Paper as part of the Joint Project "Effective Implementation and Regulation Under the New Brazilian Data Protection Law"

The Role of the Brazilian Data Protection Authority (ANPD) under Brazil's New Data Protection Law (LGPD)

Centre for Information Policy Leadership (CIPL) and *Centro de Direito, Internet e Sociedade* of *Instituto Brasiliense de Direito Públic*o (CEDIS-IDP)

17 April 2020

This is one of a series of Short Papers produced as part of the special Joint Project "Effective Implementation and Regulation Under the New Brazilian Data Protection Law (LGPD)," by CIPL and CEDIS-IDP. This project aims to facilitate information sharing about the LGPD; inform and advance constructive, forward-thinking and consistent LGPD implementation and interpretation; enable sharing of industry experience and best practices; and promote effective regulatory strategies and oversight of the LGPD.

Contents

I. INTRODUCTION 3

II. THE CASE FOR AN EFFECTIVE ANPD, AND WHAT SHOULD BE ITS PRIORITIES 3

A. Why it is important to have a strong, technical and effective ANPD 3

B. Prioritizing the ANPD's specific roles and responsibilities under the LGPD 5

1. Preparing the National Policy for the Protection of Personal Data and Privacy 5

2. Recognizing good practices and best-in-class examples of accountable privacy programs 5

3. Establishing rules, procedures and guidance for organizations as required by the LGPD 6

4. Clarifying LGPD provisions 12

5. Encouraging the adoption of industry technical standards, and providing technical standards to organizations 13

6. Enabling international transfers of personal data 14

7. Raising awareness of data protection, and educating individuals and organizations 14

8. Developing its procedures for enforcement 15

C. Composition, staffing and resourcing of the ANPD 16

D. Final considerations about effective regulation 16

III. CONCLUSION 17

Appendix – Mapping of ANPD Tasks under the LGPD 18

The Role of the Brazilian Data Protection Authority (ANPD)
under Brazil's New Data Protection Law (LGPD)

I. INTRODUCTION

The *Lei Geral de Proteção de Dados Pessoais* (LGPD) provides for the establishment of a national data protection authority (DPA) for Brazil—the *Autoridade Nacional de Proteção de Dados* (ANPD). The LGPD gives the ANPD important responsibilities related to its interpretation, application and enforcement. Therefore, the ANPD will be of central importance to the effectiveness and success of this law.

Given the short timeline leading up to the effective date of the LGPD and the urgency of the LGPD's immediate priorities, it is important that the ANPD be established and become operational as quickly as possible. Regardless of the LGPD applicability date, the ANPD should be established immediately as a matter of urgency, given the number of ANPD actions that are necessary before the LGPD becomes effective and enforceable.

The LGPD includes many provisions that require further interpretation, guidance and action by the ANPD before they can be effectively implemented by covered organizations. These responsibilities and tasks require that the ANPD be made up of individuals with subject-matter and technical expertise in data protection, information technology and data science. It also requires that the ANPD has appropriate structure, resources, budget and institutional autonomy to be able to operationalize and discharge its responsibilities. Having such knowledge and operational structure will enable the ANPD to fulfill both the mandate of the LGPD and meet the reasonable expectations and needs of Brazilian individuals and regulated organizations.

This paper will briefly discuss the following issues: (a) why an effective national DPA is essential for the success of the LGPD and Brazil's digital economy; (b) the ANPD's specific responsibilities and tasks under the LGPD; (c) staffing and resourcing the ANPD, including the necessary professional backgrounds and profiles that must be represented within the ANPD members and staff; and (d) considerations and principles for effective oversight and regulation and constructive engagement with the regulated organizations.

II. THE CASE FOR AN EFFECTIVE ANPD, AND WHAT SHOULD BE ITS PRIORITIES

A. WHY IT IS IMPORTANT TO HAVE A STRONG, TECHNICAL AND EFFECTIVE ANPD

All international DPAs share a number of core responsibilities that are inherent to their regulatory position. These are responsibilities relating to protecting individuals; ensuring that digital, economic and societal development is in line with data privacy values; and ensuring the effectiveness of the LGPD. They illustrate the importance of the immediate establishment of a strong and effective ANPD.

- **Ensuring appropriate conditions for the digital transformation of Brazil's economy and society**. Protecting personal data is about building trust in the digital society and ensuring economic and technological development, innovation and free enterprise (see Article 2 of the LGPD). The ANPD will be well placed to support this digital transformation, given that it must have technical expertise on data protection, information technology and data science.
- **Driving consistency in the interpretation and enforcement of the LGPD and related laws**. Consistency results in legal certainty for both individuals and organizations as well as

A 2017 report by the US Chamber of Commerce showed that a favorable regulatory environment in Brazil's cross-border information technology and communications services would add $1.19 billion in government revenue, $25.44 billion in GDP contribution, $5.31 billion in increased investments and 78,420 jobs in the long term in Brazil.

trust in the digital economy. Brazilians should be able to expect the same level of privacy protection and substantive rights regardless of where they are located and who they interact with. Businesses need consistency and legal certainty in order to operate effectively, and foreign companies expect such consistency in order to invest in Brazil.

- **Providing necessary guidance to organizations on data protection**. The LGPD is principles-based and therefore leaves flexibility for organizations to implement many of its provisions as appropriate to their businesses and the risks of their processing activities. However, certain provisions require further clarification by the ANPD—see Section B below. It is important that the ANPD prioritize the development of guidance to support organizations, in particular SMEs and startups, in implementing appropriate measures to protect individuals' personal data.
- **Educating individuals and organizations about data protection**. The LGPD is the first comprehensive data protection law in Brazil and, as such, brings new rights to individuals as well as compliance requirements for public and private organizations. As Brazil moves towards a digital society and economy, Brazilians must be educated about their data protection rights. They must have a basic understanding of how they can control their personal data and trust the data ecosystem. In turn, organizations must be made aware of their obligations and responsibilities to individuals. They must take appropriate protective measures and be accountable in order to enable digital trust. The ANPD has a key role in educating both individuals and organizations by working with them in a collaborative and constructive manner.
- **Delivering legal certainty on enforcement to both individuals and organizations**. The ANPD must have primary responsibility for the interpretation and enforcement of the LGPD—see Section B below. In parallel, it must interact with other regulators (e.g., consumer or competition regulators and public prosecutor's offices) where there are areas of overlap. A consistent and centralized approach to data protection interpretation and enforcement by the ANPD will make it easier for individuals to submit complaints and help clarify the most appropriate complaint channel. It will also prevent individuals from making multiple complaints on the same issue to various regulators. In turn, it will provide organizations with legal certainty and a single interlocutor on all matters of data protection regulation and enforcement. It will also prevent regulators from undertaking multiple enforcement measures on the same issue.
- **Serving as Brazil's primary expert on emerging data protection policy thought-leadership and practices**. The ANPD must lead and competently inform the national debate on data protection. To effectively do so, it must not only have expertise on the law it enforces, but also on the technologies and organizations it regulates. For this, it should constructively engage with organizations in the private and public sectors, as well as with other regulators—see Section D below.
- **Enabling effective bilateral collaboration with international counterpart DPAs**. Most modern data uses are not confined within national borders. Similarly, many alleged data protection violations will have international dimensions and implications. This will require the ANPD to collaborate with its counterpart DPAs in foreign countries.
- **Being Brazil's main point of contact and representative in international forums and organizations**. DPAs around the world are currently working together through a number of cooperation bodies, conferences and mechanisms. The ANPD must participate in these to ensure that Brazil has a voice in global data protection discussions and on the development of global data protection policies. Article 55-J-IX specifically gives

