VLK ADV

WWW.VLKLAW.COM.BR

THE FUTURE OF PRIVACY:

How to be prepared for

2025

- Contextualization and relevance of the theme
- AI and Data Protection
- Resolution and Guide for the ANPD Officer
- International Transfer of Personal Data
- Cybersecurity and Incident Response

TABLE OF CONTENTS

ABOUT US 4

SUMMARY 5

1. **CONTEXTUALIZATION AND RELEVANCE OF THE TOPIC** 7

2. **AI AND DATA PROTECTION** 8

2.1. How to identify and detail purposes and legal bases in the context of AI?

2.2. Purpose of the processing activity

2.3. Legal basis – general aspects

2.4. What is the most appropriate legal basis for AI development?

2.5.What precautions are important to base the development of AI on legitimate interest?

2.6. What is the difference between the Data Protection Impact Assessment (DPIA) and the Algorithmic Impact Assessment (AIA)?

2.7. When to do it?

2.8. Is it possible to reuse the RIPD for the AIA? How?

3. **RESOLUTION AND GUIDE FOR THE PERSON IN CHARGE OF THE ANPD** (Nº 18/2024) 18

3.1. Appointment of the Officer in Charge and the Substitute Officer

3.2. What is a conflict of interest and what is its importance for the Person in Charge?

3.3. Is it possible to appoint a Global DPO or LATAM DPO to function as a DPO in Brazil?

3.4. What are the main measures to be adopted by the controller in relation to the Officer?

3.5. Is it possible to hold the Person in Charge liable?

4. **INTERNATIONAL TRANSFER OF PERSONAL DATA** (TID) 24

4.1. What is international transfer and what are the TID Mechanisms?

4.2. Is there a deadline for the application of Resolution No. 19/2024?

4.3. What are the most appropriate transfer mechanisms? How is it different from the legal basis?

4.4. In addition to the international data transfer mechanism, is it necessary to indicate a stand-alone legal basis for the international transfer?

4.5. What should I do if I already adopt Standard Contractual Clauses from another country or international organization?

4.6. What is the best mechanism for international data transfer to the US and the European Union?

4.7. What is the means made available by the ANPD to carry out the requirements provided for in Resolution No. 19/2024?

5. **CYBERSECURITY AND INCIDENT RESPONSE** 30

5.1. What security measures should be adopted?

5.2. What should I adjust in my Incident Response Plan?

5.3. When may I have to pay the holder compensation?

5.4. How to mitigate sanctions resulting from an Incident?

Direito,
Inovação
& Tecnologia

ABOUT US

Vainzof, Lima e Karassawa Advogados (VLK) sees the law as a tool to drive innovation, business success, and a more prosperous and just society.

We actively participate in the construction of regulatory frameworks and hundreds of innovative projects, which allows us to anticipate trends and generate legal security to make business viable in the following practice areas:

- Ethical Governance and Data Protection;
- Artificial Intelligence;
- Cybersecurity and Incident Response;
- Creative Economy, Legal Marketing and Intellectual Property;
- Legal Design and Visual Law;
- Advocacy and Strategic Technology Regulation;
- Strategic Litigation.

SUMMARY

Celebrated on January 28, **International Privacy Day** reinforces the relevance of personal data protection in a global scenario shaped by emerging technologies, in which the constant flow of information challenges companies and organizations to maintain high standards of governance.

To mark this date, VLK Advogados has prepared a strategic guide outlining essential measures for data management in compliance with the latest legal and ethical requirements. The material covers detailed guidance on governance measures for the development and application of artificial intelligence systems in an ethical and transparent manner, the role and responsibilities of the Data Protection Officer (DPO), requirements to ensure legality in the international transfer of personal data, and advanced strategies for cybersecurity. This booklet aims not only to strengthen the rights of data subjects, but also to align corporate practices with the growing demand for trust, legal certainty, accountability, and responsible innovation in an increasingly dynamic and constantly evolving digital environment.

1. CONTEXTUALIZATION AND RELEVANCE OF THE TOPIC

Personal data has already surpassed the analogy of "new oil" and has established itself as the backbone of public policies and one of the main drivers of modern markets and economies. They are essential resources for building economic and social strategies that guide decision-making in different sectors. Its influence permeates everything from fraud prevention and credit protection, to targeted marketing, digital commerce, predictive medicine, and the development of AI.

Not by chance, the General Law for the Protection of Personal Data (LGPD) also provides as a foundation for the protection of personal data economic and technological development and innovation, bringing greater legal certainty and a guide for companies on how to use data ethically, safely and responsively. Now, the LGPD is already in a new phase, with its regulation and inspection by the National Data Protection Authority (ANPD).

The ANPD's agenda shows a strong tendency to demand greater transparency in cases of incidents, good cybersecurity practices and level of governance and accountability documents compatible with legislation that has existed for more than 6 years and has been in force for more than 4 years, including the updated record of personal data processing activities, storage of logs, adequate mechanisms for international transfer, assessment of legitimate interest and preparation of impact report, when applicable, in addition to an empowered Person in Charge with technical autonomy in the organizations.

Thus, in this #PrivacyDay we present four main Privacy Governance trends in 2025, considering the most recent and main regulatory changes that affect the protection of personal data in Brazil and worldwide.

2. AI AND DATA PROTECTION

The use of AI systems, whether specialized or general-purpose, has become essential for business competitiveness. However, the development and application of these systems often involve the processing of personal data, requiring compliance, among others, with data protection legislation.

