Privacy Series

15 THE REGULATION OF PERSONAL DATA PROTECTION IN BRAZIL

VEIRANO ADVOGADOS

This is the fifteenth chapter of the Data Privacy Series. Click here to access the chapter 14.

In 2023, the Brazilian General Data Protection Law (Law No. 13,709 of 2018 or "LGPD") celebrates 5 years of its publication - now also including the possibility of the application of administrative sanctions by the ANPD since August 2021. The Brazilian National Data Protection Authority ("ANPD") has been active in fostering discussions and disseminating concepts, practices and principles of privacy and data protection, through the publication of several materials for awareness and regulation of the LGPD since its creation.

Veirano Advogados has been following and participating in discussions regarding these issues. For this reason, our Data Protection & Privacy team has prepared the Privacy Series, in which we will periodically publish on different topics related to privacy, bringing not only LGPD concepts, but also ANPD publications on the subject, relevant considerations, among other contents.

As mentioned in previous episodes of this series, the LGPD sets forth well-defined principles and guidelines governing the collection, processing, and sharing/transferring of personal data. It encompasses not only the rights of data subjects but also the responsibilities of Data Processing Agents, the role of the Data Processing Officer, parameters for information security, criteria for International Data Transfers, and directives concerning the functions of the National Data Protection Authority, among other crucial aspects.

Since the LGPD came into force, various sector-specific initiatives have been proposed by both governmental and private entities. These initiatives aim to harmonize different sectors with the legislation and propose specific regulations tailored to ensure the protection of personal data within various economic domains.

At the federal level, one notable initiative is the "Good Practices Guideline on LGPD", published by the Federal Government in August 2020. Alongside the documents and publications set forth by the ANPD (e.g., Guidelines, Manuals, Booklets) and the Regulatory Impact Assessments (RIAs) and Public Consultations, in the last few years Ordinances, Statements, Resolutions, and Technical Notes have also been issued and published aimed at regulating the protection of personal data at the national level.

In response to the evolving landscape of data protection, ANPD took significant steps in 2023. It released a report on the monitoring and execution of the Regulatory Agenda for the years 2021 and 2022. Furthermore, it published the Regulatory Agenda for the 2023-2024 biennium and approved, trough Resolution CD/ANPD No. 5 of 2023, the Regulatory Result Evaluation Agenda for the period 2023-2026. These actions have substantially improved the transparency, visibility, and efficiency in regulatory measures, facilitating society participation and bringing further legal certainty to the relationship with regulated agents.

The Scope of the Topic Within Economic Sectors

To align the operations of diverse industries with the principles and obligations outlined in the LGPD and to cultivate a culture of privacy and information security regulatory authorities in different economic sectors, leveraging their legal competencies and those delegated to the ANPD, have been actively issuing regulations and guidelines. These directives are designed to ensure the safeguarding of personal data through sector-specific procedures for data processing.

Additionally, it's worth highlighting governmental initiative to encourage the establishment of advisory councils comprising sector experts, civil society organizations, and government representatives. These entities play a pivotal role in formulating sectoral guidelines tailored to the unique characteristics of each industry. This approach fosters a clearer comprehension of legal obligations and the adoption of best compliance practices.

Furthermore, within the public and private sectors, a range of good practices have been implemented, including: (i) promoting education and training initiatives trough workshops and training sessions across various sectors that aim to streamline compliance with personal data protection regulations and cultivate a culture that adheres to best practices; (ii) the release of guidelines/manuals for economic sectors, among others tailored to specific economic sectors, among other valuable resources.

Considerations on Sectoral Regulations on Personal Data Protection and Their Relevance

Telecommunications Sector

The telecommunications sector is governed by a comprehensive legal and regulatory framework that aimed safeguard personal data and upholding the privacy right of telecommunications service users.