Forums where DPAs around the world work together include the OECD Working Party on Security and Privacy in the Digital Economy (SPDE), the Global Privacy Assembly (GPA) (formerly the International Conference of Data Protection and Privacy Commissioners (ICDPPC)), the Ibero-American Data Protection Network (RIPD), the Global Privacy Enforcement Network (GPEN) and the APEC Cross-border Privacy Enforcement Arrangement (CPEA).

the ANPD the duty to "promote cooperation with DPAs of other countries, of international or transnational nature."

- **Advancing global harmonization of data protection**. Enabling and preserving regional and national differences in privacy and data protection can be important. However, the vast majority of core privacy protection principles can and should be harmonized between different global privacy regimes. The ANPD should be able to identify where the LGPD aligns with recognized global privacy regimes (such as the EU's General Data Protection Regulation—GDPR[1]), and where it differs from them. This will enhance the overall level of data protection for Brazilians and enable Brazilian organizations to do business on a global scale.

B. PRIORITIZING THE ANPD'S SPECIFIC ROLES AND RESPONSIBILITIES UNDER THE LGPD

The LGPD sets forth a significant role for the ANPD. The ANPD must ensure that personal data is protected under the LGPD (Article 55-J-I) through issuing technical opinions and guidance (Article 55-J-XX), education (Article 55-J-VI), enforcement (Article 55-J-IV), complaint-handling (Article 55-J-V), international facilitation (Article 55-J-IX), and drafting and updating rules and regulations (Article 55-J-XIII).

To enable this role, the LGPD also gives a wide array of specific duties and tasks to the ANPD that are crucial to the LGPD's effectiveness. The ANPD needs to be established as quickly as possible so it can begin to execute these tasks and, in particular, to develop the necessary guidance that organizations need to come into compliance with the LGPD. Absent such guidance and required clarifications from the ANPD, organizations will not be able to fully and effectively implement and comply with the law.

The following LGPD provisions contain the most urgent obligations of the ANPD:

1. Preparing the National Policy for the Protection of Personal Data and Privacy

Article 55-J-III requires the ANPD to issue guidelines for the National Policy for Privacy and Data Protection (National Policy).

The National Policy will be the instrument through which the ANPD will set out its strategy and priorities, and define how it will operate in the most effective manner—see Section D. When drafting this document, the ANPD should take into account the short time between its establishment and the effective date of the LGPD and tailor its enforcement plan to that. This plan should focus on the immediate actions that the ANPD should take to most act more effectively towards the protection of Brazilians and the Brazil economy—as per outlined in the following points of this Section B.

Working on this strategic plan should be a top priority for the ANPD, as it will help the ANPD carry out the rest of its duties. This National Policy should be subject to public consultation to ensure that stakeholders of all types are able to provide input.

2. Recognizing good practices and best-in-class examples of accountable privacy programs

Article 50 provides that controllers and operators[2] can develop good practices relating to the governance of data processing activities. Article 50, paragraph 2 provides that such good practices could be operationalized

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1567000484507&uri=CELEX:32016R0679>.

[2] "Operators" is the term used in the LGPD equivalent to "data processors" in the GDPR. According to Article 5, VII of the LGPD, operators are "natural or legal persons, of a public or private nature, who process personal data on behalf of the controller."

in the form of privacy governance programs, and outlines a series of elements for these programs that relate to organizational accountability.[3] Article 50, paragraph 3 provides that the ANPD can acknowledge and promote such good practices. In fact, developing good practices and governance can help organizations comply with Article 6-X, which provides that data processing activities shall adhere to an accountability requirement.

Accountability is globally recognized as a key building block for effective privacy and data protection regulation. It allows organizations to be able to effectively protect personal data, and to demonstrate the measures taken towards such protection. Having a comprehensive privacy program in place is the foundation for compliance with all applicable privacy obligations established by law, regulation or other standards. The specific core elements of accountability-based privacy programs (such as risk assessment, monitoring and enforcement) ensure ongoing privacy compliance and that the program remains current when technologies and business practices change.

The LGPD explicitly incorporates the principle of accountability and encourages organizations to establish privacy programs to operationalize it. The ANPD should, as its top priority, exercise its mandate to promote and recognize such programs. This will be particularly helpful for SMEs and less mature Brazilian companies that may not have the experience or resources to effectively comply with the LGPD without examples of best practices and tools.

This work does not have to start from scratch. For instance, CIPL's Accountability Framework[4] has been widely used by global organizations for compliance with privacy laws across multiple jurisdictions. There are also other global frameworks that provide models for appropriate good practices and governance frameworks that might eventually be developed in Brazil—such as the ISO Standards, the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) System and binding corporate rules (BCR). In fact, private sector organizations in Brazil are already working with law firms and consultancies on such LGPD compliance frameworks that will need to be reviewed and recognized by the ANPD.

3. Establishing rules, procedures and guidance for organizations as required by the LGPD

Another top priority for the ANPD should be providing guidance on various topics where required and allowed by the LGPD. Organizations in Brazil need clarity and guidance on whether their internal processes are in accordance with the LGPD, in order to implement the LGPD and appropriately provide for effective protection to individuals' personal data.

3.1 Rules on data sharing

Data sharing is a key feature and enabler of the digital economy. According to the Information Commissioners' Office (UK ICO), data sharing consists of the sharing of personal data between organizations

[3] CIPL has worked extensively on organizational accountability and has published a series of papers outlining the elements of accountability and how organizations can operationalize accountability. Please see the following CIPL white papers: The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society, July 23, 2018, available at <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf>; and Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability, available at <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf>.

