Machine Translated by Google
RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 06/11/2026 | Accepted: 11/11/2026 | Publication: 16/11/2026

From formal compliance to effective protection: privacy by design, third-party management, and the decoupling of norms and practice in personal data protection.

From formal compliance to effective protection: privacy by design, third-party management and the decoupling between law and practice in personal data protection

From formal compliance to effective protection: privacy from design, management of third parties and the decoupling between norms and practices in the protection of personal data

Cassiano Rodolfo Jung
Master's student in Cybersecurity at American Global Tech University (AGTU). Specialist in Open Source Intelligence and Investigation (OSINT) from WB Educação. Specialist in Computer Forensics and Information Security from the Institute of Postgraduate and Undergraduate Studies (IPOG). Specialist in Strategic Management of Information Technology from Estácio de Sá University. Technologist in Information Security from the University of Vale do Rio dos Sinos (UNISINOS).

SUMMARY

The proliferation of personal data protection laws, such as the General Data Protection Law in Brazil and the General Data Protection Regulation in the European Union, has not been accompanied by a proportional reduction in incidents that expose the information of clients, patients, and consumers. This article investigates the gap between formal compliance, expressed in policies, records, and contracts, and the effective protection of data in the technological environment of organizations. The research, with a qualitative approach and exploratory and descriptive character, combines a narrative review of legal, organizational, and privacy engineering literature with documentary analysis of legislation, technical standards, sectoral reports, official statements, and decisions of data protection authorities in Brazil, the European Union, and the United States. The analysis indicates that compliance tends to become decoupled from practice when treated as the production of documents, and that the most recurrent failures in the cases examined involve basic technical controls, lack of knowledge of their own data flows, and insufficient third-party supervision. The most recent sanctioning decisions have begun to examine the architecture of systems, and not just the existence of documents. It is concluded that effective protection depends on translating legal obligations into engineering requirements, up-to-date inventories, and verifiable controls throughout the supply chain.

Keywords: Personal data protection. Regulatory compliance. Privacy by design. Third-party risk management. LGPD (Brazilian General Data Protection Law).

ABSTRACT

The proliferation of personal data protection laws, such as Brazil's General Data Protection Law and the European Union's General Data Protection Regulation, has not been matched by a proportional reduction in incidents that expose the information of customers, patients and consumers. This article examines the gap between formal compliance, expressed in policies, records and contracts, and the effective protection of data within organizations' technological environments. The study follows a qualitative, exploratory and descriptive approach, combining a narrative review of legal, organizational and privacy engineering literature with documentary analysis of legislation, technical standards, industry reports, official testimony and decisions issued by data protection authorities in Brazil, the European Union and the United States. The analysis indicates that compliance tends to decouple from practice when it is treated as the production of documents, and that the most recurrent failures in the cases examined involve basic technical controls, limited knowledge of the organization's own data flows and insufficient oversight of third parties. Recent enforcement decisions have begun to scrutinize system architecture rather than merely the existence of documents.

The study concludes that effective protection depends on translating legal obligations into

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 06/11/2026 | Accepted: 11/11/2026 | Publication: 16/11/2026

engineering requirements, up-to-date inventories and verifiable controls across the supply chain.

Keywords: Personal data protection. Regulatory compliance. Privacy by design. Third-party risk management. LGPD.