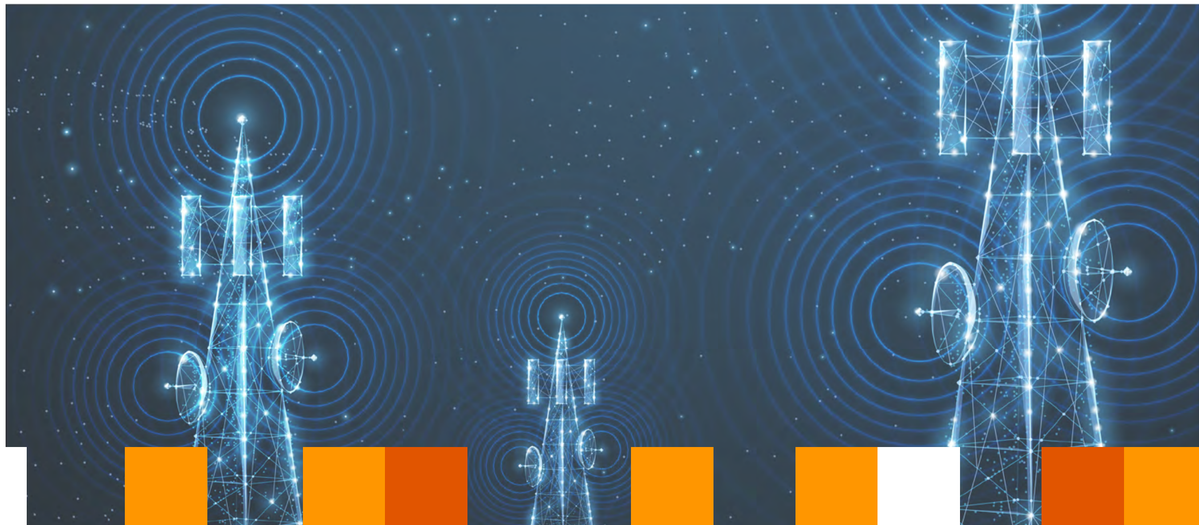
In this context, two legal norms stand out: the General Telecommunications Law (Law No. 9,472 of 1997, known as "LGT") and the Internet Civil Rights Framework (Law No. 12,965 of 2014, known as the "MCI"). These laws play a key role by establishing fundamental principles and guidelines governing the processing of personal information by entities operating within the telecommunications sector.

In particular, the LGT defines (i) user rights, encompassing data privacy and communication confidentiality; (ii) the responsibilities and entitlements of service providers; and (iii) the guidelines governing the proper processing of this data by the entities involved.

The Brazilian Civil Rights Framework for the Internet defines the principles and rights of Internet use in the country, including the guarantee of privacy and the protection of personal data, with certain exception, such as requests for disclosure by a competent authority or by court order.

Furthermore, the telecommunications sector is also regulated by specific resolutions, such as the General Regulation for Consumer Rights in Telecommunications Services ("RGC"), approved by Resolution No. 632 of 2014 of the National Telecommunications Agency ("ANATEL"), and currently under review by the Agency. The RGC comprehensively addresses various aspects of consumer rights, including data protection and privacy. It sets forth clear rules governing the collection, storage, and processing of personal data, mandating that companies implement transparent and secure practices.

The Telecommunications Services Regulation (approved by ANATEL's Resolution No. 738 of 2020) is another crucial component of the regulatory framework of this sector, as it aligns with the LGPD and mandates that telecommunications companies retain the smallest possible amount of user data, keeping its confidentiality in a controlled and secure environment, taking into account the necessary technological resources for maintaining the confidentiality



and deleting the data as soon as the purpose of its processing is achieved or when the legally or regulatory mandated retention period has expired.

Furthermore, the Regulation comprehensively addresses the retention of personal data for the purpose of fulfilling legal and regulatory obligations by telecommunications service providers, providing greater legal certainty to the processing carried out by these entities.

More recently, as the telecommunications landscape has evolved from fixed services to mobile services, regulations have adapted in response to shifts in user behavior, technological advancements, and the emergence of new service models. This transformation has heightened the significance of data and magnified the impacts of its processing.

Consequently, it became clear that these regulatory norms should function in harmony, serving as crucial safeguards for both innovation and the rights of individuals who owns personal data and fostering transparency, security, and trust within the digital environment.

In line with the mentioned above, in a recent audit conducted by the Federal Court of Accounts (Tribunal de Contas da União, also known as "TCU"), as a result of Decision No. 1384 of 2022-TCU-Plenário, which approved the audit process carried out in 382 federal public organizations to assess their adherence to the guidelines established by the General Data Protection Law, according to the Report, ANATEL obtained a score of 0.76 on the LGPD compliance indicator that corresponds to an "intermediate" level of compliance.

