A Year in Privacy

ADMINISTRATIVE PROCESS TRAIL

SANCTIONING ADMINISTRATIVE PROCESS

DECISION PHASE AND APPLICATION OF SANCTIONS

Guide 05

Authors:

Matheus Botsman Kasputis

Thiago Xavier Peregrino

Adele Mendes Weinberg

Reviewers:

Adriane Loureiro Novaes

Fernando Bousso

b/luz

Clickable summary

SUMMARY

← Return to summary

1. INTRODUCTION

In the fourth Guide of the Administrative Process Trail, we covered the phases of initiating and instructing the sanctioning administrative process of the Brazilian National Data Protection Authority (ANPD), including the issuance of the notice of violation, the defense of the accused, the production of evidence, the participation of interested parties, the involved deadlines, and the final arguments and preparation of the instruction report.

In this fifth Guide, we will address the decision phase in the first instance of the sanctioning administrative process, including the sanctions that may result from a condemnatory decision by the ANPD's General Coordination of Inspection and how these sanctions may be mitigated considering the circumstances of the Authority's Regulation on Dosimetry and Application of Administrative Sanctions[1].

1 BRAZIL. Resolution CD/ANPD No. 4/2023. Official Gazette of the Union: Brasília/DF. Available at: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077. Accessed on August 18, 2024.

← Return to summary

2. THE DECISION PHASE OF THE SANCTIONING ADMINISTRATIVE PROCESS

The ANPD's Internal Regulation establishes that it is the responsibility of the General Coordination of Inspection to make decisions in the first instance in sanctioning administrative processes[2]. The Authority's Inspection Regulation echoes this provision, adding that the decision will be issued after the conclusion of the procedural instruction phase.[3]

The General Coordination of Inspection will issue the first-instance decision in the form of a **decision order[4],** based on the instruction report's information – covered by our Guide 04 – Sanctioning Administrative Process –, and always in a reasoned manner, including, at a minimum:

2 Internal Regulation of the ANPD: Art. 17, Item II. BRAZIL. ANPD Normative Ordinance No. 1/2021. Official Gazette of the Union: Brasília/DF. Available at: https://www.in.gov.br/en/web/dou/-/portaria-n-1-de-8-de-marco-de-2021-307463618. Accessed on August 18, 2024.

3 Inspection Regulation: Art. 55. BRAZIL. Resolution CD/ANPD No. 1/2021. Official Gazette of the Union: Brasília/DF. Available at: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-1-de-28-de-outubro-de-2021-355817513. Accessed on August 18, 2024.

4 Internal Regulation of the ANPD: Art. 51, Item III.

the facts described in the context of the administrative process;

the legal grounds supporting the decision; and

the sanctions applied, if any.

After the decision order of the General Coordination of Inspection, the sanctioned parties will be notified by an ANPD official letter to:

i. comply with the decision within the deadline indicated in the order; or

ii. appeal to the ANPD's Board of Directors within ten business days of the notification.

In any case, **the notification concludes the decision phase**, and the administrative process moves on to the sanction enforcement phase (or collection and execution) or administrative appeal, topics that will be addressed in the upcoming Guides.

If the ANPD determines that there has been **no violation of Law 13,709/2018 (General Data Protection Law or LGPD)**, for instance, it may use the decision order to simply close the case without imposing sanctions. This occurred in Decision Order Nº. 20/2024/PR/ANPD[5], where the General Coordination of Inspection found that the Instituto de Pesquisas Jardim Botânico do Rio de Janeiro did not incur in a security incident under the General Data Protection Law due to the absence of personal data.

In addition to the possibility of closing the case without imposing sanctions, the ANPD also has other procedural mechanisms, such as joint judgments, which may be used to ensure uniformity and coherence in decisions.

Joint Judgment

Provided for in Article 57 of the ANPD's Inspection Regulation, joint judgment is an institute that may be used by the General Coordination of Inspection in the first-instance decision phase or in appeals, allowing for the consolidation of processes under certain circumstances.

5 BRAZIL. Decision Order No. 20/2024/PR/ANPD. Official Gazette of the Union: Brasília/DF. Available at: https://www.in.gov.br/en/web/dou/-/despacho-decisorio-n-20/2024/pr/anpd-569297245. Accessed on August 18, 2024.