[4] CIPL's Accountability Framework can be found in the papers mentioned in footnote 3. It is composed of seven accountability elements: leadership and oversight; risk assessment; policies and procedures; transparency; training and awareness; monitoring and verification; and response and enforcement.

that are controllers (rather than between controllers and processors, who act upon the instructions of controllers). Data sharing includes giving access to data to a third party, by whatever means, regardless of their location. It can take place in a routine, scheduled way or on a one-off basis.[5]

The LGPD sets forth specific rules and limitations on data sharing that require further elaboration from the ANPD. Without guidance on data sharing, organizations may choose not to invest resources into certain common and/or necessary data sharing practices. It might also paralyze organizations in cases where data sharing is urgent and needed for public interest purposes.[6] Organizations, both private and public, will fear that the ANPD might prohibit such data sharing practices and take enforcement measures against them.

(i) Sharing of sensitive personal data between controllers

Article 11, Paragraph 3 gives the ANPD the authority to regulate or prohibit the sharing of sensitive personal data "for the purpose of economic advantage" upon consultation with the relevant public entities.

Guidance relating to the sharing of sensitive personal data is particularly important. Such guidance should address, for instance:

- The meaning of "for the purpose of economic advantage" and whether sharing of personal data would be allowed for public interest purposes;
- Whether data sharing would be allowed when individuals provide informed consent;
- Sharing of sensitive personal data where individuals are unable to provide consent or where it is substantially difficult to obtain consent, in particular when there is no direct threat or risk of harm to individuals (e.g., health crisis);
- Sharing of sensitive personal data by SMEs and startups and how to measure risks (e.g., local pharmacies);
- Cases of data sharing through application program interfaces (APIs); and
- Cases of sharing of sensitive data in AI applications where such data is necessary to ensure fair processing and avoid algorithmic bias and discrimination.

(ii) Data sharing from public to private organizations

Article 26, paragraph 1 prohibits data sharing from public organizations to private organizations, except when it falls under one of the circumstances described therein (e.g., when data is publicly available or when needed for the execution of a contract). Article 27 provides that such data sharing may happen only with the data subject's consent, except when: (i) the law determines that consent is not needed; (ii) public organizations have provided information to the public according to Article 23-I; and (iii) it is allowed under one of the exceptions of Article 26, paragraph 1. Article 27 and its sole paragraph also provide that public sector organizations will have to notify the ANPD whenever they share data with private organizations, and that the ANPD may further regulate how this information should be provided. Finally, Article 30 provides that the ANPD may issue complementary rules on data sharing from public to private organizations.

Data sharing between public and private organizations is common practice in any economy, but must be accompanied by accountability measures and safeguards from all parties involved in the sharing scheme. Hence, the ANPD guidance on this topic is also of particular importance.

---

[5] UK ICO Data Sharing Code of Practice – Draft code for consultation. Available at <https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-the-draft-data-sharing-code-of-practice/>.

[6] See as an example guidance provided by the UK ICO on Data Protection and Coronavirus, which aims at providing organizations, in particular of the health sector, with certainty that they can proceed with virus containment measures that require processing of personal data. Available at <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/data-protection-and-coronavirus/>, 12 March 2020.

Such data sharing is needed, for instance, during the onboarding process of new payment service providers as banks must obtain their tax information from the Brazilian tax authority (*Receita Federal*). It is also needed in the context of commercial acquisitions where organizations must obtain certain information from federal and state authorities, which in many cases includes personal data about the individuals involved in the operation. Data sharing from public to private organizations is relevant for public interest purposes where industry lacks information that could be used to develop products and services that would drive improvements in the public sector (such as the health sector).

Finally, the current COVID-19 pandemic has reinforced the need for specific data sharing between the private and public sectors in order to track, model, predict and combat the spread of the virus. Many DPAs around the globe have issued information, guidance and advisory statements and documents to their national and international stakeholders.[7]

The ANPD should clarify, as soon as possible:

- The circumstances under which public sector organizations may share personal data with private sector organizations;
- The role of consent and contracts in such data sharing, and circumstances where consent is not needed or obtaining consent is a cumbersome task;
- Whether all data sharing activities require notification of the ANPD, or whether such notification should be provided based on the level of risk involved in the data sharing; and
- The type of accountability measures and safeguards to enable trusted data sharing.

3.2 Rules on the right to data portability

Article 18, V of the LGPD provides the ANPD with authority to issue regulations on how to implement the right to data portability.

Data portability is a key enabler of the digital economy. It allows for individuals to promptly move their personal data from a service to another instead of being "locked" into a particular service provider. If well regulated, this right can work as an enabler of digital trust, competition and economic growth, particularly for SMEs.

The right to data portability is not a new right under Brazilian laws and regulations. The banking sector is working with data portability in the context of credit portability between financial institutions and open banking. Users of telecommunications services also benefit from portability rules. In addition, the tech industry is also working internationally to implement data portability as a data protection right.[8]

The ANPD should work with multiple stakeholders, including industry sectors and other Brazilian regulators, to understand and maximize the benefits and opportunities of data portability for individuals and organizations. ANPD regulation on data portability has the potential to drive the standardization of interoperability rules related to personal data. This will result in efficiency gains to the Brazilian digital economy, better and diversified services for consumers, and the accomplishment of this data protection right.

3.3 Guidance on information to be given to individuals about processing activities

Article 55-J-X requires the ANPD to lay out the means by which companies should communicate information about their data processing operations to the public, with regards to trade and industrial secrecy. This is a

[7] See, for example, the Global Privacy Assembly's Data Protection and Coronavirus (COVID-19) Resources, which has compiled guidance and information from data protection authorities on data protection <https://globalprivacyassembly.org/covid19/>.
[8] See, for instance, the Data Transfer Project, available at <https://datatransferproject.dev/>.

key piece of the LGPD's transparency principle enshrined in Article 6, VI, and of the right of data subjects to obtain clear, adequate and comprehensive information about data processing under Article 9 of the LGPD.

For individuals to be able to exercise their data protection rights under the LGPD and have control over their personal data, they first need to understand how organizations are collecting and using such data. However, the level of understanding and of information provided will depend on a number of circumstances such as the context of the processing operations (e.g., Internet of Things devices versus mobile applications), the age group of individuals (e.g., children versus adults versus elderly people), the complexity of the processing activities (e.g., data processed for payroll versus data analytics), etc.