Supplementary Health Sector

The supplementary healthcare sector is particularly sensitive when it comes to the protection of personal data, primarily due to its potential impact on individuals' privacy and personal intimacy. This heightened sensitivity is largely attributable to the substantial volume of sensitive information and data, such as medical records, treatment histories, clinical test results, and health conditions, which are collected, processed, and retained by healthcare institutions and professionals within the sector, including clinics, hospitals, and pharmaceutical companies.

Moreover, the processing of data within the healthcare sector is inherently intertwined with the advantages offered by its services and products. In other words, within the context of healthcare services and product offerings, the proper collection and processing of this data is essential for customizing treatments, preventing, and combating diseases, and ensuring the efficacy of medical care. Additionally, they play a crucial role in the development of new drugs and therapies.

In attention to the significance of this sensitive data and the necessity for stringent protection, the LGPD establishes critical guidelines for the collection, use, and processing of sensitive personal data. This category encompasses information, including genetic data and data related to health and sexual life, whose misuse or exposure can have profound implications to the privacy and dignity of the data subjects.

Regarding this topic, in 2022, Law No. 14.510, of 2022, was enacted, authorizing and regulating the practice of telehealth throughout the country and the Federal Council of Medicine (*Conselho Federal de Medicina*, also known as "CFM") published Resolution No. 2,314 of 2022, which defines and regulates telemedicine for the purposes of healthcare, education, research, disease and injury prevention, health management, and health promotion.

According to the regulation, the provision of telemedicine services should adhere to the usual normative and ethical standards of in-person care and the provision of care must be preceded by explicit consent. In this consent, the patient or their legal representative should be made aware of the possibility of their personal data being shared, as well as their right to revoke consent, except in situations of medical emergency.

Furthermore, in the telemedicine services provided, patient data and images in the medical record must be preserved, in compliance with the relevant legal regulations and CFM guidelines regarding the storage, processing, integrity, accuracy, confidentiality, privacy, irrefutability, and professional confidentiality of the information.

Another relevant aspect is the interoperability of healthcare systems, which allows for the exchange of information among different entities but requires special care in data protection during this process.

The sensitivity of the topic highlights the need for a careful and ethical approach to the collection, storage, and sharing of medical information to preserve the dignity and rights of individuals while also enabling significant advancements in healthcare services delivery.

Indeed, the private sector has been coordinating self-regulation initiatives, such as the Code of Good Practices - CNSAúde (National Health Confederation), which provides a compilation of guidelines to be followed by healthcare agents. The Code addresses aspects like transparency in data collection, obtaining proper consent from data subjects, adopting robust security measures to prevent data breaches and cyberattacks, as well as guidelines for the secure sharing among healthcare professionals.

Similarly, the booklet prepared by the Brazilian Institute of Consumer Defense (*Instituto Brasileiro de Defesa do Consumidor*, also known as "IDEC") provides an overview of data protection in the context of the healthcare sector and addresses topics such as the right to healthcare, digital transformation, the use of personal data in accessing medicines and healthcare services, and challenges posed by Artificial Intelligence. According to the Institute, data processing policies are still in the process of development in Brazil and worldwide, but there are already specifics concerns in the healthcare sector. The National Supplementary Health Agency (*Agência Nacional de Saúde Suplementar*, also known as "ANS") has been playing a crucial role in regulating and supervising the activities of healthcare entities in the supplementary health sector.

Among the Agency's initiatives, its Personal Data Protection Booklet stands out, playing a fundamental role in regulation the subject. Indeed, the Booklet addresses topics such as the need for transparency in data collection and processing personal data, data subjects' rights, the importance of information security, and the adoption of appropriate technical and organizational measures to prevent unauthorized access, data breaches, and other security incidents, among other matters.

Lastly, since 2022, the ANS's activities have been guided, among other things, by Resolution No. 80 of 2022, which establishes the Personal Data Protection Policy within the scope of the Agency.