Given the relevance of AI to society and its potential impacts on data subjects, data protection authorities have intensified efforts to ensure compliance with the rules already applicable. In Brazil, the ANPD has given special attention to the topic, with actions such as:

- Public Consultation on AI and Data Protection, aiming at the creation of future regulations on the subject;
- Adoption of inspection measures in AI-related projects, such as the case of AI training by Meta and X and the Safe Stadium Project;
- Statements on the intersection between the AI Bill (2,338/23), the LGPD, and the ANPD's functions;
- Technological Radar about Generative AI; and
- Regulatory sandbox for AI.

In this context, we will present our understanding of relevant issues to be considered at the intersection between AI and Data Protection.

2.1 How to identify and detail purposes and legal bases in the context of AI?

When talking about AI and data protection, it is essential to understand that Artificial Intelligence (AI) has its Life Cycle structured in several phases, in which personal data is processed and, consequently, requires the clear identification of the purposes for the processing and the justification on a legal basis.

In general, the life cycle of artificial intelligence can be divided into **four main stages:** (1) design; (2) data acquisition and preparation; (3) training, testing, and validation; and, finally, (4) implementation, application and monitoring [1]. It is common for the processing of personal data to occur in the last three stages. For the purposes of this topic, the data acquisition and preparation phases (2), as well as training, testing, and validation (3), can be grouped into a single step called "**development**".

2.2 Purpose of the processing activity

When selecting the **purpose of the[1] processing activity** , it is important to take into account, in addition to the stage of the AI life cycle, what is the context related to the AI we are processing. In general terms, we can speak of **three distinct contexts**[2][2]:

Development or application of Expert Systems:

Specialists are the AI systems developed for specific operational uses. In these hypotheses, the purpose (whether in its development or in its application) usually corresponds to the operational objective of the AI. Thus, if the objective is to develop AI to perform collections, for example, this tends to be the purpose pointed out throughout the AI life cycle.

Scientific Research related to AI:

In the context of artificial intelligence, it is common to conduct scientific research for objectives that include developing or evaluating the capacity of models and identifying useful patterns in databases, which may be applied in the future in AI-based solutions. In these situations, it may not be feasible to establish a specific purpose at the beginning of the processing, since the effective use of the data

[1] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/ai-and-data-protection-risk-toolkit/
[2] https://www.cnil.fr/en/defining-purpose

will depend on the results obtained during the research and development process. For example, a bank can analyze transactional data to identify useful patterns in that data (e.g., fraud, delinquency, etc.). Only after concretely discovering the standards is it possible to define the specific purpose for which the data will be used.

In these cases, it is permissible to define purposes, but generic (e.g., discovery of useful patterns in data, improvement of products and services, etc.), which should be more detailed and concretized, as the result allows.

Development or application of General Purpose AI Systems:

As the name suggests, general-purpose AI is one that is able to efficiently perform several different tasks, consequently, there is no clear and pre-established purpose for the solution from the design phase.

In these cases, at the development stage, the purpose of training (or developing) the general-purpose solution may, in itself, be a legitimate purpose[3][3].

Considering the application of General Purpose AI, it is possible to come across two distinct situations: the adaptation of a general purpose AI model for a specific purpose (e.g. by finetuning) or its availability to the target audience, as general purpose AI.

In the first case, the rules for AI Expert Systems apply. In the second case, we understand that the principle of finality should be seen in a more flexible way, being encompassed not by a specific and concretely determined purpose, but by the set of permitted and prohibited uses, under the terms of any acceptable use policy.

2.3 Legal basis – general aspects

Equally, when determining the **legal basis**, the purpose and stage of the AI life cycle must be considered. Some legal bases may be more prone and appropriate for AI training and/or deployment than others. For example [4][4]:

- Facial recognition system can be trained to recognize faces, but this functionality can be used for multiple purposes, such as: crime prevention, authentication, and tagging friends on a social network. Each of these additional applications may require a different legal basis;

- You implement a third-party AI system, any processing of personal data carried out by the developer will have been for a different purpose (e.g. to develop the system) than that for which you intend to use the system, so you may need to identify a different legal basis;

- The use of the legal basis of "performance of contract" is limited to those cases in which the processing is strictly necessary to, concretely, enter into or perform a contract with the data subject. Thus, although an AI solution can be used to, for example, perform a contracted activity based on this legal basis, the use of the holder's data to train this system, as a rule, cannot be based on this basis.

Thus, while in the application stage, the most distinct legal bases are applicable, according to the specific purpose of AI, the legal bases applicable to the AI development stage, especially those of general purpose, will be, mainly, the following:

- Legitimate Interest;
- Consent; and
- Conducting Research, for processing agents that qualify as research bodies.

It is also possible that other legal bases may be applicable in the development of AI solutions with a specific purpose, especially:

- Fraud prevention, for the development of biometric identification solutions; and

- Credit Protection, for the development of solutions that assess credit risk.

2.4 What is the most appropriate legal basis for AI development?

The requirement of consent in the context of AI development faces challenges such as lack of scalability, overload on individuals, and negative impact on third parties, and it is more appropriate to explore legal bases such as legitimate interest to meet the complexity of the digital environment and protect the rights of data subjects. These challenges include[1][5]:

- **Constant revalidation of consent:** changes or expansions in the purpose of

[3] https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_applying_data_protection_principles_genai_dec24.pdf

[4] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-lawfulness-in-ai/#contract

[1] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-lawfulness-in-ai/#consent e https://www.sciencedirect.com/science/article/pii/S026736492200108X

the processing require new collection of consent, making the process onerous and repetitive.