1 INTRODUCTION

The last decade has consolidated a cycle of regulatory expansion in the area of data protection.
Personal data. The European Union's General Data Protection Regulation has come into effect.
in May 2018 and served as a reference for several national laws, including Law No.
13.709/2018, the Brazilian General Data Protection Law (European Union, 2016; Brazil,
2018; Doneda, 2019). Brazilian law began requiring, among other measures, the indication of
responsible for the processing of personal data, maintaining a record of processing operations.
and the adoption of safety measures from the design of products and services (Brazil, 2018). This
The expansion of obligations, however, was not accompanied by a proportional reduction in incidents.
A Verizon report published in 2025 analyzed 12,195 confirmed data breaches, and the study
A study conducted by the Ponemon Institute for IBM estimated the average global cost of a breach at US$
4.88 million in 2024 (Verizon, 2025; IBM, 2024).
The coexistence of increased regulation and persistent exposure suggests that formal compliance and...
Effective protection does not always go hand in hand. Waldman (2020) argues that privacy laws
They risk failing when symbols of compliance, such as protocol training,
Audits and documentary records are now treated as if they were the very protection.
promised by law. Organizational literature has described a similar phenomenon for decades, showing
Which organizations can adopt formal structures to gain legitimacy in the environment?
institutional, without these structures actually altering their core activities (Meyer; Rowan, 1977).
The question guiding this work is how this distance manifests itself in the protection of
personal data and what factors contribute to reducing it.
The aim of this article is to analyze the mechanisms by which compliance with consumer protection laws...
Data protection can be dissociated from the effective protection of information, and identifying, from the literature, that
Technical standards and documented case studies outline the conditions that favor convergence between the two.
The text explores the theoretical foundations of decoupling norms from practice, the principle of...
Privacy by design and its translation into engineering, the role of data inventory, the
Technical security as a legal requirement, third-party management, and finally, what the decisions of
Regulatory authorities reveal details about how compliance is now being assessed. Attention.
Special consideration is given to the health and financial sectors, which process health data classified under the LGPD (Brazilian General Data Protection Law).
such as sensitive personal data and financial data, both subject to specific sectoral regulation.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 06/11/2026 | Accepted: 11/11/2026 | Publication: 16/11/2026

(Brazil, 2018).

2 METHODOLOGY

This is a qualitative research study with exploratory and descriptive objectives.
As proposed by Gil (2008), exploratory research seeks to provide a general overview and greater familiarity with a phenomenon that is still poorly systematized, while descriptive analysis deals with Characterization of phenomena and establishment of relationships between variables. The topic requires this. combination, since the distance between compliance and effective protection involves legal dimensions, organizational and technical aspects, and no standardized indicator was identified in the consulted literature that allow for its direct measurement. The methodological choice, therefore, prioritizes articulated interpretation. from sources of different natures.

The bibliographic procedure took the form of a narrative review, a modality that, according to Rother (2007), lends itself to the discussion of the state of the art of a topic from a theoretical or contextual perspective, without The need for systematic search and selection protocols. Three sets of literature were compiled.
The first encompasses legal and socio-legal studies on the application of privacy laws in organizations, such as those of Bamberger and Mulligan (2011), Edelman (2016), and Waldman (2020).
The second work brings together contributions from organizational theory on symbolic conformity and auditing.
The third category includes works of privacy engineering, such as those by Spiekermann and Cranor.
(2009) and Hoepman (2014). The works were identified through Google Scholar, from the portals from publishers and institutional repositories.
The document analysis considered Brazilian and European data protection legislation and resolutions. from the National Data Protection Authority and the National Monetary Council, publications techniques from the National Institute of Standards and Technology, standards from the International Organization for Standardization, guidelines from the European Data Protection Board and the EU Agency.
European Union for Cybersecurity and the proposed update to the security rule of North American legislation.
American healthcare. Industry reports published by IBM and Verizon were also examined.
a joint warning from US agencies, a report from the Government Accountability Office,
a testimony given to the United States Senate and sanctions decisions by the authority.
Irish data protection authority, the Office of the Comptroller of the Currency and the ANPD,
supplemented by journalistic reports used only for specific factual data.
The material was organized into six analytical axes, namely, the fundamentals of decoupling between Standard and practice, privacy by design, data inventory and minimization, security Technical expertise as a condition for compliance, third-party management, and oversight. Within each axis, the

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 06/11/2026 | Accepted: 11/11/2026 | Publication: 16/11/2026

Regulatory requirements were confronted with empirical evidence and concrete cases, in such a way to identify convergences and gaps. The main limitation of the study stems from the use of case studies. public events, which tend to involve large-scale incidents and therefore do not reflect necessarily the reality of smaller organizations. Data from industry reports, Produced with proprietary samples and methods, they are treated as indicators of trends.