Internationally, organizations have developed good practices concerning informing individuals about data processing. These include, among others: using a layered approach to providing information, using resources such as videos and illustrations rather than only text-based information, and providing information in different stages of the transaction between the user and organization. Providing information to individuals has, therefore, moved well beyond mere legalistic privacy notices to more design-led and user-centric transparency.

The ANPD must prioritize issuing guidance on how organizations should seek to provide contextual, effective and actionable information to individuals in a way that does not create "notice fatigue."

3.4 Rules on the timeframe and means for responding to data subject rights requests

Article 18 of the LGPD sets out the individual data protection rights. Paragraph 5 establishes that the timeframes and means for organizations to respond to requests relating to the exercise of these rights will be further regulated (with no express mention to the ANPD).

In addition, Article 18, I and II of the LGPD provides that individuals have the right to obtain confirmation about the existence of data processing activities from controllers, as well as the right to have access to their personal data. Article 19 provides that these should be provided in simplified format and immediately, or in a comprehensive manner within 15 days. In addition, Article 19 paragraph 3 authorizes the ANPD to issue further regulations on access in specific circumstances.

The exercise of data protection rights allows individuals to have control over their personal data. Due to the complexity of data processing operations, organizations need time to respond to individual requests. This may include verifying the identity of the individual making the request; analyzing and clarifying the request where necessary; locating the data in various systems, databases and servers; responding to individuals in an intelligible format; deleting data/limiting the processing where requested; and other operations. Most organizations will need to adapt exiting processes and will need to take factors into account such as interoperability issues between different systems.

The ANPD is the best-placed authority to issue rules on the timeframe and means for organizations to respond to data subject rights requests and should do so as a matter of priority. The LGPD is silent on the timeframe for most rights and only sets out a short timeframe of 15 days for the right of access. The ANPD should engage with organizations of various sizes and sectors to help it understand the complexity of their processing operations in order to determine the most appropriate and realistic timeframes and means for responding to requests. It should also consider following international standards—for instance, the GDPR sets out a timeframe of one month to respond to data subject rights requests, extendable for two further months depending on the complexity and number of requests.[9]

3.5 Rules on the role and duties of the data protection officer

Article 41 of the LGPD provides that controllers must appoint an individual or entity to be in charge of processing personal data. Such an individual, referred by the LGPD as "person in charge," is often referred to internationally as a data protection officer, or DPO. Paragraph 2 lists the DPO activities and paragraph 3

[9] Article 12(3) of the GDPR.

provides that the ANPD may issue complementary rules concerning the definition and tasks of DPOs. These include where organizations would be exempt from appointing a DPO due to their nature and size, as well as the size of their data processing operations.

The function of the DPO is an essential component of data privacy accountability. It plays a crucial role in enabling organizations to ensure and demonstrate both data privacy compliance and effective privacy protection of individuals.[10]

There are some areas that may present challenges for organizations, or require clarification, interpretation and guidance to ensure an effective implementation of the DPO role. These include: whether multiple organizations within a single corporate group can appoint a single DPO; whether organizations can have multiple DPOs; whether the role of the DPO can be outsourced; and others. When issuing rules on the role of the DPO, the ANPD must encourage a flexible and outcome-based interpretation of the DPO requirements to make them work for large multinational organizations, as well as SMEs, start-ups, NGOs and public authorities.

3.6 Rules and procedures on risk assessments and the concept of "high-risk" processing

One of the tasks of the ANPD under Article 55-J-XIII is to issue rules and procedures concerning privacy and data protection, as well as on data protection impact assessments (DPIAs) when data processing may result in high risk to the data protection principles outlined in the LGPD. In addition, Article 38 provides that the ANPD may require controllers to prepare DPIAs. Article 10, Paragraph 3 further specifies that the ANPD may require DPIAs when controllers process personal data based on their legitimate interests.

The LGPD also touches upon the notion of risk in various other provisions, including: (i) Article 44-II, which provides that data processing will be considered "irregular" when unlawful or when it does not meet the reasonable expectations of data subjects concerning security of their personal data, taking into account the risks that are reasonably expected from data processing; (ii) Article 48, which determines that controllers must communicate to the ANPD and to data subjects about the occurrence of data breaches that may result in risks to data subjects; (iii) Article 50, Paragraph 1, which provides that the controllers will have to take into account the risks to, and benefits of, processing activities when developing good practices relating to the governance of such activities; and (iv) Article 50, Paragraph 2, I-d, which outlines risk assessments as one of the possible elements of privacy compliance programs.

As seen above, various provisions of the LGPD specifically refer to the concepts of "risk" and "high-risk" processing, and to risk assessments (including DPIAs). Thus, the LGPD effectively incorporates a risk-based approach to data protection, requiring organizations to undertake a balancing exercise between risks and benefits to individuals resulting from data processing activities both when setting their privacy program and when implementing certain requirements of the LGPD. The LGPD, however, does not define the term "high-risk," nor the notion of a risk-based approach. The LGPD requires the ANPD to issue rules on DPIAs and requires organizations to undertake these assessments.

Before the ANPD requires risk assessments to be undertaken, it should consult with industry and provide guidance on the notion of risk and the elements to be balanced out as part of these assessments.[11]

---

[10] CIPL DPO Paper - Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation, available at <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_gdpr_dpo_paper_17_november_2016.pdf>.

[11] CIPL has written extensively on the notion of risk-based approach: Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR, available at <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf>; A Risk-based Approach to Privacy: Improving Effectiveness in Practice, available at <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-

Furthermore, the ANPD rules and procedures should provide guidance on different methodologies for the risk assessments that underlie many of the LGPD's compliance requirements, but give flexibility to organizations to decide on the methodology that is most appropriate to their business and data processing activities. The ANPD should also address the timelines for organizations to provide DPIAs when requested by the ANPD. It should consider that, given the nature of the requirement and the nature and complexity of the processing operations being assessed, organizations may need longer periods, such as 30 to 60 days, to provide DPIAs upon request.

3.7 Rules concerning the timeframe for data breach notification to the ANPD

Article 48 provides that controllers shall notify the ANPD and data subjects, within a reasonable timeframe, about data security incidents that may result in risk or harm to data subjects. Paragraph 1 gives the authority to the ANPD to define what constitutes a "reasonable timeframe."

As with the timeframes for responding to individual rights requests as mentioned above, organizations need legal certainty in order to implement this LGPD requirement. The ANPD must define, as soon as possible, what constitutes a "reasonable timeframe" for notification of data security incidents. For instance, 10 working days would constitute a reasonable timeframe, as it would allow organizations to analyze the security incident and work on measures to minimize its impact on individuals, instead of concentrating their efforts on the notification requirements.