- **Lack of purpose at the beginning of the project:** research projects often do not have a specific purpose at the beginning, which prevents the validation of consent.

- **Ensuring adequate information and granularity:** it is challenging to provide clear, detailed, and understandable explanations in complex technical contexts.

- **Possibility of revocation of consent:** the deletion of data, especially in unstructured databases, can be technically difficult and compromise the effectiveness of the system, particularly in situations of high demand for deletions.

Thus, legitimate interest is more appropriate, as long as its classification requirements are met – that is, the activity passes the balancing test.

2.5 What precautions are important to base the development of AI on legitimate interest?

As with any data processing activity, the framing of legitimate interest in the context of AI development requires the performance of the Balancing Test. In this Test, the data processing must meet the following criteria:

- **Absence of sensitive personal data:** the processing must not involve categories of sensitive personal data.

- **Basis on a legitimate interest:** the interest must be legitimate, which may be that of the processing agent, a third party or the company.

- **Reasonable necessity:** the processing must be indispensable to achieve the legitimate interest(s) pursued.

- **Reasonableness of legitimate interests:** the legitimate interest pursued cannot be outweighed by the negative impacts on the rights and interests of data subjects.

Although the measures to meet this test depend on the specific case, some practices can significantly increase the chances of qualifying for legitimate interest:

- **Data filtering:** when mining information from the internet or using open-source databases, it is common for sensitive personal data to be collected, even if unintentionally. To mitigate these risks, it is recommended to carry out two-step filtering [1[6]]:

  1. Before collection:

  define precise criteria that reduce the likelihood of capturing sensitive personal data;

  2. After collection, but before AI training:

  Adopt processes to anonymize or delete sensitive data collected, whenever possible, and document these steps in detail.

- **Definition of hypotheses:** to ensure that the data processed are reasonably necessary for the desired purposes, it is recommended to justify, through well-founded hypotheses, the logic of linking the data used and the intended purpose;

- **Data minimization:** whenever possible and without compromising system performance, prioritize anonymization or, at the very least, pseudonymization of training data. This practice reduces potential impacts on data subjects; and
- **Opt-out made easy:** guaranteeing holders the possibility of choice is essential to preserve their autonomy and align with their expectations. Thus, it is essential to offer a clear and accessible mechanism for the exercise of the Right to Object, preferably highlighted in the default settings of the privacy portal or other solution adopted by the organization to manage requests from data subjects.
- **Transparency:** for the basis of the activity on legitimate interest, it is important to provide appropriate information to the data subjects about the purposes and data processed. In the case of General Purpose AI development, it is recommended to provide information on the expected capabilities of the model.

2.6 What is the difference between the Data Protection Impact Assessment (DPIA) and the Algorithmic Impact

[2] https://www.edpb.europa.eu/system/files/2024-
[3] https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-cautelar-do-tratamento-de-dados-pessoais-para-treinamento-da-ia-da-meta

SEI_0130047_Voto_11.pdf

Assessment (AIA)?

The Algorithmic Impact Assessment (EIA) and the Personal Data Protection Impact Report (RIPD) are different risk analysis instruments, although they have similarities. The RIPD, provided for in the LGPD, is mandatory in situations of processing of personal data that may generate risks to civil liberties and fundamental rights, according to arts. 5, XVII and 38 of the Law. It focuses exclusively on the impacts of the processing of personal data on individuals, addressing processed data, methodologies used and mitigation measures to protect fundamental rights, always observing commercial and industrial secrets.

The EIA, on the other hand, although not yet a legal obligation at this time, being provided for in Bill No. 2338/21, is more comprehensive, going beyond the risks related to the processing of personal data, but also seeks to assess the impacts on fundamental rights. It considers the entire operation of AI systems, including programming, the unpredictability of the algorithm, and possible negative externalities in any context of the technology's performance. In addition to legal aspects, the EIA addresses ethical reflections, intentional and unintended impacts, and mitigation strategies. However, due to the absence of specific regulation, the EIA lacks a universal standard for its implementation, resulting in discretion and lack of clear guidance on its methodology.

2.7 When to do it?

The RIPD is defined in article 5, XVII of the LGPD as the "documentation of the controller that contains the description of the personal data processing processes that may generate risks to civil liberties and fundamental rights, as well as measures, safeguards and risk mitigation mechanisms".

Thus, considering that, by the very nature of technology, the processing of personal data by AI involves automated data processing, the DPPI will be necessary whenever the processing activity operates on a large scale or may generate significant damage to the rights and interests of the data subject.

The EIA (considering the approval of PL 2338/21 as it stands at this moment) must be carried out prior to the introduction or placement in circulation on the market of

an AI system, whenever the developer or applicator introduces or puts an AI system into circulation on the market, when the system or its use is of high risk, considering the role and participation of the actor in the chain – that is, when the intended use of AI, by itself, can significantly impact the fundamental rights and interests of the people affected.