Civil Aviation Sector

The processing of personal data plays a crucial role in the development and modernization of the civil aviation sector, as it entails the collection and analysis of personal data from passengers, crew members, and other stakeholders, all of which are indispensable for meeting applicable standards and ensuring a high level of safety, efficiency, and convenience in aviation operations. Airlines and aviation authorities rely on this information, including names, personal histories, and personal data, to conduct background checks, facilitate passenger and crew identification, and ensure compliance with safety and immigration regulations.

Furthermore, the use of personal data enables airlines and aviation authorities to deeper understand the specific necessities of passengers with disabilities to adapt its services and facilities to meet these specific needs in accordance, in the light of accessibility standards.

Additionally, the use of personal data is important to enhance the overall passenger experience. Airlines leverage this data to personalize services, extend special offers aligned with passenger preferences, and optimize operational efficiency, encompassing processes such as boarding and disembarking, seat preferences, and dietary requirements. This not only contributes to a more enjoyable and convenient travel experience for passengers but also enables airlines to streamline their operations and allocate resources more effectively.

However, the significance of using this information in the civil aviation sector also raises pertinent questions regarding privacy and data protection. This is particularly relevant given the substantial volume and continuous flow of personal and sensitive data involved in aviation operations.

Within the scope of the National Civil Aviation Agency ("ANAC"), the groundwork for data protection was laid in 2015 with the publication of the Manual for the Treatment of Restricted Access Information. This comprehensive manual, in its section 3.2, delineated the information categorized as personal and/or sensitive, emphasizing the importance of respecting the privacy and private life of data subjects.

After the enactment of the LGPD, ANAC took significant steps to ensure compliance with data protection legislation. In August 2021, ANAC's Personal Data Protection Policy, ensuring compliance with data protection legislation. Also, the ANAC Privacy Notice was published along with Decree No. 2,235 in August 2020, which designates the DPO within the Agency.

In a recent audit conducted by the Federal Court of Accounts to diagnose the controls implemented by federal public organizations for compliance with the LGPD, it was found that ANAC obtained a score of 0.48 for the LGPD compliance indicator, corresponding to the "initial" level.

However, from the perspective of best practices, it's worth noting that ANAC has a Cybersecurity Incident Prevention, Treatment, and Response Team ("ETIR"), established by Decree No. 9,367/STI. This team is responsible for receiving, analyzing, and responding to notifications related to security incidents, as well as taking proactive measures to reduce the risk and impact of potential information security incidents.

Maritime Transport Sector

The collection and processing of personal data, encompassing information pertaining to passengers and crew members, empower maritime authorities and transportation companies to effectively oversee and enforce safety regulations. These regulations encompass essential measures like background checks and access control to sensitive areas on vessels. Such oversight is instrumental in thwarting potential security threats, such as piracy and illicit activities.

Moreover, personal data utilization is pivotal in enhancing the overall experience of passengers and data subjects. Maritime transportation companies can harness this data, including preferences, travel history, and passenger feedback, to offer personalized services. This personalization extends to aspects like menu offerings, onboard entertainment, and accommodations, rendering them more appealing to customers and heightening their competitiveness in the market.

Additionally, leveraging personal data enables economic actors to identify patterns in demand, consumer behavior, and operational efficiency. This invaluable insight equips them to fine-tune their operations, schedules, and routes with greater precision to meet evolving demands. Consequently, this optimization not only reduces costs but also augments the quality of service provided.

However, given the substantial volume and potential sensitivity inherent in the personal data processed, adherence to personal data protection standards within the maritime sector is imperative. Such compliance serves as a crucial safeguard to ensure the security of information belonging to data subjects, including passengers and crew members, among others.

The National Agency for Waterway Transportation (“ANTAQ”) approved the Personal Data Protection Policy (PPDP) through Decree No. 425 of 2022. The PPDP establishes universally, encompassing all individuals, both directly and indirectly, engaged in activities related to the processing of personal data maintained by the agency. This policy lays out explicit and comprehensive guidelines for the management and safeguarding of personal data within ANTAQ, encompassing vital aspects such as data collection, storage, processing, and the sharing of personal information. It ensures adherence to the provisions outlined in the LGPD within the agency’s operational framework.

Moreover, ANTAQ’s dedication to aligning itself with sectoral norms and guidelines is evident in the TCU Feedback Report. This report, while scrutinizing the agency’s initiatives to adapt its operational and strategic practices to guarantee the security and privacy of the personal data, resulted in a score of 0.60 on the LGPD compliance indicator. This score signifies an intermediate level of compliance with personal data protection standards.