The ANPD should also provide clarity on what would constitute "risk or harm to data subjects," and how organizations can assess these risks in the context of a data breach—see above on rules and procedures on risk assessments and the concept of "high-risk" processing. It is important for both organizations and the ANPD to limit incident notification to only what is absolute necessary to avoid the ANPD's and individuals' being overwhelmed with minor and trivial notifications. Excessive notification may result in unnecessary reputational damage to organizations and may unnecessarily increase the ANPD's workload. It should not be considered necessary for organizations to notify the ANPD and data subjects about minor incidents. For example, some international guidelines provide examples of incidents that are or are not subject to notification requirements.[12]

3.8 Rules, guidelines and simplified and special procedures for SMEs

Article 55-J-XVIII provides that the ANPD shall issue rules, guidelines and simplified procedures, including timelines, to assist SMEs and startups with implementing the LGPD.

Complying with the LGPD will be particularly challenging for SMEs due to their limited resources, budget, data protection maturity and compliance experience. The ANPD should not only provide user-friendly guidance, but also simplified tools that would empower SMEs to assess the risks of their data processing activities and implement key LGPD requirements to mitigate those risks. The ANPD should look at examples of simplified guidance and tools for SMEs provided by DPAs across the globe, such as the UK ICO,[13] the Irish

---

a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf>; Protecting Privacy in a World of Big Data, The Role of Risk Management, available at <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big_data_paper_2_the_role_of_risk_management_16_february_2016.pdf>; The Role of Risk Management in Data Protection, available at <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_2-the_role_of_risk_management_in_data_protection-c.pdf>.

[12] See the Working Party 29 Guidelines on Personal data breach notification under Regulation 2016/679, adopted on 3 October 2017 and endorsed by the European Data Protection Board during its first Plenary Meeting. Available at <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>.

[13] ICO SME data protection hub, available at <https://ico.org.uk/for-organisations/business/>.

Data Protection Commissioner (Irish DPC)[14] or the Spanish Data Protection Agency,[15] among others. It should also consider setting out specific helplines to answer SMEs' queries and support their compliance.[16]

3.9 Rules for legacy (pre-LGPD) databases to comply with the LGPD

Article 63 provides that the ANPD will issue rules on how existing databases established prior to the LGPD applicability date can gradually comply with its requirements, taking into account the complexity of the involved data processing and the nature of data.

The LGPD, however, does not define the term "databases." In theory, all organizations that hold and process personal data use databases in some form and the term could be interpreted to mean any IT systems processing personal data. The ANPD should clarify the intent of this LGPD requirement. It should also clarify under what circumstances organizations would fall under it, as well as what LGPD obligations they would be able to gradually comply with under these circumstances and how.

4. Clarifying LGPD provisions

Article 55-J, XIII provides to the ANPD a general task to issue guidance and procedures concerning privacy and data protection.

As mentioned before, the ANPD must have primary responsibility for the interpretation of the LGPD. This includes interpreting LGPD provisions that require further clarification in order for organizations to implement them with legal certainty.

Provisions that require clarification include (but are not limited to):

- Which organizations would fall under scope of the LGPD as per Article 3 in complex data processing circumstances, such as whether the law would apply to a controller that is located outside of Brazil solely for the fact that it uses operators who are located in Brazil, even though this controller did not collect personal data in the Brazilian territory nor did it target or offer services to Brazilian individuals;
- How organizations can "take into account the purposes, good faith and public interest" when processing publicly available personal data, as per Article 7, paragraph 3 of the LGPD, and what consists of "publicly available personal data";
- Who is responsible for providing information to individuals about data processing activities and under what circumstances, as required by Article 9 of the LGPD;
- What consists of "misleading and abusive information about data processing," which would render consent invalid under Article 9, paragraph 1 of the LGPD;
- How rules around governance and good practice adopted under Article 50 can lay down the obligations for each party involved in data processing activities, in particular taking into account that the LGPD does not expressly require them to enter data processing agreements or related contractual measures; and
- How organizations should comply with the LGPD provisions concerning the processing of children's personal data, including providing information to children under Article 14, paragraph 6 of the LGPD; addressing identity verification issues; addressing issues concerning vulnerable children who cannot obtain parental consent but still have a right to benefit from accessing the internet, etc.; and others.

[14] Irish DPC Guidance for SMEs, available at <https://www.dataprotection.ie/en/guidance-landing/guidance-smes>.
[15] AEPD Tool for SMEs "Facilita RGPD," available at: <https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd>.
[16] See, for instance, the ICO helpline available at <https://ico.org.uk/global/contact-us/advice-service-for-small-organisations/>.

5. Encouraging the adoption of industry technical standards, and providing technical standards to organizations

Technical standards are an important and flexible tool to enable implementation of legal requirements in the field of data protection and data security. The ANPD should encourage more broadly the creation of standards and also the consideration and adoption of already established international standards.

5.1 Industry technical standards for data subjects' rights

Articles 51 and 55-J-VIII give the ANPD the duty to "encourage" the adoption of technical standards that facilitate the data subjects' control over their personal data, taking into account the nature of the processing activity as well as the size of controllers and operators.

Even though the LGPD envisions that such technical standards will be developed by industry groups, the LGPD implies a proactive role for the ANPD in facilitating the development of such technical standards. This role requires recognition of, and familiarity with, the complexity of the digital economy, businesses and the nature of their processing activities. The ANPD should also actively engage with industry and other relevant stakeholders on this issue.

5.2 Technical and organizational standards for data security

Article 46 of the LGPD provides that controllers and operators must implement technical and administrative security measures to protect personal data. Paragraph 1 provides the ANPD with the authority to articulate the minimum technical standards for these security measures, in particular concerning the protection of sensitive personal data.

Organizations, particularly SMEs, need clarity on what is the minimum expected from them in the various scenarios of data processing, so that they can adequately protect personal data, taking into account the risks of their processing activities. In carrying out its duty with respect to data security standards, the ANPD must take into account that appropriate security protection measures will vary depending on the nature of the business and the processing activities involved as well as the types of personal data processed. It must also devise standards that are flexible, adaptable and future-proof and not locked into the current state of the art in data security.

Finally, the ANPD should be also guided by the existing international data security standards, such as the PCI Payment Card Industry standards[17] and the different ISO data security standards,[18] as these are already commonly used globally and will be familiar to many Brazilian companies that operate globally.