Although it has never been adopted by the ANPD to date, joint judgment is not a new mechanism in the Brazilian legal-pr ocessual universe. Indeed, it is observed that the Authority has approached it in a manner very similar to that found in the Brazilian Civil Procedure Code, for example:

Civil Procedure Code	Resolution CD/ ANPD Nº. 1/2021
"Art. 55 § 3: Processes that could result in conflicting or contradictory decisions if decided separately, even without connection between them, shall be consolidated for joint judgment."	"Art. 57: It is possible to consolidate processes for joint judgment if they could result in conflicting or contradictory decisions if decided separately, even without connection between them, whether in the first-instance decision phase or in appeals."

In light of this, it can be understood that the institute of joint judgment can be applied by the General Coordination of Inspection when there are multiple decisions to be made, whether on the same subject or not, as long as there is a risk that different decisions might conflict or contradict each other. This practice can be employed to ensure uniformity and coherence in decisions, as well as to promote greater efficiency in the handling of cases.

← Return to summary

3. THE APPLICATION OF ADMINISTRATIVE SANCTIONS IN CONDEMNATORY DECISIONS BY ANPD

As previously discussed, the decision phase is the first moment when, if there is a violation of the General Data Protection Law, the ANPD may apply administrative sanctions.

When addressing sanctions, it is important to remember the ANPD's method of operation. As outlined in Guide 03 – Sanctioning Administrative Process, the responsive regulation approach adopted by the Authority involves mechanisms of oversight and enforcement, with the sanctioning process being a fundamental part of the second phase of regulation. According to the ANPD's Inspection Regulation, the enforcement activity typically occurs after the oversight process, when monitoring, guidance, and prevention activities have not achieved the desired results, necessitating the investigation of violations of the General Data Protection Law and the possible application of sanctions.

The applicable sanctions are established in the General Data Protection Law and detailed in the Regulation on Dosimetry and Application of Administrative Sanctions[6]. These sanctions can be applied progressively, individually, or cumulatively, depending on the specific case and considering parameters and criteria such as the severity of the violation, the good faith of the offender, the benefit obtained by the offender, recidivism, among others. Below, we will briefly address each of the possible sanctions individually.

6 BRAZIL. Resolution CD/ANPD No. 4/2023. Official Gazette of the Union: Brasília/DF. Available at: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077. Accessed on August 18, 2024.

3.1. WARNING

Established by Article 52, I, of the LGPD and Article 9 of the Regulation on Dosimetry and Application of Administrative Sanctions, the warning is the most basic sanction possible, serving only as a notice in cases of minor or moderate violations (as classified in Article 8 of the Regulation), provided there is no specific recidivism.

Specific recidivism *is defined by Article 2, Item VIII, of the Regulation on Dosimetry and Application of Administrative Sanctions, as the repetition of an infraction by the same offender concerning the same legal or regulatory provision, within a period of 5 (five) years. This period is calculated from the date of the final decision in the sanctioning administrative process to the date of the new infraction.*

Generic recidivism*, as defined by Article 2, Item IX of the Regulation on Dosimetry and Application of Administrative Sanctions, refers to any new infraction committed by the offender within a period of 5 (five) years, regardless of the specific legal or regulatory provision violated.*

The warning will always be accompanied by the indication of a corrective measure and a deadline for the offender to correct the infraction identified by the ANPD.

Practical Example

The ANPD's first sanction[7], for instance, involved a warning issued to a microentrepreneur who failed to designate a data protection officer, violating Article 41 of the LGPD. According to the Authority, the failure to designate a data protection officer was classified as a minor infraction, necessitating a warning with a 10-business-day deadline for the offender to designate a data protection officer.

7 BRAZIL. National Data Protection Authority. ANPD Imposes First Fine for Non-Compliance with LGPD. Available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd. Accessed on August 19, 2024.

← Return to summary

3.2. FINES

According to Items II and III of Article 52 of the LGPD, there are two distinct types of fines that can be imposed: a simple fine and a daily fine. Initially, the General Data Protection Law established only the limits for simple and daily fines[8], with the Regulation on Dosimetry and Application of Administrative Sanctions providing a detailed system for applying sanctions in Sections IV, V, and VI.