According to the ANPD itself , although the scope of processing of a DPIPR is restricted to contexts involving the processing of personal data and its analysis is limited to the management of risks to fundamental freedoms and rights affected by this processing, there is no doubt that there is a correlation between the two tools, both in the methodological aspect of their elaboration, and content (for cases where AI systems process personal data). In fact, the Laboratory of Public Policies and the Internet (LAPIN) comments that, as EIA is used to manage risks of AI systems to fundamental rights, inevitably, the rights to privacy and protection of personal data must be considered in the analysis[6].[7]

2.8 Is it possible to reuse the RIPD for the EIA? How?

Yes, even the EU AI Act itself provides for this possibility . PL 2,338/23 also provides that if the AI agent has to prepare RIPD, under the terms of the LGPD, the EIA may be carried out in conjunction with said document.

According to article 38, sole paragraph, of the LGPD, the RIPD involves, at least:

[4] Recently approved in the Federal Senate and now in the Chamber of Deputies for consideration.
[5] Available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/analise-preliminar--do-pl-2338_2023-formatado-ascom.pdf
[6] Available at: https://lapin.org.br/2023/04/13/

(i) description of the types of data collected;

(ii) methodology used to collect and ensure information security; and

(iii) the controller's analysis of the measures, safeguards and risk mitigation mechanisms adopted.

Similarly, the EIA generally involves a description:

(a) of the system and its use;

(b) the measures adopted to conform the system to the principles of AI;

(c) an assessment of the risks to the persons affected; and

(d) the measures to be adopted to mitigate such risks, including human supervision, and treatment of their eventual materialization.

Thus, it is possible to reuse the RIPD for the EIA, as long as it is complemented, in the following sense:

- the description of the processing activity is deepened in order to cover the functioning and application of the AI-system as a whole;

- Deepening of the principles, so that they start to cover AI issues. For instance:
  1. Autonomy and criteria for human review;
  2. When addressing the principle of non-discrimination, it is important to highlight the measures adopted regarding the selection of the database and the tests in the system to avoid bias;
  3. When addressing the principle of quality, it is necessary to highlight measures to ensure the statistical accuracy of the system, avoiding AI hallucinations and other incorrect or inaccurate results.
  4. When addressing the principles of prevention and security, it is important to highlight the measures adopted to ensure the technical robustness of AI (e.g., failure approval plans) and protect the system from attacks typically aimed at AI solutions (e.g., adversarial attacks);
  5. Explainability: it must determine whether the AI system is sufficiently explainable and interpretable for developers and users;
- Reliability: AI system produces consistent results;
- Resilience and continuity: consider an action plan, in case there is a problem with the AI system;
- Environmental Impact Assessment.[8]

[7] Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

3. RESOLUTION AND GUIDE FOR THE PERSON IN CHARGE OF THE ANPD (No 18/2024)

The contemporary economy and business are increasingly driven by personal data, the driving force of various economic transactions and essential vectors for the development of various markets. In this context, the role played by the DPO gains fundamental importance and is presented as strategic as it occupies a central position in ensuring compliance, especially of the controller, with the personal data protection legislation in Brazil.

The relevance of the Data Protection Officer (DPO) began to be better assimilated when the lawful, ethical and responsible treatment of personal data proved to be a great competitive advantage among economic agents [1] [2]. The position became more valued and more resources began to be made available for data protection within organizations. [3] Increasing companies' data protection budgets bring a return on investment by improving customer trust, business partners, and regulatory compliance.

The National Data Protection Authority (ANPD) regulated the topic through Resolution No. CD/ANPD No. 18/2024[4] and recently brought good practices with the Guidance published in December 2024 [4].

3.1 Appointment of the Officer in Charge and the Substitute Officer

The appointment of the Person in Charge is a legal obligation of the controller, detailed in Resolution No. 18 and reinforced in the Guidance Guide for the Person in Charge. As there is no such obligation to the operator or to small agents expressly, the appointment of a Person in Charge is optional, and is considered good practice.

According to these documents, there must be a formal indication of the Person in Charge (and a substitute or "Interim DPO"), their forms of action and the activities to be performed. However, the substitute Person in Charge does not need to be appointed in the same act, so this will be at the choice of the processing agent who can define the most opportune time for this (e.g., on the eve of the Holder's vacation, or in situations of conflict of interest), provided that the constant occupation of the position is guaranteed to enable the exercise of the rights of the holders of personal data and/or compliance with ANPD communications.

Do I need to indicate the name and contact details of the Data Officer?

Although a controversial legal obligation because it puts some fundamental rights at risk, the Resolution requires and the Guide ratifies the need for public disclosure of the identity (full name) and contact information of the DPO and, in the case of the DPO being a legal entity, in addition to its corporate name, the full name of the natural person responsible it must also be publicly informed in a prominent and easily accessible place, in a clear and objective manner, on the website or in any other means of communication available and used to contact the holders, including when the DPO is external to the organization (DPO as a Service). In the case of contact information, the indication of the e-mail or telephone number of the Person in Charge

complies with the legislative requirement.

Therefore, while this legal obligation is in force, the controlling shareholders must comply with it. In fact, at the end of 2024, the ANPD published news on its website about the establishment of 20 (twenty) inspection procedures against controllers who would have failed to appoint a Person in Charge and to provide a direct and/or effective communication channel with data subjects [5].

3.2 What is a conflict of interest and what is its importance for the Person in Charge?

The ANPD, following a European example on the subject, emphasizes that the **absence of "conflict of interest"** is a prerequisite for the accumulation of functions, aiming to ensure the independent performance and technical autonomy of the Officer.