5.3 Anonymization standards and techniques

Article 12 of the LGPD provides that anonymized data will not be considered personal data under the LGPD, except when the anonymization process is reversed or capable of being reversed by reasonable means. Therefore, processing of anonymized data falls outside the scope of this law. Paragraph 3 of Article 12 provides the ANPD with the authority to issue anonymization standards and techniques, and to verify their security, after consulting the National Data Protection Council.

Strong data anonymization should be encouraged and enabled, as it is key to innovation and the Brazilian digital economy. It allows for not only protective data processing in general, but also organizations to continue processing and extracting value from data in contexts outside of the original purposes for which the

[17] PCI Security Standards, available at <https://www.pcisecuritystandards.org/pci_security/>.
[18] See, for example, ISO/IEC 27001, Information Security Management, available at <https://www.iso.org/isoiec-27001-information-security.html>; and ISO/IEC 27701: 2019, Security techniques – Extension to ISO/IEC 27001 and ISO 27002 for privacy information management – Requirements and guidelines, available at <https://www.iso.org/standard/71670.html>.

data was collected. The ANPD should provide anonymization standards and techniques as soon as possible, as well as issue guidance on what constitutes "reasonable means" for reversing data anonymization. Finally, the ANPD should draw inspiration from and encourage convergence with some of the existing anonymization guidance and best practices issued by DPAs and some academic and commercial organizations.[19]

6. Enabling international transfers of personal data

Article 33-I provides that international transfers of personal data will be allowed to countries or international bodies that provide for a level of data protection that is equivalent to the protection provided by the LGPD. Alternatively, Article 33-II also allows for international data transfers to be carried out when organizations put in place protective mechanisms. These mechanisms include: standard contractual clauses, contractual clauses that are specific to certain data transfers, global corporate rules, seals, certificates and codes of conduct.

The ANPD is responsible for determining when a third country or international body has an adequate level of data protection under Article 34. Similarly, the ANPD is responsible for defining the content of the mechanisms mentioned above under Article 35.

Data transfers are a key component of data processing activities, in particular for businesses that operate in a global digital economy—either conducting businesses with global companies or expanding their businesses beyond Brazilian borders. Having appropriate data transfer mechanisms in place is particularly relevant for SMEs, whose growth may often depend on partnering with international businesses.

As drafted, the LGPD could be interpreted to prohibit international transfers until the ANPD publishes a list of adequate countries or defines the content of transfer mechanisms. Therefore, the ANPD should clarify as soon as possible that organizations can still apply the mechanisms of Article 33 of the LGPD to enable international transfers of personal data (e.g., specific contractual clauses), while the ANPD is working on the content of transfer mechanisms and assessing the adequacy of third countries.

Moreover, when defining the content of transfer mechanisms and undertaking adequacy assessments, the ANPD should look at international examples and engage with international bodies who have already gone through this experience (e.g., the European Commission and APEC). In particular, the ANPD should recognize international privacy certification schemes as enablers of international transfers, as they require certified organizations to put in place a series of high-standard data protection measures. Examples of such certification schemes include certifications provided by the:

- International Organization for Standardization (ISO);
- APEC-CBPR System;
- APEC Privacy Recognition for Processors (PRP);
- EU-US Privacy Shield;
- Binding Corporate Rules (BCR); and
- National Institute of Standards and Technology (NIST).

7. Raising awareness of data protection, and educating individuals and organizations

One of the tasks of the ANPD under Article 55-J-VI is to raise public awareness of data protection laws and regulations. A related task under Article 55-J-VII is for the ANPD to encourage and undertake studies concerning national and international privacy and data protection activities.

[19] See, for example, the ICO's "Anonymisation: Managing Data Protection Risk Code of Practice," available at <https://ico.org.uk/media/1061/anonymisation-code.pdf>; and the Irish DPC's guidance on "Anonymisation and Pseudonymisation," <https://www.dataprotection.ie/en/guidance-landing/anonymisation-and-pseudonymisation>.

For the LGPD to be an effective law, all stakeholders involved must be made aware of their rights and obligations under this law. Individuals must be educated about their data protection rights and how to exercise them, and organizations must be made aware of their obligations. Raising awareness is thus one of the most important tasks for the ANPD. The ANPD should develop an education, communications and awareness-raising strategy accompanied by a short-term action plan (e.g., two years). To do so, it should identify and engage with key stakeholders who could work as partners for delivering such a plan (e.g., academic institutions, NGOs, privacy experts, media and tech platforms).

8. Developing its procedures for enforcement

8.1 Establishing an administrative procedure for enforcement

Article 53 requires the ANPD to set out enforcement rules concerning sanctions for LGPD noncompliance, including on how the ANPD will calculate fines. These rules must be subject to public consultation. Article 52, paragraph 4 provides that the ANPD may take into account the annual turnover of organizations when issuing fines.

The ANPD duties relating to clarifying and interpreting the LGPD, issuing guidance concerning its implementation and educating stakeholders are key initial responsibilities for any newly established DPA. This is particularly relevant in the context of a country that does not have a history with a legal framework for data protection. However, no DPA can be effective without appropriate procedures for enforcing the law it has been charged to enforce.

The ANPD should therefore develop and be transparent about its enforcement priorities and procedures, including addressing how it will calculate fines. These should take into account the severity of the noncompliance activity, its risks to individuals and any mitigation measures taken by organizations in the context of their accountability efforts and privacy compliance programs. The ANPD should also take into consideration that, in the short-medium term, organizations are working toward LGPD compliance in an uncertain scenario as many LGPD provisions are still open to further regulation and clarification by the ANPD.

In addition, when enforcing the LGPD, the ANPD must always take into account and follow the principles and criteria of the Brazilian Constitution and in Law No. 9.784 from January 29, 1999. These include, among others, the principles of legality, purpose, motivation, reasonableness, proportionality, morality, right to a full defense and legal certainty.

Finally, transparency is an important principle for the ANPD—not only when setting and communicating these enforcement priorities and procedures, but also when executing its supervisory and enforcement powers. Transparency builds trust among all stakeholders, including with individuals and regulated organizations.

8.2 Implementing mechanisms to receive complaints

Article 55-J-V requires the ANPD to appraise petitions from data subjects if a controller has not resolved an earlier related complaint. Article 55-J-XXIV also requires the ANPD to implement mechanisms to register complaints from data subjects, and Paragraph 6 of that section notes that complaints may be analyzed and resolved in an aggregated manner.

Handling complaints is one of the key duties of any DPA, and is a key enabler of individuals' redress and control over their personal data. The ANPD is a regulator for organizations, but also for individuals. As such, it must be available to respond to their concerns, queries and complaints.