The **simple fine** is applied when the offender fails to comply with preventive or corrective measures imposed, when the infraction is classified as serious, or when, due to the nature of the infraction, applying another sanction is not suitable.

In line with the General Data Protection Law, the Regulation on Dosimetry and Application of Administrative Sanctions stipulates that the base value of the fine should be determined considering the classification of the infraction, the company's revenue, and the degree of harm caused, using gross revenue and other financial parameters to define the base amount and avoid disproportionate penalties.

Additionally, the Regulation defines aggravating and mitigating circumstances that can adjust the fine amount. Aggravating circumstances, such as recidivism and non-compliance with preventive or corrective measures, are used to increase the penalty amount, aiming to discourage repetitive behavior and ensure that the sanction reflects the infraction's severity and the resistance to complying with the rules. Conversely, mitigating circumstances, such as rectifying the infraction and adopting good practices, can lead to a significant reduction in the fine amount, encouraging the offender's cooperation and proactive compliance practices.

Daily fines use similar parameters but aim to ensure compliance with non-monetary sanctions or other established requirements, seeking an approach that pressures offenders until compliance is achieved. On the other hand, the Regulation sets a cap on the accumulated value of the fine per infraction, preventing excessively punitive sanctions.

8 General Data Protection Law: "Article 52. II - Simple fine, of up to 2% (two percent) of the private legal entity's, group's, or conglomerate's revenue in Brazil for its last fiscal year, excluding taxes, limited, in total, to R$ 50,000,000.00 (fifty million reais) per infraction; III - Daily fine, respecting the total limit referred to in item II".

← Return to summary

The Regulation on Dosimetry and Application of Administrative Sanctions also sets a deadline for paying fines, with a standard limit of 20 business days, with the possibility of granting extended deadlines for small-scale data controllers. Additionally, there are provisions for late payment charges, such as interest and late fees, ensuring compliance within the due timeframe.

Practical Example

In addition to issuing a warning, the ANPD's first sanction also included imposing a simple fine on the offender, totaling R$ 14,400.00 for violations of Article 5 of the Inspection Regulation and Article 7 of the LGPD, demonstrating the possibility of accumulating sanctions when necessary.

3.3. PUBLIC DISCLOSURE OF THE INFRACTION

According to the Regulation on Dosimetry and Application of Administrative Sanctions, public disclosure of the infraction is a sanction that requires the offender to make their infraction public once it has been investigated and confirmed.

This sanction might be one of the strictest within the ANPD's sanctions framework, potentially even more detrimental than a fine. Announcing an infraction related to a security failure of a product or service that resulted in a data breach, for example, can have a significant negative impact on the image of the data controller.

The sanction is closely related to transparency and public interest.[9] It is believed that when an infraction is of public interest, it is relevant for the ANPD to determine that the responsible data controller publicly informs about the infraction to as many data subjects as possible.

9 BRAZIL. National Data Protection Authority. Regulatory Impact Analysis Report – Construction of the Regulatory Model Provided in the LGPD Regarding the Application of Administrative Sanctions and the Methodologies for Calculating the Base Value of Fines. July 2022. Available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2022-06-30___air_reg_dosimetria_.pdf. Accessed on August 18, 2024.

← Return to summary

Practical Example

Recently, this sanction was applied in a notable case involving the National Social Security Institute (INSS) for failing to notify data subjects of a security incident in 2022 and not complying with the Authority's determinations. According to the ANPD: "the security incident could have caused significant harm to the rights of data subjects, as it involved a database containing information about social security benefits. Therefore, the INSS was required to notify the affected data subjects of the security incident". Thus, even after an appeal by the Institute, the Authority deemed it necessary to impose the sanction of public disclosure, requiring the INSS to publicize the infraction and the sanction imposed by the ANPD on its website and the "Meu INSS" app for 60 days from the date of awareness of the decision[10].

3.4. DATA BLOCKING AND DELETION

Articles 22 and 23 of the Regulation on Dosimetry and Application of Administrative Sanctions address two measures concerning data processing: data blocking and the deletion of personal data processed by the offender. The data blocking sanction involves temporarily suspending data processing until the infraction is corrected. This measure aims to immediately stop any improper use of data, preventing ongoing harm while the offender adjusts their practices to meet the General Data Protection Law requirements.