The concept of conflict of interest is brought by Resolution No. 18/2024 and is configured in **"situations that may compromise, influence or affect, in an improper way, the objectivity and technical judgment of the Person in Charge in the performance of their duties"**. Its analysis, therefore, must be done on a case-by-case basis.

In this sense, for the ANPD and data authority and European bodies, some situations are examples of conflict of interest, namely:

- Conflict of interest between duties exercised internally by the DPO in a processing agent with functions/positions:

  1. that involve decisions about data protection in the organization;
  2. senior management, such as Executive Director, Operational Director, Financial Director, Medical Director, Marketing Director, HR Director, IT or Information Security Director, Compliance, Audit and Risk Director (WP29 and EDPB, Belgium's data protection authority);
  3. lower in the company's organizational structure, when their performance leads to the determination of the purposes and means of processing personal data, as in the case of an IT Manager, or a lawyer in the Legal Department of a company that also defends it in cases about personal data (WP29 and EDPB, CNIL, ICO);
  4. that have competing objectives and that put the protection of personal data in the background in relation to the company's commercial interests (ICO).

- Conflict of interest in the exercise of the activity of Person in Charge in different processing agents:

  1. commitment to the effective performance of functions, taking into account the structure and size of these organizations;
  2. lack of resources necessary to develop their role in organizations and lack of support from a team, when necessary;
  3. companies with divergent interests;
  4. impossibility of access to the Person in Charge who serves a group of companies (headquarters and branches) due to the lack of adequate organization.

Thus, although the DPO cannot accumulate its functions with those involving decisions on data protection in the organization, the processing agent, by ANPD Resolution No. 18/2024, must mandatorily consult it for the purposes of assistance and guidance when carrying out activities and making strategic decisions regarding the processing of personal data.

Therefore, in addition to the care of the processing agent to avoid a conflict of interest, it is also the duty of the Data Processor, and also of the substitute, to declare to the processing agent any situation that may configure it, being responsible for the veracity of the information provided.

3.3 Is it possible to appoint a Global DPO or LATAM DPO to function as a DPO in Brazil?

Some Latin American countries also require the appointment of the Data Controller, such as **Colombia and Mexico;** others require it only for some specific sectors and if the controller's predominant data processing has certain characteristics, such as large-scale processing of sensitive personal data, such as **Ecuador and Uruguay.**

In this context, there is no prohibition in Brazilian law on the appointment of a Global DPO or LATAM DPO to also act as a Person in Charge and processing agent located in Brazil. However, Resolution No. 18/2024, in its article 13, **expressly requires** that the Person in Charge knows how to communicate clearly and accurately in Portuguese. Therefore, the

Global DPO or the LATAM DPO can play this role in Brazil, as long as it communicates in Portuguese.

If communication in Portuguese is not possible, it will be necessary to appoint a representative here in Brazil to be the Person in Charge.

It is important to note that the exercise of the activity of Person in Charge does not presuppose registration in any entity or specific certification or professional training, but your specialized knowledge in data protection is important, considering the activities of your controller.

3.4 What are the main measures to be adopted by the controller in relation to the Person in Charge?

In addition to the attention to the analysis of the conflict of interest, it is worth summarizing the main duties of the controllers in relation to the performance of the Person in Charge:

i) provide it with sufficient human, technical and administrative resources for the proper performance of its role;

ii) engage you for assistance and guidance in strategic decisions about data protection. It is not up to the Person in Charge to make the decision;

iii) guarantee its technical autonomy by ensuring that it does not suffer undue interference;

iv) ensure means for good communication; and

v) ensure access to people at a higher hierarchical level, as well as to other areas of the organization.

3.5 Is it possible to hold the Person in Charge liable?

The civil liability for the compliance of processing agents with the LGPD falls on them (controllers and operators), and not on the Data Protection Officer, as expressly provided for in the LGPD, in articles 42 to 45. The Person in Charge, for performing strategic and technical functions, without decision-making power over data processing operations, cannot be punished for the unlawful action of the controller or the operator. Therefore, any administrative or judicial sanctions related to violations of the LGPD are directed to the processing agents.

However, the Person in Charge (service provider or CLT employee) assumes legal and contractual obligations, whose intentional or culpable non-compliance may give rise to some type of indirect liability, according to the rules of Civil Law and the Consolidation of Labor Laws (CLT). This situation is remote and may materialize in situations in which it is proven that the Person in Charge acted in bad faith (willful misconduct) or in a negligent, reckless or malpractice (faulty) manner in the exercise of his duties, under the terms of articles 186, 187, 927 and 934, of the Civil Code and 462, paragraph 1 of the CLT. [6]

For more information on the subject, access here the 2nd Edition of the Officer's Guide, prepared by VLK.[9]

[1] Available at: https://dponapratica.com.br/wp-content/uploads/2023/01/2023-cisco-privacy-benchmark-study-2023-Portuguese-Brazilian.pdf
[2] Available at: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2024.pdf?CCID=cc000160&DTID=odicdc000016&OID=rptsc032067
[3] Available at: https://www.edpb.europa.eu/system/files/2024-01/edpb_report_20240116_cef_dpo_en.pdf
[4] Available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia_da_atuacao_do_encarregado_anpd.pdf
[5] Available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-fiscaliza-20-empresas-por-falta-de-encarregado-e-canal-de-comunicacao
[6] Available at: https://www.migalhas.com.br/depeso/334947/responsabilidade-civil-do-encarregado-pelo-tratamento-de-dados-pessoais--regime-celetista

4. INTERNATIONAL TRANSFER OF PERSONAL DATA (TID)

4.1 What is international transfer and what are the TID Mechanisms?

The international transfer of data must **necessarily** involve at least **two processing agents**: the exporter and the importer, located in countries other than Brazil or in international organizations of which Brazil is a member.