3. Symbolic Conformity and the Decoupling Between Standard and PRACTICE

The theoretical starting point for understanding the gap between compliance and protection lies in in the sociology of organizations. Meyer and Rowan (1977) argued that organizations They incorporate formal structures, such as positions, programs, and procedures, largely because These structures are socially recognized as rational and legitimate, and not necessarily Because they increase their efficiency. When formal requirements conflict with the activity. In everyday life, organizations tend to maintain structures as a facade and decouple them from practices. effective. The concept of decoupling offers a useful reading key for data protection. a field in which policy adoption and the appointment of officials can coexist with practices.

Techniques have changed very little.

Edelman (2016), in studying the application of anti-discrimination laws in the United States, developed The concept of legal endogeneity to describe the process by which organizations create Symbolic structures of conformity, and over time, these structures become accepted by... The courts themselves serve as proof of compliance with the law. The meaning of the rule, in this process, is progressively shaped by the organizations it intended to regulate. The contribution is relevant. because it shifts the analysis from the simple question of whether the law is being obeyed to investigating how In practice, organizations define what compliance means and who participates in that definition. Waldman (2020) transposed this framework to the field of privacy. Based on interviews with engineers, privacy professionals, and executives from companies that provide solutions for In addition to analyzing product demonstrations and industry literature, the author argues that in compliance... that privacy laws risk failing because compliance symbols, such as Training programs without practical effect, audits, and document trails are becoming confused with... real adherence to the law. In a later work, Waldman (2021) further analyzed how routines Internal practices within technology companies influence the interpretation of privacy obligations. The problem pointed out by the author, therefore, does not lie in the existence of documents, but in the possibility. that they be taken as substitutes for royal protection.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 06/11/2026 | Accepted: 11/11/2026 | Publication: 16/11/2026

The literature is not unanimous regarding the scope of this diagnosis. Bamberger and Mulligan (2011), in study based on interviews with privacy directors identified by their peers as Industry experts identified that some US companies had shifted their focus. from a procedure-centered approach, such as warning and consent, to a concern substantive with the prevention of violations of consumers' privacy expectations. Among the Among the factors associated with this change, the authors point to the actions of the Federal Trade Commission, the Market and press pressure, the professionalization of the field, and state notification laws incidents that have increased the cost of mismanagement of personal information.

Audit theory adds another layer to the problem. Power (1997) described the expansion of verification practices in contemporary societies and observed that auditing tends to evaluate the The existence of control systems, and not necessarily the substantive performance of the activities. that these systems should control. Applied to data protection, this diagnosis helps to explain why an organization might receive favorable evaluations regarding the existence of policies and records and yet still retain exploitable technical flaws. Taken together, the authors discussed in this The sections indicate that the effectiveness of compliance depends less on the quantity of documents. produced, and more importantly, the ability of these documents to alter technical and operational decisions.

4. PRIVACY BY DESIGN: FROM LEGAL PRINCIPLE TO ENGINEERING

The idea that data protection should be incorporated into systems from their inception, and not added at the end, it was systematized by Cavoukian (2009) into seven fundamental principles, among They emphasize proactive and preventative action, privacy as the default setting, and the incorporation of... Privacy in the design, full functionality, end-to-end security throughout the entire lifecycle. The lifeblood of information, visibility and transparency, and respect for user privacy. The conversion However, the application of these principles to concrete system requirements does not automatically follow from their statement. The report prepared for the European Cybersecurity Agency by Danezis *et al.* (2014) The goal was precisely to reduce the gap between the legal framework and the available technical measures. which indicates that this translation constitutes a problem of its own, requiring a specific method.

The General Data Protection Regulation has turned the principle into a legal obligation in Article 25, which requires the data controller to adopt technical and organizational measures. appropriate both at the time of defining the means of treatment and during the treatment itself. treatment, in addition to ensuring that, by default, only the data necessary for each purpose is processed. treaties (European Union, 2016). Brazilian legislation followed a similar orientation. Article 46 The LGPD (Brazilian General Data Protection Law) requires data processing agents to adopt security measures, both technical and...

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 06/11/2026 | Accepted: 11/11/2026 | Publication: 16/11/2026

administrative measures capable of protecting personal data, and paragraph 2 of that article stipulates that these measures should be observed from the product or service conception phase to its execution (Brazil, 2018).

