOSING DATA BREACHES, INCLUDING INSS DECISION

On April 26, 2024, the ANPD published Resolution CD/ANPD No. 15 on how companies should communicate and handle security incidents. The regulation requires communication to ANPD within three business days after a company obtains knowledge of an incident involving relevant risk or harm to personal data comprising one of the following:

- Sensitive personal data;
- Data from children, adolescents, or the elderly;
- Financial data;
- Authentication data in systems;
- Data protected by legal, judicial, or professional secrecy; and
- Large-scale data.

The information communicated to the ANPD is not presumed to be confidential, and confidential treatment needs to be justified in a request to the ANPD. The security incident

communication must also be made to the data subjects, preferably in a direct and individualized way (telephone, email, electronic message, or letter), in simple and easy-to-understand language, including the contact to obtain information and that of the DPO. The controller is required to maintain a register of all incidents, even if the relevant risk or harm suffered did not require it to be communicated to the ANPD.

In a significant enforcement action, on February 1, 2024, the ANPD published a decision, which was affirmed by the ANPD on appeal on July 26, 2024—the first decision of the ANPD to be appealed administratively. The February 1 decision required the INSS to publish on the first page of its website a communication about the breach of data that occurred between August and September 2022. In addition to reporting the leak, the nature and the extent of the breach, and the attendant risks to data subjects, must be disclosed. The decision stated that the disclosure must note that "among the data that may have been affected are official identity verification data, financial and health data (such as name, CPF, NIT, identity card, date of birth, gender, professional activity sector, bank details, and number of dependents) of an undetermined number of INSS beneficiaries and insured individuals, which could lead to the risk of identity theft, fraud, commercial harassment, among other damages." Such disclosure could obviously lead to legal actions by those affected by the disclosure.

In the decision, the ANPD also states that "the INSS immediately carried out preventive and corrective actions in the entity's processes and computer systems to mitigate the vulnerability detected in the system." The decision required the INSS to adopt several measures to improve its data protection practices. Given that the INSS is a public authority, no fines or penalties were assessed on the INSS.

INTERNATIONAL TRANSFER OF DATA

On August 23, 2024, the ANPD published Resolution CD/ANPD No. 19 providing a framework for international transfers of personal data. As with the European GDPR, a comprehensive framework is established ensuring that data transfers to third countries or international organizations must be done to entities and jurisdictions that provide an adequate level of data protection as per the LGPD. Just as the European Commission can decide if a third country ensures an adequate level of protection, the ANPD can recognize adequacy based on similar criteria.

Both frameworks provide for the use of standard contractual clauses ("SCCs") to ensure adequate safeguards. In the case of the LGPD, the clauses must be subject to Brazilian law and the jurisdiction of Brazilian courts. Processing agents who intend to use SCCs as a safeguard for international data transfers must incorporate them within 12 months.

The LGPD and the Resolution CD/ANPD No. 19/24 also enable processing agents to adopt tailored contractual clauses for international transfers of personal data, and binding corporate rules for intra-group transfers, both being subject to ANPD approval.

Although both the GDPR and the LGPD have transparency requirements, the LGPD mandates that controllers publish detailed information about international transfers on their websites in the Portuguese language, which can be done by a specific section within a privacy notice.

These recent actions in four areas make it clear that the ANPD intends to put teeth into requiring compliance with data privacy and protection rules by companies operating in Brazil, which need to enact and actively implement data privacy compliance policies.

LAWYER CONTACTS

S. Wade Angus
New York/São Paulo
+1.212.326.3755
swangus@jonesday.com

Sanjiv K. Kapur
Cleveland/São Paulo
+1.216.586.7114/+55.11.3018.3911
skapur@jonesday.com

Guillermo E. Larrea
Mexico City
+52.55.3000.4064
glarrea@jonesday.com

Mauricio F. Paez
New York
+1.212.326.7889
mfpaez@jonesday.com

Fernando F. Pastore
São Paulo
+55.11.3018.3941
fpastore@jonesday.com

Marcelo Padua Lima, a partner at Cascione Advogados, and Leonardo Albuquerque Melo, an associate at Cascione Advogados, contributed to this White Paper.