To enable the international transfer of data, the LGPD requires processing agents to adopt specific mechanisms (article 33 of the LGPD), some of which are regulated by the ANPD and others self-applicable. Resolution CD/ANPD No. 19/2024 regulated instruments such as adequacy determinations

(i) standard contractual clauses (detailed in Annex II);

(ii) equivalent standard contractual clauses;

(iii) specific contractual clauses for a particular transfer; and

(iv) global corporate standards. Specific regulations are still pending: seals, certificates and codes of conduct

Adequacy determinations

Although the Standard Contractual Clauses are the most used mechanism worldwide, adequacy determinations stand out for promoting economic integration with strategic partners, such as the European Union (EU), and aligning Brazil with global data protection standards. This regulatory harmonization strengthens legal certainty, attracts foreign investment, and boosts international trade, essential elements for the country's sustainable growth. The ANPD is negotiating with the EU to enable mutual adequacy determinations and it is likely that in mid-2025 Brazil and the European Union will recognize each other as being mutually adequate to the degree of protection of personal data required by their respective legislations.

4.2 Is there a deadline for the application of Resolution No. 19/2024?

Resolution No. 19/2024 entered into force on the date of its publication, that is, on 08.23.24, establishing a period of 12 months for processing agents who decide to adopt the Standard Contractual Clauses (SCCs) (Annex II, of Resolution No. 19/2024) to, within this period, incorporate them into their respective contractual instruments.

The other mechanisms on international transfer, therefore, have been applicable since August 2020, with the LGPD coming into force, or became applicable on 08.23.2024, with Resolution No. 19/2024, except:

(i)) the Standard Contractual Clauses (SCCs) whose deadline for full adoption ends on **08.23.25;** and

(ii) the seals, certificates and codes of conduct that have not yet been regulated.

Thus, it is possible to summarize these deadlines as follows:

Mechanisms provided for in article 33, III to IX of the LGPD

Applicable and enforceable since **August 2020**

Decision of adequacy (art. 33, I)

Applicable since 08.23.2024 with the adoption procedure provided for in Resolution No. **19/2024**

Standard Contractual Clauses (SCCs) (Annex II of Resolution No. 19/2024)

Applicable since 23.08.2024 and payable

from **23.08.25**

Equivalent standard contractual clauses

Applicable since 08.23.2024 with the adoption procedure provided for in Resolution No. 19/2024

Specific contractual clauses for a particular transfer

Applicable since 08.23.2024 with the adoption procedure provided for in Resolution No. 19/2024

Global Corporate Standards

Applicable since 08.23.2024 with the adoption procedure provided for in Resolution No. 19/2024

Seals, certificates and codes of conduct

Inapplicable (pending regulation by the ANPD)

4.3. What are the most appropriate transfer mechanisms? How is it different from the legal basis?

The mechanisms for the international transfer of personal data are a legal provision (article 33 of the LGPD) whose proper adoption makes the TID lawful. Legal bases, on the other hand, are legal hypotheses that the LGPD requires to be adopted to make the personal data processing operation itself lawful and are listed in articles 7, 11 and 14 of the LGPD.

However, the LGPD has elected some legal bases as international transfer mechanisms, which generates some confusion. This occurs in article 33, items:

IV (protection of the life or physical safety of the holder or a third party);

VII (execution of public policy or legal attribution of public service);

VIII(specific and highlighted consent);

IX only for non-sensitive personal data **(compliance with legal or regulatory obligations; execution of contracts and preliminary procedures to which the holder is a party; regular exercise of rights in judicial, administrative or arbitration proceedings).**

Thus, the controller may adopt any of the TID mechanisms provided for in article 33 of the LGPD. The decision on the adoption of the most appropriate transfer mechanism is up to the agent and processing, more precisely to the controller-exporter and according to its processing activities. Therefore, it is up to him to define the best mechanism to adopt to comply with Brazilian data protection legislation.

Contract Execution and Preliminary Procedures (article 33, V c/c article 7, item V of the LGPD)

The ITE mechanism based on the legal basis of contract execution and preliminary procedures related to the contract has some conditions to be accepted, such as:

(i) the holder must be a party to the contract;

(ii) the data processing must take place at the request of the data subject;

(iii)) it can only be used if the processing in question is essential for the execution of the contract signed between the processing agent and the data subject, according to European precedents.

Therefore, the choice of the controller is not acceptable (e.g. chose to use a cloud storage service abroad), but it must be necessary for the execution of the contract to which the holder is a party (e.g. contract made in Brazil for car rental on a trip abroad: the holder's personal data must be transferred to the country where the car will be picked up, otherwise, the execution of the contract is impossible).

Consent

The TID mechanism that deals with consent, as provided for in article 33 item VIII, must meet its legal conditions and must be:

(i) specific;

(ii) in particular for the transfer;

(iii) it can only be used as long as there has been prior information about the international nature of the operation; and

(iv)the purposes have been clearly differentiated from other purposes for which consent was collected.