Furthermore, the ANPD requires the offender to notify the data controllers and processors with whom the data was shared to ensure effective blocking throughout the data processing chain. However, the Authority recognizes that in some cases, communication might be impossible or require disproportionate effort, introducing flexibility if such impediments are proven and recognized. For data unblocking, the offender must prove compliance with their conduct with the ANPD.

10 BRASIL. Autoridade Nacional de Proteção de Dados. ANPD sanciona INSS e Secretaria de Educação do DF por violações à LGPD. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-sanciona-inss-e-secretaria-de-educacao-do-df-por-violacoes-a-lgpd>. Acesso em 09 ago. 2024.

← Return to summary

The data deletion sanction demands the definitive removal of stored data. This measure is more drastic and aims to ensure that data involved in an LGPD violation is completely removed, preventing its misuse in the future. As with blocking, the offender must notify the data controllers and processors to ensure the procedure is replicated. The ANPD again allows exceptions for situations where communication would be impossible or require disproportionate effort, ensuring that the application of the sanction is practical and adaptable to real circumstances.

Practical Example

To date, there have been no cases where the ANPD has applied the sanctions of data blocking or deletion.

3.5. PARTIAL SUSPENSION OF DATABASE OPERATION

The partial suspension of database operation, as provided in Article 24 of the Regulation on Dosimetry and Application of Administrative Sanctions, is intended to halt the operation of databases that do not comply with data protection rules, reflecting the severity of the infractions.

The Regulation stipulates that partial suspension can last up to six months, with the possibility of extension for an equal period, depending on the complexity of compliance and the classification of the infraction. This period allows the offender sufficient time to implement necessary changes and ensures that the sanction is proportional to the infraction's severity and the complexity involved in achieving compliance. Considering public interest and the impact on data subjects' rights reflects a balance between the need to correct the infraction and minimize adverse impacts on the organization.

As with the previous sanction, the Regulation requires the offender to prove the regularization of data processing activities for the database operation to be fully restored, ensuring that normal operation resumes only after confirming that all corrective measures have been satisfactorily implemented.

← Return to summary

Practical Example

To date, there have been no cases where the ANPD has applied the sanction of partial suspension of database operation.

3.6. SUSPENSION AND PROHIBITION OF DATA PROCESSING ACTIVITIES

Regarding the exercise of data processing activities, the Regulation on Dosimetry and Application of Administrative Sanctions outlines two potential sanctions: suspension and prohibition. Article 25 of the Regulation specifies the suspension of data processing activities, aiming to temporarily halt processing operations that do not comply with legal and regulatory requirements. This sanction can be imposed for up to six months, extendable for an additional six months, depending on the complexity of the compliance process and the seriousness of the violation.

This measure allows the ANPD to intervene directly when data processing compromises the fundamental rights of data subjects, ensuring companies adjust their practices to meet legal requirements. The possibility of extending the suspension underscores the importance of protecting personal data, even if it means halting business operations.

Article 26 of the Regulation addresses the prohibition of data processing activities, either partially or entirely. This is the most severe sanction and may be applied in cases of repeated violations after a suspension has been imposed without achieving the desired result, or when data processing is done for illegal purposes or without legal basis. Additionally, it can be used if the company loses or fails to meet the necessary technical and operational conditions for proper data processing.

The prohibition is a stringent measure intended to correct violations and prevent the continuation of illegal or inadequate practices. It serves as a more rigorous control mechanism, ensuring companies maintain high compliance standards to avoid severe penalties that could significantly impact their operations.

Practical Example

To date, there have been no cases where the ANPD has applied the sanctions of suspension and prohibition of data processing activities.

International Overview

To create a comparative perspective on the international landscape regarding sanctions, we can look at two of the main data protection regulations globally: the General Data Protection Regulation (GDPR) from the European Union and the California Consumer Privacy Act (CCPA) from the United States.

When compared with Brazilian legislation, it is clear that — as discussed in previous guides — the LGPD and some of the ANPD's regulatory standards are heavily inspired by the GDPR and the European data protection framework. This is also true when discussing sanctions.