Therefore, the ANPD must establish procedures to allow it to receive, analyze and respond to individuals' complaints. It should take into account the high number of Brazilians who classify as data subjects under the LGPD and who could potentially submit complaints, and explore any technological tools available to streamline this process (e.g., identity verification tools, ticketing systems, etc.). It should be ready to take a

position or adapt its processes where there are peaks in complaints, e.g., after a possible large data breach by a tech company that caught media attention). Finally, it should also consult with other Brazilian regulators and learn from their experiences of dealing with the public.

To ensure efficiency and avoid being "paralyzed" by large numbers of complaints, the ANPD should educate individuals and remind them that they should initially address their complaints to the relevant organizations. It is a duty of accountable organizations to develop a complaint-handling procedure and deal with any issues individuals may have. Only those complaints that are not initially resolved by an organization should be channeled to the ANPD.

C. COMPOSITION, STAFFING AND RESOURCING OF THE ANPD

The ANPD must be properly resourced (both financially and in terms of headcount) and possess the necessary technical knowledge and expertise to effectively perform its duties and enforce the LGPD. This means having sufficient numbers of lawyers, information security professionals, technologists, economists and other professional staff with relevant technical expertise, taking into account Brazil's characteristics and size.

By comparison, since the implementation of the GDPR, the UK ICO has increased its workforce by 40 percent to 700 employees, and aims to have 825 full-time employees by 2021.[20] The UK's population is 66.5 million, while Brazil's is more than three times as large at 211 million, which gives an indication of just how many employees the ANPD might need to carry out its duties. Similarly, Ireland's Data Protection Commissioner (DPC) increased its staff from roughly 110 at the end of 2018 to 140 at the end of 2019.[21] Twenty-one EU countries in total increased their budgets for their DPAs in 2019, seventeen of which said they would need at least a 30–50 percent increase in budget.[22]

Brazil may not be able to immediately achieve the same level of resourcing and staffing as these jurisdictions, in particular since the LGPD established the ANPD without increasing the overall budget of the office of which it is a part, the Brazilian Presidency. However, a combination of reasonable reallocation of resources, qualified and experienced staff, and strategic prioritization of tasks will nevertheless enable the ANPD to achieve reasonable effectiveness within the existing time and budgetary constraints.

D. FINAL CONSIDERATIONS ABOUT EFFECTIVE REGULATION

Effective regulation depends on effective strategies to make the best possible use of available resources. This includes prioritizing and concentrating on regulatory activities that promise the best outcomes for individuals and society.

As outlined above, the ANPD should prioritize its activities related to "responsive" regulation, which attempts to foster effective regulatory oversight approaches that are adapted to contemporary societal and economic realities. CIPL's previous research has shown that this type of regulation is more effective than deterrence

[20] ICO Annual report 2018-19, available at <https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf>.
[21] DPC 2019 Annual Report, available at <https://www.dataprotection.ie/sites/default/files/uploads/2020-02/DPC%20Annual%20Report%202019.pdf>.
[22] First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities, European Data Protection Board, 26 February 2019, page 7. Available at <https://www.dataprotection.ro/servlet/ViewDocument?id=1633>.

and punishment (which, of course, have an important role to play as well).[23] Responsive regulation also results in the promotion of both effective privacy and the beneficial use of data and innovation.[24]

Responsive regulation is based upon constructive engagement with regulated organizations by providing them information, advice and support. It also means fostering a culture of open dialogue between regulators, regulated organizations and other relevant stakeholders (such as academia and privacy experts) and learning from their experience on processing personal data in a protective and compliant manner. Listening to, and learning from, these stakeholders will equip the ANPD to issue guidance and regulations and to enforce the LGPD in an informed, realistic and effective manner.

In other words:

- A regulatory system is most effective where it is consistent and supports behaviors that are widely seen as fair, proportionate and ethical;
- Organizations should be accountable for demonstrating, with evidence, their commitment to behavior that will attract the trust of regulators, as well as their own management and staff, customers, suppliers, investors and other stakeholders;
- Learning is fundamental and is encouraged by open and constructive engagement between regulators and regulated organizations, but is deterred by emphasis on blame and punishment;
- Regulatory systems need to be based on dialogue and mutual cooperation that are explicitly directed at maximizing compliance, prosperity and innovation; and
- Where organizations break the rules, a proportionate response is needed, with the toughest penalties reserved for deliberate, repeated or willful wrongdoing.

III. CONCLUSION

The importance and urgency of setting up an effective and strong ANPD cannot be overstated. In order for organizations to implement and comply with the requirements of the LGPD effectively, it is essential that the ANPD be established with no further delay and that it start carrying out its responsibilities soon. Given the resourcing and timing challenges it will face in light of the upcoming LGPD effective date, the ANPD should devise a results-based strategy that prioritizes its immediate and short-term duties, in particular providing guidance to organizations and establishing further rules where needed. It should also establish a long-term regulatory oversight approach that is consistent with modern regulatory approaches.

If you have any questions about this paper or require additional information, please contact Giovanna Carloni, gcarloni@huntonAK.com; Matthew Starr, mstarr@huntonAK.com; Markus Heyder, mheyder@huntonAK.com; Laura Schertel Mendes, lsm@laurashertel.com.br; or Danilo Doneda, danilo@doneda.net.

[23] CIPL paper on Regulating for Results: Strategies and Priorities for Leadership and Engagement, available at <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_final_draft_-_regulating_for_results_-_strategies_and_priorities_for_leadership_and_engagement_2_.pdf>.

[24] CIPL Paper on Incentivizing Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability, available at <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf>.

Appendix – Mapping of ANPD Tasks under the LGPD

Note: Unofficial translation of LGPD provisions by CIPL below. These are not literal translations; rather, they incorporate some degree of interpretation.