4.4. In addition to the international data transfer mechanism, is it necessary to indicate an autonomous legal basis for the international transfer?

Although the LGPD does not expressly require this indication, the ANPD in its Resolution No. 19/2024 determined so in its article 4, III c/c article 9, I and II. Therefore, the processing

agent must support its international data transfer in one of the international data transfer mechanisms and indicate the independent legal basis for the transfer of personal data.

This will bureaucratize international transfer and has the effect of making it virtually impossible to transfer sensitive personal data, as the legal basis of legitimate interest, which underpins most organizations' strategic decisions in terms of international data transfer, cannot be used for this category of personal data.

In any case, in cases where the TID mechanism reproduces a legal basis, both the mechanism and the legal basis for that particular TID will be the same. (Ex. Vehicle rental agreement signed in Brazil to pick up the car in Paris, France). There will be a need to transfer the personal data collected from the holder for the execution of this contract, of which the holder is a party. Therefore, the TID mechanism will be **contract execution (Article 33 IX of the LGPD),** as well as the legal basis for international data transfer will be **contract execution (Article 7 V).**

4.5 What to do if I already adopt Standard Contractual Clauses from another country or international organization?

It is possible to file a request for recognition of equivalence before the ANPD (articles 18 to 20 of Resolution No. 19/2024), by which the ANPD will analyze the Standard Contractual Clauses and verify:

(i) whether they are compatible with the provisions of the LGPD and Resolution No. 19/2024;

(ii) they ensure a level of data protection equivalent to that guaranteed by the national contractual standard clauses;

(iii) the risks and benefits provided by the approval, considering, among other aspects, the guarantee of the principles, the rights of the holder and the data protection regime of the national legislation; in addition to

(iv) impacts on the international flow of data, diplomatic relations, international trade and international cooperation of Brazil with other countries and international organizations.

4.6 What is the best mechanism for international data transfer to the US and the European Union?

European Union (EU)

For the international transfer of data between processing agents located in Brazil (exporter) and the European Union (importer), the ANPD's Standard Contractual Clauses can also be immediately adopted, however, if the processing agents have already regularized this transfer via European Standard Contractual Clauses (EU's SCCs), Resolution No 19/2024 allows them to be submitted to a procedure for recognition of equivalence before the ANPD. There are reports that there is already a request in this regard in progress at the ANPD, therefore, once the equivalence of the EU's SCCs is recognized, Brazilian processing agents will also be able to validly use them for the purposes of international data transfer from Brazil to the EU.

In any case, once the European Union's adequacy decision is issued by Brazil (ANPD), this decision will be sufficient to support international data transfers.

United States of America (USA)

For the international transfer of data between processing agents located in Brazil (exporter) and the USA (importer), in principle, the best mechanism to be adopted is the ANPD's Standard Contractual Clauses. This is because Brazil does not have an adequacy decision with the US similar to the European Union's decision with the US, the "USA-EU Data Privacy Framework", adopted on July 10, 2023[1], nor are there any North American Standard Contractual Clauses.

4.7. What is the means made available by the ANPD to carry out the requirements provided for in Resolution No. 19/2024?

In September 2024, the ANPD launched on its website, a specific page for the international transfer of personal data. Requests for the approval or review of international data transfer mechanisms must be submitted to the ANPD via the Electronic Information System (SEI), which aims to ensure efficiency and security in the processing of requests, allowing companies to monitor the progress of their requests. [2]

For more information visit our Q&A on the topic on our website here.[10]

[1] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023D1795

[2] Available at: https://www.gov.br/anpd/pt-br/assuntos/assuntos-internacionais/assuntos-internacionais-pt

5. CYBERSECURITY AND INCIDENT RESPONSE

Cybersecurity and Incident Response are among the highest priority topics for the ANPD. Of the 10 sanctioning proceedings initiated by the Authority so far, 8 are directly related to this issue [1].

Given this scenario, we present the main aspects that deserve attention when dealing with cybersecurity in the context of personal data protection.

5.1 What security measures should be adopted?

There is no "single solution" to answer this question. Security measures must always be proportional to the risk and adjusted to the specific case, according to article 44 of the LGPD, which requires that the processing meets what is "reasonably expected" by the data subject.

But what does "reasonably expected" mean?

Although this analysis depends on the risks of each specific activity, the measures indicated by the ANPD in the Checklist for Small Processing Agents represent the minimum expected of any processing agent, including [1]:

- **Information Security Policy:** establish and review periodically;
- **Contracts:** include specific data protection and security clauses;
- **Training and awareness:** promote capacity building on privacy and security, including prevention of common threats such as viruses and social engineering;
- **Access controls:** limit access permissions to the minimum necessary, implement periodic password change and multi-factor authentication (MFA);
- **Data minimization:** reduce the processing of personal data to what is necessary and remove data unnecessarily exposed in public environments;
- **Encryption:** protecting data at rest, including external devices, and in transit;
- **Security of external devices:** controlling, inventorying and minimizing their use;
- **Backups:** make periodic offline copies and store them securely;
- **Disposal of physical media:** formatting, overwriting, or destroying media before disposal. Ensure disposal/ destruction record when hiring third parties, through a contract.
- **Firewall or WAF:** install and maintain Firewall or Web Application Firewall;
- **Email Protection:** implement antispam filters and integration with antivirus software;
- **Security updates:** keeping systems up to date to fix security flaws;
- **Protection software :** install, update

and perform periodic scans with antivirus and antimalware;

- **Mobile device security:** segregate institutional devices from private individuals, protect with MFA, and enable remote deletion;

- **Cloud Services Security:** Ensure compliance with security requirements, robust access controls, and appropriate service-level agreements..