The European Data Protection Committee's guidelines on Article 25 sought to reduce the The distance between the legal text and its application. The document clarifies that the obligation is directed to The effectiveness of the measures, and not their mere existence, is what matters, and the person responsible must be able to... demonstrate that the safeguards adopted produce the intended effects in relation to each principle. data protection (EDPB, 2020). This emphasis on effectiveness brings the legal obligation closer to Engineering concerns and dispels the interpretation that compliance with Article 25 could can only be achieved through the development of policies or contractual clauses.

The literature on privacy engineering offers tools for this translation. Spiekermann and Cranor (2009) distinguished two design approaches, one based on policies, which depends on warning, choice and compliance with rules by the person in charge, and another based on architecture, which It seeks to reduce the identifiability of data and limit its collection, making protection less effective. dependent on organizational behavior. Hoepman (2014) proposed eight design strategies. which allow privacy to be applied from the early stages of development, namely, minimizing, To conceal, separate, aggregate, inform, control, impose, and demonstrate. Strategies translate objectives. protection in concrete design choices, such as collecting only the necessary data or Separation of databases to make cross-referencing information more difficult.

The same report by Danezis *et al.* (2014) examined the state of the art of reinforcement technologies for privacy and noted that although these technologies have demonstrated their potential in Research and pilot projects, however, had not yet become a standard and widespread component. used in systems design, with the exception of cryptography, and proposed a method for relating the Legal obligations regarding design strategies. In terms of technical standards, ISO/IEC 27701, whose The 2025 edition began to be published as an independent standard for management systems. Privacy information, and the NIST Privacy Framework offer structures that allow convert legal obligations into verifiable organizational and technical controls (ISO, 2025; NIST, 2020).

5. UNDERSTANDING THE DATA TO PROTECT IT: INVENTORY, MINIMIZATION AND UNMANAGED DATA

No controls can be applied to data whose existence the organization is unaware of. For this reason, Data protection laws assign a central role to the recording of data processing operations. The article

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 06/11/2026 | Accepted: 11/11/2026 | Publication: 16/11/2026

Article 37 of the LGPD (Brazilian General Data Protection Law) stipulates that the controller and operator must maintain a record of the operations they perform.
and Article 30 of the European regulation establishes an equivalent obligation, detailing the
purposes, categories of data subjects and data subjects, recipients and, whenever possible, timeframes
planned for elimination and the security measures adopted (Brazil, 2018; European Union, 2016).
From this perspective, registration is not merely a documentary requirement, but the starting point for...
risk assessment and definition of controls.

The NIST Privacy Framework gives this inventory an operational dimension. The function
Identifying the model includes inventorying and mapping the systems, products, and services that it addresses.
data, from the owners or operators of these systems, of the categories of individuals whose data is
treated and the processing actions performed at each stage of the information lifecycle (NIST,
(2020). This mapping guides the other functions of the model, such as governing, controlling, and communicating.
and protect, and makes explicit the dependency between knowing the data flows and being able to manage them.
risks that they produce. An outdated inventory, therefore, compromises all decisions that
They depend on him.

Empirical data shows that this dependence has concrete consequences. The IBM study
A 2024 study recorded that 35% of the violations analyzed involved unmanaged data, also
so-called shadow data, that is, information stored outside of controlled environments and
inventoried by the organization (IBM, 2024). According to the same report, the violations that
Studies involving this type of data had an average cost 16% higher and required more time to complete.
identified and contained, and approximately 40% of the breaches involved data distributed across multiple networks.
environments, such as public clouds, private clouds, and local infrastructure. The fragmentation of
These environments tend to increase the likelihood that copies of data will escape formal inventory.

Data minimization is the counterpart to inventory. Article 6 of the LGPD establishes the principle of...
necessity, which limits treatment to the minimum necessary to achieve its purposes,
with coverage of relevant, proportionate and non-excessive data (Brazil, 2018). From the point of view of
From a security perspective, minimization reduces the surface area exposed, since data that was not
Collected or already eliminated assets cannot be subtracted in an incident. The strategy of
To minimize, the first of the proposals by Hoepman (2014), stems precisely from this reasoning.
European regulations clarify the scope of this obligation by specifying, in paragraph 2 of Article 25,
that the default protection applies to the amount of data collected, the extent of the processing, and the
data retention period and accessibility (European Union, 2016).