Land Transportation Sector

Particularly within the scope of the land transportation sector, the processing of personal data, carried out by the Public Administration (including the National Land Transportation Agency, also known as "ANTT") and regulated entities, has the primary objective of ensuring adequate infrastructure and the provision of land transportation services to users with transparency and effective regulation, thereby facilitating the continuous improvement of the services offered. To achieve this, personal data related to (i) passengers of road and, where applicable, rail transportation; (ii) individual transporters, such as those listed in the National Registry of Road Freight Transporters; and (iii) service providers or suppliers, are processed.

In view of this, the CNT/SESTSENAT/ITL, in partnership with representatives from various modes of the transportation sector, published the "Good Practices Guide for Data Protection in the Transportation Sector". This guide is designed to establish standardized practices and protocols for the processing of personal data, streamlining and enhancing the efficiency with which transportation companies adhere to the related norms.

In the current context of ANTT, despite the initiatives are still in their early stages, through Deliberation No. 448 of 2020, the Board of Directors established the Commission to Support Personal Data Protection. This commission's objective is to formulate guidelines related to the LGPD and provide support in the development of internal procedures and protocols for actions of processing of personal data and privacy protection.

Furthermore, according to the Agency's Privacy Notice, ANTT is in the process of aligning with legal regulations regarding data protection. This includes the publication of manuals and guides, as well as the establishment of committees dedicated to the topic.

Financial and Payment Methods Sector

Even before the enactment of the General Data Protection, specific regulations had already emphasized the importance of maintaining the confidentiality and secrecy of personal data and information processed and stored by financial institutions and other institutions authorized to operate under the purview of the Central Bank. One noteworthy example is Complementary Law No. 105 of 2001, commonly known as the Bank Secrecy Law, which guarantees the confidentiality of financial data, except when a court order mandates disclosure for the purpose of investigating illegal activities.

This regulatory framework safeguards the privacy of banking activities and enforcing rules to deter illicit practices. Additionally, BACEN Resolution No. 4,658 of 2018, revoked by CMN Resolution No. 4,893 of 2021, addresses cybersecurity policies and establishes requirements for data processing, storage services, and cloud computing contracts that institutions authorized by the Central Bank of Brazil must adhere to.

Within a sector characterized by multifaceted operations involving processes, personnel, software, hardware, internal protocols, and legal guidelines, the architecture of this system must encompass various facets of personal data protection and privacy. These include elements such as access control, traceability, understanding of declared and executed purposes, data anonymization, and more.

It comes as no surprise that the safeguarding of personal data has become an integral component of the sector's efficient functioning. Proper processing of personal data, ensuring information security, and effective information management are all pivotal aspects of financial operations. Given the ongoing digitization of services, cultivating a culture centered on personal data protection has become an increasingly urgent imperative for all stakeholders.

With the entry into force of the LGPD, new guidelines and obligations have been introduced, aiming to protect credit through a regulatory approach with elements of innovation.

Although financial data is not included in the exhaustive list of sensitive personal data outlined in LGPD, as is the case with article 9 of the GDPR, the risks arising from a potential security incident have been recognized in the context of sanctions, thereby introducing new concerns regarding their protection. The correlation between the confidentiality of financial data and the protection of intimacy and privacy justifies the adoption of robust technical measures.

Over the last few years, the sector has experienced significant technological and market-driven evolution, largely facilitated by pro-competitive regulations.

By example, we can mention the regulation of Open Finance (initially referred to as Open Banking), which aims to facilitate data and service sharing through an open and interoperable system, empowering data owners. This is an excellent example of the innovations being introduced in this sector. The topic has been the subject of extensive discussion and was subsequently regulated through Joint Resolution No. 01 of 2020, whose text has been amended by other norms. In this context, Joint Resolution No. 05 of 2022, which introduced significant changes to the regulation in question, defined interoperability as '*the standardized sharing of data, with customer consent, in a secure, agile, and precise manner among participants in the regulated systems*,' with the aim of (i) stimulating innovation; (ii) promoting competition; (iii) increasing the efficiency of the National Financial System and the Brazilian Payments System; and (iv) promoting financial citizenship.