It is also important to highlight that the LGPD provides the ANPD with the possibility of determining minimum technical standards for information security – which tend to be more robust than those aimed at small agents. It is expected that these standards will be issued by the ANPD in 2025, as it is one of the activities provided for in phase 1 of the authority's Regulatory Agenda for the 2025-2026 biennium[2].

Finally, many regulated sectors have specific cybersecurity standards or related requirements, which should also be considered as part of the "reasonably expected minimum" by the holders of processing agents who are part of these sectors. Therefore, it is essential to observe sectoral regulations because non-compliance tends to constitute irregularity in the treatment. Examples of sectoral standards include:

Sector Financial

CMN Resolution No. 4,893/2021 (updated in January 2024) – Provides for the cybersecurity policy, including minimum controls to be adopted, and cloud services [3].

Sector Telecommunications

ANATEL Resolution No. 740/2020 (updated in August 2024) – Regulates the conducts and procedures for the promotion of security in telecommunications networks and services, including Cybersecurity [4].

Sector Health

CFM Resolution No. 1,821/2007 and COFEN Resolution No. 754/2024 – Provide rules for the electronic medical record, establishing the need for compliance with the security requirements applicable to NGS2, of the Certification Manual for Electronic Health Record Systems [5][6].

It is also important to consider the application of rules from other jurisdictions. For example, the European Union's Digital Operational Resilience Act (DORA)[7] establishes a number of obligations for European financial institutions, including the management of risks related to ICT providers. Thus, suppliers that provide services, especially those considered critical, to these institutions must adapt to meet the level of security required by this regulation.[11]

5.2 What should I adjust in my Incident Response Plan?

A significant part of the sanctioning proceedings at the ANPD stems from the lack of communication of incidents to the data subjects and to the Authority itself. Therefore, it is essential that organizations adjust their Incident Response Plans to the requirements set forth in the Security Incident Communication Regulation [1].

On this topic, read the Security Incident Communication E-Book (click here), which includes the following simultaneous actions, in the case of responding to security incidents involving personal/sensitive data:

[1] https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/checklist-vf.pdf
[2] https://www.gov.br/anpd/pt-br/acesso-a-informacao/acoes-e-programas/governanca/governanca-estrategica/resolucao-no-23-de-9-12-2024-agenda-regulatoria-2025-2026.pdf
[3] https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4893
[4] https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1497-resolucao-740
[5] https://www.cofen.gov.br/resolucao-cofen-no-754-de-16-de-maio-de-2024/#:~:text=Normatiza%20o%20uso%20do%20prontu%C3%A1rio,guarda%20e%20armazenamento%20nesta%20tecnologia.
[6] https://www.cofen.gov.br/resolucao-cofen-no-754-de-16-de-maio-de-2024/
[7] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554&from=FR

5.3 Is it necessary to pay the holder compensation?

Civil liability typically requires the presence of three basic elements: unlawful act or omission of the processing agent, damage to the data subject, and causal link between the act and the damage.

In a recent decision handed down in Special Appeal No. 2147374 – SP, the Third Panel of the Superior Court of Justice (STJ) came to an understanding that the liability regime does not fit into the traditional regimes of subjective and objective liability, but into a new regime of "proactive liability" [1].

In this regime, it is not enough to comply with the law to avoid liability. It is also necessary to demonstrate the effectiveness of the measures adopted in terms of preventing potential damage resulting from its activities. [2].

Thus, the processing agent that suffered an incident and did not adopt and/or did not demonstrate sufficient security measures that the data subject could reasonably expect, he may be held liable for the damages resulting

from the incident.

Regarding damages, they can be classified as material (related to property losses) or moral (linked to non-property aspects, such as honor, image, and dignity). In the case of moral damages, they can be presumed (in re ipsa) or depend on proof of the violation of personality rights.

Regarding moral damages, in the Interlocutory Appeal in Special Appeal No. 2130619/22 – SP (Brazil) [3], which dealt with the leakage of registration data, the Second Panel of the STJ distinguished between sensitive personal data [4] and other personal data. For sensitive data, it was understood that there was a presumption of moral damages due to the strong connection of these data with the intimacy of the affected person. In the case of other personal data, proof of damage is required.

As for material damages, based on precedents on leakage of bank data, such as Special Appeal 2077278/23 – SP[5], the Third Panel of the STJ understood that the processing agent can be held liable not only for direct material damages resulting from the leak, but also for losses caused by practices facilitated by it, such as financial fraud resulting from social engineering, that is, it held the processing agent liable for indirect damages.

[4] " Sensitive personal data includes information on racial or ethnic origin, religious beliefs, political opinions, union membership, or affiliation with religious, philosophical, or political organizations, as well as health, sexual life, genetic, or biometric data when linked to an identifiable individual" (See article 5 II of the LGPD).

WWW.VLKLAW.COM.BR

E-book - The future of Privacy: How to be prepared for 2025. March, 2025

This document is intended to provide information for educational and academic purposes. It should not be construed as legal advice.