Generally, the penalties under the GDPR are quite similar to those in Brazil, including warnings, data blocking and deletion, suspension, and prohibition of data processing activities and international transfers, among others.[11] However, the main difference between Brazilian and European sanctions lies in the application of fines for breaches of legislation. As stated above, in Brazil, there are two types of fines:

daily fines and simple fines, with limits of up to 2% of the company or conglomerate's revenue in Brazil, capped at R$ 50 million per infraction. The GDPR, on the other hand, sets fines at two levels based on severity:

(i) up to 2% of the company's global revenue or 10 million euros for minor violations, such as failure to report an incident to authorities and data subjects; or

(ii) up to 4% of global revenue or 20 million euros for more severe violations, such as non-compliance with basic data processing principles or data subjects' rights[12]. These fines are applied differently across various European countries, as explained further in our Guide 03.

11 EUROPEAN UNION. General Data Protection Regulation. Art. 58 (2). Available at: https://gdpr-info.eu/art-58-gdpr/. Accessed on August 12, 2024.

12 EUROPEAN UNION. General Data Protection Regulation. Art. 83 (4), (5) and (6). Available at: https://gdpr-info.eu/art-83-gdpr/. Accessed on August 12, 2024.

The similarities observed in Europe, however, do not appear when comparing Brazilian rules with the CCPA in the United States. While Brazil has several types of sanctions available, the CCPA is limited to three types of fines: for unintentional violations, up to $ 2,500 per violation, and for intentional violations or violations involving minors, up to $ 7,500 each[13]. Additionally, the CCPA allows individuals who suffer damages from a personal data breach to sue the responsible company, with possible compensation ranging from $ 100 to $ 750 per incident, or higher amounts if actual damages are greater. Additionally, the CCPA allows individuals who suffer damages from a personal data breach to sue the responsible company, with possible compensation ranging from $ 100 to $ 750 per incident, or higher amounts if actual damages are greater[14].

In summary, the CCPA adopts a mixed approach combining administrative sanctions and private enforcement, allowing data subjects to claim their rights. Although individual fines may be smaller, class actions have the potential to cause significant financial impacts and harm the company's reputation due to their visibility.

13 UNITED STATES. California Consumer Privacy Act. Section 1798.155. Available at: https://cppa.ca.gov/regulations/pdf/cppa_act.pdf. Accessed on August 12, 2024.

14 UNITED STATES. California Consumer Privacy Act. Section 1798.150(a). Available at: https://cppa.ca.gov/regulations/pdf/cppa_act.pdf. Accessed on August 12, 2024.

← Return to summary

4. AGGRAVATING OR MITIGATING CIRCUMSTANCES IN SIMPLE FINES IMPOSED BY ANPD

In the case of simple fines, the ANPD has established mitigating and aggravating circumstances in the Regulation of Dosimetry and Application of Administrative Sanctions to ensure that they are proportional to the severity of the infraction and the infringer's conduct, promoting fairness and appropriateness in the punitive process.

These circumstances allow for the evaluation of factors such as the infringer's intent, cooperation with the authority, and the impact of the infraction, adjusting the penalty to, on the one hand, encourage compliance with the General Data Protection Law and the adoption of good data protection practices, and on the other, discourage negligent or malicious behavior.

4.1. AGGRAVATING CIRCUMSTANCES

Circumstance	Illustrative Example	Percentage of Increase *(per circumstance)*	Limit
Specific recidivism	Three years ago, a large healthcare company was sanctioned by the ANPD after a data breach, where an attacker exploited a vulnerability in the system and accessed unauthorized medical diagnoses, histories, and prescriptions. Recently, the company suffered another cyber-attack. The attacker, using more advanced techniques, exploited the same vulnerability and exfiltrated new information, including updates to medical records and confidential recent treatment data. The investigation revealed that the vulnerability had never been fixed, demonstrating the company's recidivism in the same infraction within a 5-year period.	10%	40%
Generic recidivism	A digital marketing company was fined by the ANPD for conducting campaigns using personal data of third parties, violating the principle of minimization while also lacking a legal basis. Two years later, the company was sanctioned for sharing customer data with business partners without implementing adequate security measures, resulting in a security incident. Although the infractions are different, the fact that the company has been penalized for violations of the General Data Protection Law on multiple occasions within a 5-year period constitutes generic recidivism.	5%	20%
Non-compliance with preventive or guidance measures in the inspection or preparatory procedure prior to the administrative sanction process	A cloud storage service company was advised by the ANPD, through a compliance plan, to implement a governance program including an Information Security Policy and an Incident Response Plan. Upon inspecting the company on another occasion, the ANPD found that there had been no improvement in its governance structure, revealing that its compliance plan had not been followed and, therefore, the guidance was not observed by the company.	20%	80%