In Brazilian doctrine, Bioni (2019) examines the function and limits of consent as
protection instrument, considering the asymmetry between holders and organizations, and discusses the
The need for mechanisms that do not depend exclusively on the individual choice of the data subject.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Year VII, v.2 2026 | Submission: 06/11/2026 | Accepted: 11/11/2026 | Publication: 16/11/2026

Doneda (2019), in reconstructing the formation of the LGPD, defends the recognition of data protection.
Personal rights as a fundamental right and examines the centrality of principles in the regulatory model.
adopted by law. Read together with the technical literature, these contributions reinforce that the
Inventory and minimization are material duties of data controllers, not mere formalities.
accessories.

6. TECHNICAL SAFETY AS A CONDITION OF CONFORMITY

The LGPD (Brazilian General Data Protection Law) does not treat information security as a separate issue from data protection. In addition to...
In addition to the general duty stipulated in Article 46, Article 44 considers treatment that fails to be irregular.
the security that its holder can expect, considering circumstances such as the manner in which it is
realized, the result and the reasonably expected risks, and the techniques available at the time, and the
The sole paragraph of the same article assigns responsibility for damages resulting from the violation of
data security is at risk for the controller or operator who, by failing to adopt the measures provided for in
Article 46, causes the damage (Brazil, 2018). Compliance, in this legal framework, includes
necessarily depends on the quality of the technical controls actually implemented.
The case of Equifax, a US credit reporting company, illustrates how failures in
Security controls can lead to large-scale exposure. According to the report...
According to the Government Accountability Office regarding the 2017 incident, the attackers gained access through...
The internet, a consumer complaint portal, and obtained personal data from at least
145.5 million people (United States, 2018). The investigation, conducted by the company itself,
as reported in the document, the incident was attributed to failures in four areas, the identification of
vulnerabilities, intrusion detection, database access segmentation, and governance
data. These are areas covered by security controls that are widely described in the literature.
technically, the problem lies more in the application of these controls than in the unavailability of
solutions.
In the healthcare sector, the attack targeted Change Healthcare, a healthcare transaction processing company.
controlled by UnitedHealth Group, offers another example of this dynamic. In testimony to
US Senate Finance Committee, on May 1, 2024, the CEO of
The group stated that the criminals accessed a company portal that was not protected by
Using multifactor authentication, they extracted data and deployed *ransomware* on February 21 of that year.
and confirmed the payment of a $22 million rescue (Witty, 2024). In January 2025, the company
It was estimated that around 190 million people were affected (Fierce Healthcare, 2025).
The security rule of the Health Insurance Portability and Accountability Act distinguishes specific requirements.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 06/11/2026 | Accepted: 11/11/2026 | Publication: 16/11/2026

mandatory implementation and specifications classified as addressable. According to the author himself
Department of Health and Human Services, none of them were optional, but the designation allowed
that each entity should assess whether the measure was reasonable and appropriate in its environment, with the objective
to provide greater flexibility (United States, 2025). In January 2025, the department published
The proposed update to this rule is motivated, according to its preamble, among other factors, by the strong
The increase in reported health data breaches between 2018 and 2023. The proposal eliminates
This distinction makes encryption of health data at rest and in transit mandatory, and
Multifactor authentication is now required, along with a written inventory of technological assets and a network map.
(United States, 2025).
The same proposal includes the obligation to restore critical systems and data within 72 hours of a failure.
loss, of conducting compliance audits at least every twelve months and of obtaining, with the same
periodicity, written verification that business partners have implemented the safeguards.
required techniques (United States, 2025). In the case of cryptography, the proposal text itself explains
that the change would relieve entities from assessing whether the measure is reasonable and appropriate, which expresses
The replacement of case-by-case assessments with verifiable requirements. This example is relevant to...
Brazilian debate, as it indicates that, even in a consolidated regulatory system, the regulator has passed
to consider it necessary to explicitly specify basic controls, instead of relying solely on
General safety obligations subject to assessment by each entity.