Article	Primary duties of the ANPD under Art. 55-J	Related tasks outlined in other LGPD provisions
Activities concerning guidelines, recommendation, industry self-regulation		
55-J, I	Ensure the protection of personal data, as provided in legislation	
55-J, II	Ensure commercial and industrial secrecy, as long as there is also compliance with data protection and information security laws, or as long as breach of such secrecy results in noncompliance with the principles listed under Art. 2 of the LGPD	
55-J, VIII	Encourage the adoption of standards for services and goods that enable data subjects' control over their personal data, taking into account the nature of the processing activity as well as the size of controllers and operators	• Encourage the adoption of technical standards that facilitate the data subjects' control over their personal data (Art. 51)
55-J, X	Determine the means by which data processing activities will be informed to the public, with due regards to commercial and industrial secrecy	• Decide on the means by which public entities will make information about their processing activities publicly available (Art. 23, paragraph 1)
55-J, XIII	Issue guidance and procedures concerning privacy and data protection, as well as on data protection impact assessments when data processing may result in high risk to the data protection principles outlined in the LGPD	• Issue technical opinions or recommendations concerning the national security LGPD exception, and require that data protection impact assessments are undertaken in these cases (Art. 4, paragraph 3) • Prohibit or set out rules for the sharing of sensitive personal data for economic advantage purposes, upon consultation with the relevant public entities (Art. 11, paragraph 3) • Issue technical guidance on anonymization techniques and monitor their effectiveness, upon consultation with the Advisory Council (Art. 12, paragraph 3) • Set out rules for access to personal data used for research and studies concerning public health (Art. 13, paragraph 3) • Set out rules concerning the right to data portability (Art. 18, V) and develop interoperability standards for portability, free access to data, data security and record keeping (Art. 40)

Article	Primary duties of the ANPD under Art. 55-J	Related tasks outlined in other LGPD provisions
		• Set out rules concerning the right of access to personal data processed based on consent (Art. 19, paragraph 3) • Decide on new timeframes for specific industry sectors to respond to the right of access (Art. 19, paragraph 4) • Set out minimum standards for data security (Art. 46, paragraph 1) • Develop complementary rules about the role and tasks of data protection officers (Art. 41, paragraph 3) • Set out rules concerning access to personal data processed by the Federal Government in the context of national education (Art. 62) • Set out rules concerning LGPD compliance specifically by databases (Art. 63) • Set out rules concerning how organizations will inform the ANPD about data sharing from public entities to private organizations (Art. 27, sole paragraph) • Set out complementary rules concerning data sharing (Art. 30)
55-J, XVIII	Issue rules, guidance and simplified proceedings for SMEs, start-ups and similar organizations, in particular with regards to deadlines	
55-J, XIX	Ensure that processing of personal data of elderly people is carried out in a form that is simple, clear, accessible and adequate to their understanding, in accordance with the LGPD and the Brazilian Statute of the Elderly	
55-J, XX	Resolve, at the administrative level, any issues concerning interpretation and missing elements of the LGPD as well as its scope	
Strategic activities		
55-J, III	Issue guidelines for the National Policy for Privacy and Data Protection	
Enforcement activities		
55-J, IV	Monitor data processing activities and issue sanctions in case of noncompliance with the LGPD, through an administrative procedure that ensures offenders are able to fully defend themselves and appeal decisions	• Require controllers to present data protection impact assessments when data processing is based on legitimate interests (Art. 10, paragraph 3) • Require controllers and operators to stop processing personal data in cases of noncompliance with the LGPD (Art. 15, IV)

Article	Primary duties of the ANPD under Art. 55-J	Related tasks outlined in other LGPD provisions
		• Receive and manage information about contracts and other agreements concerning transfers of personal data from public to private entities (Art. 26, paragraph 2; and Art. 27) • Manage notifications of data security incidents (Art. 48) • Require controllers to evidence the effectiveness of their privacy compliance programs (Art. 50, paragraph 2, II) • Require controllers to undertake data protection impact assessments (Art. 38) • Assess data security incidents notified to the ANPD, and determine mitigation measures to be adopted by controllers (Art. 48, paragraph 2) • Establish an administrative procedure for enforcement, including on how to calculate fines (Art. 52, paragraphs 1 and 4, Art. 53)
55-J, V	Receive pleadings from data subjects against controllers, where data subjects evidence that their complaint has not been resolved within the timeframe set out by regulation	
55-J, XI	Request at any time, from public entities that process personal data, that they provide a specific report outlining the scope and details of their processing activities, as well as the nature of personal data processed; and issue complementary technical guidance to support their compliance with the LGPD	• Request information from public entities about their processing activities, and issue technical recommendations (Art. 29) • Determine mitigation activities in cases where public bodies are not complying with the LGPD (Art. 31) • Require public bodies to make their data protection impact assessments available to the public, and propose the adoption standards and good practice concerning data processing by public entities (Art. 32)
55-J, XVI	Carry out audits on data processing activities of controllers and operators, including public entities, or request that such audits are undertaken	• Audit controllers who deny providing information about automated decisions data due to commercial secrecy (Art. 20, paragraph 2)
55-J, XVII	At any time, settle agreements with controllers and operators in order to resolve irregularities or legal uncertainties in administrative proceedings, in accordance with Legal Decree 4.657/1942	
Educational activities		
55-J, VI	Raise awareness of data protection laws and regulations to society	

Article	Primary duties of the ANPD under Art. 55-J	Related tasks outlined in other LGPD provisions
55-J, VII	Encourage and undertake studies concerning national and international privacy and data protection activities	
Activities relating to national and international coordination and cooperation		
55-J, IX	Promote cooperation initiatives with data protection authorities of other countries, of international or transnational nature	
55-J, XIV	Engage with controllers and operators as well as with society in relevant matters, and be accountable in what concerns the ANPD activities and planning	• Undertake public consultations on any regulations and standards developed (Art. 55-J, paragraph 2)
55-J, XXI	Report any criminal offenses to the competent authorities	
55-J, XXII	Report noncompliance with the LGPD by public entities to the competent authorities within the public administration	
55-J, XXIII	Coordinate activities with other relevant regulators, where these activities fall under their scope and competence	• Coordinate activities with other regulators, including through maintaining a permanent communications forum with them (Art. 55-J, paragraphs 3 and 4).
Administrative activities		
55-J, XII	Draft annual reports about the ANPD activities	
55-J, XXIV	Adopt simplified mechanisms, including by electronic means, to receive complaints concerning noncompliance with the LGPD	
55-J, XV	Manage its budget and include the breakdown of its revenues and expenses on the ANPD annual report	

Additional ANPD Activities relating to international transfers of personal data

- Authorize international transfers of personal data submitted to the ANPD approval (Art. 33, V and Art. 35, paragraph 2)
- Assess the adequacy level of third countries and international bodies (Art. 33, I and Art. 34), including when required by public bodies or controllers (Art. 33, sole paragraph).

- Determine the content of standard contractual clauses and specific clauses for international transfers of personal data, as well as BCRs, seals, certifications and codes of conduct (Art. 35)
- Designate bodies responsible for certifications in the context of international data transfers (Art. 35, paragraph 3), and review their activities (Art. 35, paragraph 4)
- Manage notifications concerning changes to mechanisms to safeguard international data transfers (Art. 36)