Non-compliance with corrective measures	A technology startup was warned by the ANPD and instructed to (i) update its privacy policies; (ii) implement stricter access controls; and (iii) train its employees. Continuing the administrative process, the ANPD found that the startup had not complied with these requirements. The privacy policies remained outdated, access controls continued to be inadequate, and employee training was incomplete, indicating that the corrective measures were not observed.	30%	90%

REMINDING CONCEPTS

- **Preventive or guidance measure:** measures applied by the ANPD during its advisory or preventive activities, aiming to bring the data controller into compliance or prevent risks or damages

To learn more, visit Guide 4 of the Administrative Process Trail

- **Inspection process:** includes the activities of monitoring, advising, and preventive actions carried out by the ANPD

To learn more, visit Guide 2 of the Administrative Process Trail

- **Preparatory procedure:** the stage preceding the initiation of the administrative sanctioning process, in which indications of an infraction are investigated

To learn more, visit Guide 3 of the Administrative Process Trail

4.2. MITIGATING CIRCUMSTANCES

Circumstance	Illustrative Example	Observation	Percentage of Reduction
Cessation of infraction	After being alerted by the ANPD about excessive personal data collection without appropriate legal basis, an e-commerce company promptly stopped this practice. Instead of continuing to collect sensitive data like gender and ethnicity, which were deemed excessive for its activities, the company revised its data collection process to include only data necessary for completing sales. The change was immediately communicated to the ANPD, leading to the quick cessation of the infraction.	**prior** to the initiation of the preparatory procedure by the ANPDD	75%
		after the initiation of the preparatory procedure and up to the initiation of the administrative sanctioning process	50%
		after the initiation of the administrative sanctioning process and **up to** the issuance of the first-instance decision within the administrative sanctioning process	30%
Implementation of best practices and governance policies or demonstrated and repeated adoption of internal mechanisms and procedures capable of minimizing harm to data subjects	After a security incident where client data was compromised due to inadequate internal policies, an insurance company completely overhauled its data governance approach. It introduced a new governance structure, including the creation of a privacy committee, establishment of detailed information security policies, and regular employee training. The company also implemented an incident response and risk management system, demonstrating its commitment to robust data protection practices.	**up to** the issuance of the first-instance decision within the administrative sanctioning process	20%

Proven implementation of measures to reverse or mitigate the effects of the infraction on data subjects	In response to a data breach exposing users' banking information, a fintech acted swiftly. In addition to strengthening its security measures with advanced encryption and two-factor authentication, the company offered free fraud protection monitoring services to affected data subjects. These actions significantly mitigated potential damages such as fraud or financial loss.	**prior to** the initiation of the preparatory procedure or administrative sanctioning process by the ANPD	20%
		after the initiation of the preparatory procedure and up to the initiation of the administrative sanctioning process	10%
Verification of cooperation or good faith by the offender	A university was informed that a flaw in its online registration system had exposed personal data of applicants. Demonstrating readiness, the institution immediately cooperated with the ANPD by providing complete records of the breach and implementing technical corrections to the system. Additionally, it proactively notified affected applicants, offering legal and administrative support, thereby proving its good faith in handling the incident.	-	5%

Considering the circumstances outlined in the Regulation on Dosimetry and Application of Administrative Sanctions is essential for data controllers not only to avoid sanctions and reduce fine costs but also to foster a culture of responsibility and data protection.

The prompt cessation of infractions, the implementation of robust good practices and governance policies, the adoption of effective measures to mitigate the effects of incidents, and the demonstration of cooperation and good faith with authorities reflect a genuine commitment to personal data security.

In addition to ensuring compliance and enhancing the trust of data subjects, these actions can lead to a significant reduction in financial penalties, contributing to integrity and resilience in an increasingly demanding regulatory environment.

b/luz

deixa com a gente

Para saber mais, acesse nosso site ou
nos acompanhe nas redes sociais.

baptistaluz.com.br