7. Third Parties and the Supply Chain as a Vector of Exposure

The growing dependence on technology vendors shifts a significant portion of the risk away from the company.
organizational boundaries. Verizon's 2025 report noted that third-party participation
The number of violations analyzed doubled compared to the previous year, reaching 30% of cases (Verizon,
2025). This data indicates that the effective protection of an organization's data depends, to a certain extent...
considerable, from the practices of their service providers, and that limited approaches to controls
Internal data tends to leave a significant portion of the risk untreated. For this reason, both the LGPD and
European regulations expressly govern the relationship between those who decide on the treatment and
who executes it.
The LGPD establishes that the operator must carry out the processing according to the instructions provided by...
controller, it being their responsibility to verify compliance with their own instructions and the rules regarding the
matter, according to article 39 (Brazil, 2018). Article 42, in turn, provides that the operator is responsible.
jointly liable for damages caused when failing to comply with legal obligations or not following the rules.
lawful instructions from the controller. In the European regulation, Article 28 requires the controller to resort to

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 06/11/2026 | Accepted: 11/11/2026 | Publication: 16/11/2026

only to subcontractors that provide sufficient guarantees of implementing technical measures and adequate organizational structure and details the minimum content of the contract governing this relationship (Union). European, 2016).

The MOVEit Transfer case demonstrated the scale a single provider can achieve. According to a warning... joint Federal Bureau of Investigation and the Cybersecurity and Infrastructure Security Agency, Starting on May 27, 2023, the criminal group known as CL0P began exploiting a A previously unknown SQL injection vulnerability, cataloged as CVE-2023-34362, in this managed file transfer software, installing a *web shell* called LEMURLOOT in applications exposed to the internet and extracting data from their databases (FBI; CISA, 2023). By enabling the transfer of files between organizations, clients, and partners, the tool allowed the exploitation of a single vulnerability to simultaneously expose data from multiple organizations.

Technical publications recommend that third-party management be treated as an ongoing process. and not as a one-off check performed at the time of hiring. The NIST guide on management The cybersecurity risk assessment framework for the supply chain, developed by Boyens *et al.* (2022), guides the organizations are integrating these risks into corporate risk management and defining security requirements. in contracts, to assess the criticality of each supplier and to monitor their performance over time. The entire relationship. The proposal to update the safety rule in US legislation of health, by requiring annual written verification of safeguards from business partners, applies this same logic of periodic supervision (United States, 2025).

In the Brazilian financial system, CMN Resolution No. 4,893/2021 established requirements for... cybersecurity policy of institutions authorized to operate by the Central Bank and for the contracting services for data processing, storage, and cloud computing. (National Monetary Council, 2021). The rule was amended by CMN Resolution No. 5,274/2025, which It began to require, among other things, the verification of controls for acquired systems or Developed by service providers, multifactor authentication for access to the corporate network. starting from external environments and intrusion tests with a minimum annual frequency (Council) National Monetary Policy, 2025). The progressive detailing of the required controls brings regulation closer. sectorial logic of verifiable requirements.

8. INSPECTION AND SANCTIONS: WHAT THE DECISIONS REVEAL ABOUT DISTANCE Between Norm and Practice

The decisions of regulatory authorities constitute a privileged source for observing how the

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 06/11/2026 | Accepted: 11/11/2026 | Publication: 16/11/2026

Compliance is assessed in practice. In Brazil, the first monetary penalty applied by the ANPD,
Published in July 2023, it targeted a micro-enterprise, Telekall Infoservice, with a warning and
A total fine of R$ 14,400 was imposed for violating Article 7 of the LGPD (Brazilian General Data Protection Law), relating to the legal hypotheses of...
treatment, and to article 5 of the Inspection Regulations, which establishes the duties of the agents.
regulated before the authority (Mobile Time, 2023). The process had been initiated in 2022, and the
The list of findings released by the authority also mentioned the absence of records for the operations.
and of the person in charge, which shows that, in this first case, there are basic deficiencies in the legal basis and of
Documentation occupied a central position.

The Regulation on Dosing and Application of Administrative Sanctions, approved by Resolution
CD/ANPD No. 4/2023 classifies infractions as minor, moderate, and serious and provides for circumstances.
mitigating and aggravating factors for calculating fines (ANPD, 2023). Among the mitigating factors are...
implementation of a policy of good practices and governance, or the repeated and proven adoption of
Internal mechanisms capable of minimizing harm to data subjects, and the adoption of measures to reverse
or mitigate the effects of the infraction. The second hypothesis requires that the internal mechanisms be
adopted repeatedly and demonstrably, which indicates attention to their effective application, and not just
to its formal forecast.