However, data security has been a concern in the implementation of Open Finance, which requires the adoption of effective measures to protect the personal data of data owners, especially considering that system interoperability may lead to a significant increase in data sharing. It is crucial for the success of the initiative that users have trust in the security of their information.

It is also worth mentioning Joint Resolution No. 6 of 2023, which will come into effect on November 1st, 2023, and establishes requirements for data and information sharing related to fraud indicators to be followed by financial institutions, payment institutions, and other institutions authorized to operate by the Central Bank. It's important to highlight the obligation to obtain prior consent from data owners for recording data and information in their systems (except for confidential data and information, as per special

legislation, related to indications of the crimes of money laundering or concealment of assets, rights, and values, and financing of terrorism).

Furthermore, after the entry into force of the LGPD, it is noticeable that the Central Bank ("BACEN") published its Privacy Policy and approved, through Resolution BCB No. 249 of 2022, its Information Governance Policy, applicable to the processing of any information in digital, physical, or communication-derived forms received, collected, and processed by the Central Bank. This policy aims, among other objectives, to protect the information processed by the regulator, ensure the availability and appropriate quality of basic information for the fulfillment of institutional missions, guarantee the proper provision of information to society, especially those of public interest, and facilitate the sharing of information with other government agencies.

Other sectors

We should also highlight the efforts being made by other Regulatory Agencies (e.g., ANA, ANCINE and ANEEL), which, although they have not issued specific rules on the subject, have been launching initiatives to align the sector with personal data protection legislation.

Competition Defense

In face of the growing significance of data across various markets, particularly in the era of the Digital Economy, we witness an expanding convergence between this subject and competition defense. Numerous instances of investigations conducted by competition authorities highlight the central role of data possession by one or a few economic entities, the low replicability of such information, with the potential for abuse being a key factor in these cases.

It is undeniable that LGPD has a competitive aspect in its provisions, establishing free competition as one of its principles. In this regard, the Administrative Council for Economic Defense (CADE) and the National Data Protection Authority (ANPD) signed a Technical Cooperation Agreement in June 2021 to enhance actions aimed at the defense, promotion, and dissemination of competition within the scope of data protection services.

In essence, the agreement's purpose is to establish a framework for technical cooperation between the respective authorities, facilitating collaborative and coordinated efforts in addressing situations within their spheres of competence. This cooperative endeavor is instrumental in combatting activities detrimental to the economic order and in fostering a culture of free competition. To realize these objectives, the agreement delineates shared obligations, such as the exchange of documents, studies, research, information, knowledge, and experiences, as well as the organization of meetings and seminars and the production of studies.

Furthermore, it outlines specific obligations for each entity involved. For CADE, this includes the requirement to notify ANPD when initiating investigations against economic agents operating in sectors regulated by ANPD. Conversely, ANPD is obligated to inform CADE when initiating investigations that may potentially constitute a violation of the economic order.

At the same time, CADE released the report titled "International Benchmarking on Competition and Data Protection Authorities", which includes an analysis of competition and data protection authorities in twelve jurisdictions, in addition to Brazil.

Challenges

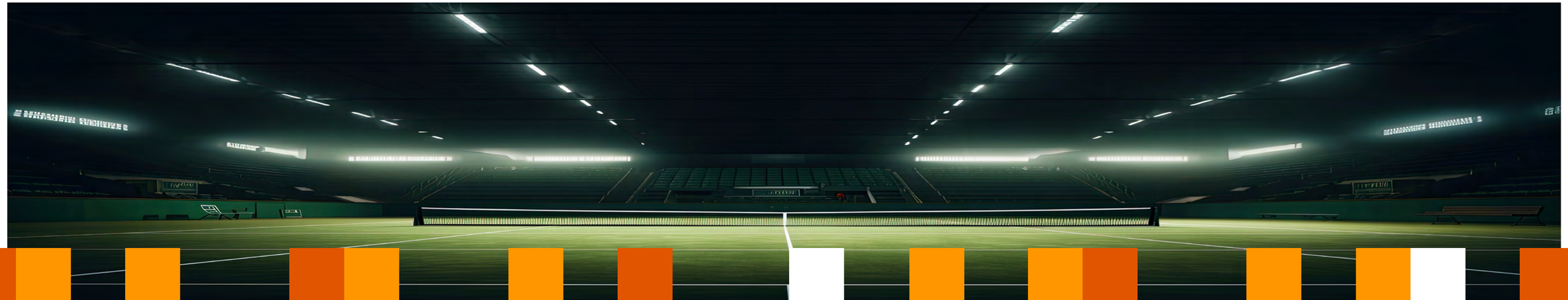
The emergence of specific data protection regulations tailored to various economic sectors, although partly necessary due to the unique characteristics of each one, has yielded a complex patchwork of rules and guidelines, presenting substantial challenges in terms of harmonization and systematic interpretation.