In the European Union, recent decisions by the Irish data protection authority have examined
directly to the architecture of the systems. In November 2022, the authority applied to Meta Platforms
Ireland fines totaling 265 million euros for violations of paragraphs 1 and 2 of Article 25 of the
regulation, due to the processing carried out through search and import tools of
Facebook and Instagram contacts, exploited for data scraping (Data Protection).
Commission, 2022). In December 2024, a new decision imposed related fines of €251 million.
of a 2018 violation, of which 240 million corresponded to violations of Article 25 and the 11
millions remaining, due to failures in notification and documentation of the breach (Data Protection)
Commission, 2024).

The 2024 decision describes how the combination of platform functionalities allowed for the generation
a failure involving an access credential, called *a token,* that grants full access to another user's profile.
exploited between September 14 and 28, 2018, and affecting approximately 29 million accounts worldwide,
of which approximately 3 million are in the European Union and the European Economic Area (Data
Protection Commission, 2024). In the United States, the Office of the Comptroller of the Currency
In 2020, it imposed an $80 million fine on Capital One for failing to establish effective processes.
risk assessment before migrating relevant technology operations to the public cloud and by
not having promptly corrected the identified deficiencies (Office of the Comptroller of the
(Currency, 2020). Table 1 summarizes these cases.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 06/11/2026 | Accepted: 11/11/2026 | Publication: 16/11/2026

Table 1 – Selected cases of sanctions related to data protection and security.

information

Organization	Authority and year	Sanction	Main principle
Telekall Infoservice (Brazil)	ANPD, 2023	Warning and fine of R$ 14,400	Article 7 of the LGPD and Article 5 of the Inspection Regulation
Capital One (United States)	OCC, 2020	US$ 80 million	Lack of effective risk assessment prior to migrating to the public cloud.
Meta Platforms Ireland (data scraping)	DPC, 2022	€265 million	Art. 25(1) and 25(2) of the GDPR, protection by design and by default
Meta Platforms Ireland (2018 violation)	DPC, 2024	€251 million	Art. 25(1) and 25(2) of the GDPR (€240 million) and art. 33(3) and 33(5) (€11 million)

Source: compiled by the author based on Mobile Time (2023), Office of the Comptroller of the Currency (2020) and Data Protection Commission (2022; 2024).

The cases compiled in Table 1 differ in terms of jurisdictions, business sizes, and...
legal foundations, which prevents direct quantitative comparisons between the sanctions. Its
The analytical contribution therefore lies not in the magnitude of the fines, but in the criteria used by the
authorities to assess compliance. In European and North American decisions, the rationale
It focuses on the absence of built-in protection in the systems' design or on the insufficiency of
Risk assessment prior to technological decisions. In the 2024 decision, the infringements relating to
Notification and documentation represented a minority portion of the fine, reinforcing, in this case, the
centrality of material protection failures. These elements suggest a supervisory orientation.
focused on verifying how legal obligations materialize in architectural choices and
management practices. From this perspective, policies, records, and procedures do not lose their
Relevance, but they need to demonstrate a link to the controls that have actually been implemented. A
Distinction is central to the debate on symbolic conformity: the existence of formal structures does not
This, in itself, is equivalent to protecting the holders. However, the heterogeneity and limited number of
These cases do not allow us to affirm a uniform trajectory of regulatory maturation; they allow us to...
to identify, in the decisions examined, signs of a more substantive assessment of the relationship between norms.
and practice.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 06/11/2026 | Accepted: 11/11/2026 | Publication: 16/11/2026

9 CONCLUSION

This article examined the gap between formal compliance with data protection laws and the Effective protection of personal information. The organizational and socio-legal literature discussed. This allows us to understand this distance not only as an individual deviation of negligent organizations, but also as a structural trend, associated with the adoption of formal structures in search of legitimacy and the possibility of these structures becoming decoupled from technical practices. The concept Legal endogeneity and its application to the field of privacy offer tools for to identify when compliance documents cease to guide decisions and begin to replace them. them.