The challenges of harmonization and coordination lie mainly in the regulatory specificities of each sector, since each one has unique characteristics (e.g., diversity of interests, technologies, and practices) in relation to the importance and volume of personal data that is collected and processed, within their respective operational dynamics.

In addition, in a society where technological evolution is occurring rapidly and data, especially in digital markets, can reveal how individuals think, decide and consume, configuring real assets and establishing new dynamics in social relations, the need for periodic monitoring by regulatory agents, responsible for regulating new technologies and reviewing current rules, arises, adding an additional layer to the complexity of harmonizing rules on the protection of personal data.

There are also legislative initiatives underway, both directly and indirectly aimed at enhancing personal data protection regulations, as well as regulating the use of artificial intelligence within the country. This underscores the critical importance of collaborative and concerted efforts between the legislative branch, regulatory bodies, and entities subject to regulation in effectively addressing these evolving challenges.

However, despite the challenges mentioned above, it is still crucial for regulators to strike a balance between the specificity required to each sector and the imperative need for consistency and clarity in data protection rules, which are essential for the country's economic development. Indeed, for groups operating in multiple sectors, for example, ensuring



compliance with a complex array of regulations can become a daunting and costly endeavor, ultimately impeding the implementation of coherent and efficient data protection practices throughout their operations.

On the other hand, the convergence of these norms brings forth a multitude of benefits.

- **Firstly**, it not only reduces the administrative burden and mitigates the risk of contradictions and regulatory gaps but also empowers regulated entities to operate in greater compliance with the legal and regulatory framework for the protection of personal data. Consequently, economic agents can develop internal systems and processes that more closely adhere to regulations that align more directly with the regulations, ensuring a more solid and comprehensive approach and minimizing operational impacts.
- **Secondly**, the legal certainty arising from the harmonization of sectoral norms tends to foster heightened trust among the market chain actors. This occurs because, when they perceive that their information and personal data are being handled appropriately, regardless of the sector of activity, they may be more inclined to allow the sharing of their personal data. Furthermore, by adhering to data protection regulations in all sectors in which they operate, regulated entities demonstrate their commitment to safeguarding the privacy and integrity of personal data. This, in turn, strengthens trust between them and third parties, and it cultivates a culture of respect for privacy.
- **Thirdly**, the alignment of sectoral norms also fosters increased transparency, mitigating concerns related to information security. In other words, this means that the effectiveness of personal data protection regulations is enhanced when stakeholders can implement comprehensive preventive measures.
- **Fourthly**, the harmonization provides advantages for interdisciplinary collaboration. Often, different economic actors from various sectors need to exchange personal data for the development and execution of business models. In this scenario, the use of norms that allow a systematic interpretation would facilitate the proper processing and sharing of this data.
- **Ultimately**, with greater alignment among regulatory norms, both the government and the private sector find it more feasible to craft more robust and comprehensive security strategies, thereby mitigating potential vulnerabilities across all areas.

Notwithstanding the regulatory progress on the subject, coordinated efforts between regulatory agencies, the legislative branch, and the private sector through collaborative mechanisms for social participation (e.g., public hearings, Regulatory Impact Analysis, Public Consultation, among others) are indispensable. These efforts are essential for minimizing regulatory gaps and interpretive discrepancies, ensure greater adherence to legal and regulatory compliance, reduce asymmetries and fostering a more unified approach to the personal data protection in the country.

VEIRANO ADVOGADOS

The Veirano Experience has a holistic, multidisciplinary, and business-oriented approach. In order to cover all the needs related to Compliance with LGPD, our Data Protection & Privacy team have developed several project formats, which comprise different scopes of work and meet specific demands of each client, whether national or international:

1. Full Compliance

With the performance of a multidisciplinary team, this project is aimed for clients whose goal is to identify and assess all ongoing processing activities within the company and based on that, identify vulnerabilities and structure an action plan for the creation of an effective privacy and data protection program based on legal, procedural, information security, and corporate governance pillars.

2. DPO as a Service

In this model, we take on the role of Data Protection Officer (DPO) on behalf of the client. To this end, we allocate a professional to perform the activities of managing and monitoring the client's data protection and privacy program.

3. M&A Legal Assistance

Designed to assist clients in the legal due diligence of merger and acquisition transactions, in order to identify relevant legal issues (red flags) and mitigate potential risks related to data protection and personal data security issues of the target company.

4. LGPD Pocket

A “pocket” advisory service for the adequacy of the activities and/or products developed by the company, regardless of its size or field of business, considering a reduced number of deliverables.

5. LGPD on Demand

LGPD On Demand is aimed at organizations that wish to have multidisciplinary advisory service on legal, information security, and corporate governance issues, with specific and timely action related to the protection of personal data.

6. LGPD Legal Helpdesk

The Helpdesk is designed to assist clients with LGPD legal consultations and demands within a monthly package of hours, either before, during, or after the initial compliance process.

7. Task Force For Security Incident Assessment And Reporting (VA Cybersecurity)

Specific and multidisciplinary legal advice in aspects related to the suspicion or occurrence of a security incident, in accordance with the most updated instructions from the ANPD and other applicable laws and regulations.

8. Representation in Administrative and Judicial Actions Involving Data Protection

Representation of clients in any administrative and/or judicial actions or potential actions involving data protection.

9. Analysis of Administrative and Judicial Decisions on Data Protection Matters

Periodic monitoring of decisions rendered in judicial and administrative proceedings involving the company or not, in order to present the authorities’ understanding and the impacts for the company or economic sector to the client in a summarized format.

10. Development and Updating of a Data Protection Impact Report

The ANPD may request from the controller to prepare a personal data protection impact report ("RIPD" or DPIA). Our team has expertise on the subject and can assist the company with the preparation and updating of the RIPD.

11. Development of Workshops

Development and application of training about the main concepts related to privacy and data protection to train its employees.

12. Playbook for Negotiating Commercial Contracts

Creation of playbooks for the negotiation of commercial contracts, to facilitate and speed up internal processes of commercial, technical, and legal teams.

13. Handbook to Reply the Data Subjetcs

Development of materials to assist the companies in prompt answering the data subjects' requests, as well as in the procedure to be followed by the company when answering the data subject, according to the business model developed by the company.

14. International Data Transfer

We help clients to understand the context of the international transfer, adapt it to the applicable legal basis, assess data localization requirements, add contracts, draft and review intra-group data sharing agreements, and generally respond to queries related to the harmonization of foreign with Brazilian regulations.

15. Privacy and Data Protection Auditing

We conduct audits to evaluate the company's level of maturity, presenting recommendations for risk mitigation.

16. Development and Review of Documents Pursuant to the Financial Sector

Our team has expertise in drafting security policies in accordance with the Central Bank's specific information security regulations, and in answering questions on the subject.

17. DEVELOPMENT OF AI USAGE POLICY

The rapid evolution of AI has brought numerous opportunities but also challenges related to ethics, privacy, and compliance. Therefore, it is essential for the success of companies to have a robust policy for the use of AI systems and applications that ensures responsible and effective use in their business.

We are at your disposal in case of any questions or in the need of any additional information.

ANA CLAUDIA BEPPU
+55 11 2313-5782
ana.beppu@veirano.com.br

ENRICO ROMANIELO
+55 11 2313 5843
enrico.romanielo@veirano.com.br

FÁBIO PEREIRA
+55 11 2313 5906
fabio.pereira@veirano.com.br

GABRIELA ANDRADE GUIMARAES DE OLIVEIRA
+55 21 3824 4637
gabriela.guimaraes@veirano.com.br

PAOLA LORENZETTI
+55 11 99976 8480
paola.lorenzetti@veirano.com.br

This material was last updated on September 21, 2023 and published on September 22, 2023 .
For more updated information please contact us.