The literature also shows that this outcome is not inevitable. The study by Bamberger and Mulligan, Based on interviews with privacy directors, it identified organizations that have shifted their focus. of formal procedures for the substantive prevention of harm, driven by the actions of Regulators, due to market pressure and the professionalization of the area. This indicates that the environment Regulatory and institutional factors influence the direction that compliance takes within organizations. and that results-oriented oversight mechanisms can promote convergence between Standard and practice.

Privacy by design, as provided for in Article 25 of the European regulation and in paragraph 2 of the Article 46 of the LGPD constitutes a central legal instrument for this convergence, provided that interpreted as an obligation of effectiveness. European guidelines on the subject and the literature on Privacy engineering approaches converge on the point that protection needs to be converted into requirements. of the system, such as data collection minimization, base separation, and protective configurations by Standard, and that generic principles, by themselves, do not alter the architecture of applications.

The data inventory proved to be a prerequisite for any control. The proportion of violations that The data involved unmanaged information, recorded in IBM's 2024 study, shows that the registration of The data processing operations required by the LGPD only fulfill their function when they reflect the real environment. including copies and repositories created outside of formal processes. Minimization, by reducing the The volume of information maintained complements the inventory and reduces exposure in case of... incident, which also makes it a safety measure.

The Equifax and Change Healthcare cases demonstrate failures in technical controls. widely known techniques, such as vulnerability identification and segmentation of database access. Data breaches and multifactor authentication can lead to exposures of tens or hundreds of millions. of people in large organizations, subject to extensive sectoral regulation. The proposal of An update to the US healthcare safety rule, making controls mandatory.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
IRCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 06/11/2026 | Accepted: 11/11/2026 | Publication: 16/11/2026

previously subject to discretionary assessment by the entities, indicates that the US regulator of
The health sector has begun to prefer explicit requirements to generic safety obligations subject to evaluation.
of each entity.

Third-party management has emerged as a crucial dimension. The increased participation of suppliers
The violations and mass exploitation of a single file transfer software suggest
that contractual compliance, limited to clauses and questionnaires applied during contracting, tends to
failing to keep pace with the dynamics of risk. The most recent technical guidelines and sector standards,
Even within the Brazilian financial system, these factors point to continuous supervision and verification.
of the controls effectively implemented by the providers.

The sanctioning cases examined suggest that oversight tends to evolve from verification.
Documentary information for examining the architecture of the systems and the quality of risk assessments.
In Brazil, the ANPD's actions are still in the consolidation phase, but the regulation of
The sentencing guidelines already include, among the mitigating factors, the repeated and proven adoption of internal mechanisms of
harm minimization. This guideline, if maintained, may contribute to reducing the incentive to
Compliance is merely symbolic, and investments in verifiable controls should be encouraged.
One limitation is that the cases analyzed are mostly large-scale and...
foreign jurisdictions, which restricts the generalization of the conclusions to Brazilian organizations.
smaller scale. For future studies, it is recommended to conduct empirical research with
national organizations that compare the documentary maturity of their privacy programs
with technical protection indicators, as well as the systematic analysis of ANPD decisions to
as its administrative jurisprudence becomes consolidated. Such studies would allow us to verify in what ways.
The extent to which the disconnect between norm and practice manifests itself in the Brazilian context.

REFERENCES

NATIONAL DATA PROTECTION AUTHORITY (ANPD). **Resolution CD/ANPD No. 4, of February 24, 2023.** Approves the Regulation on Dosimetry and Application of Administrative Sanctions. Brasília, DF: ANPD, 2023.

BAMBERGER, Kenneth A.; MULLIGAN, Deirdre K. Privacy on the books and on the ground. **Stanford Law Review,** Stanford, vol. 63, no. 2, p. 247, 2011.

BIONI, Bruno Ricardo. **Personal data protection:** the function and limits of consent. Rio de Janeiro: Forense, 2019.

BOYENS, Jon; SMITH, Angela; BARTOL, Nadya; WINKLER, Kris; HOLBROOK, Alexander; FALLON, Matthew. **Cybersecurity supply chain risk management practices for systems and organizations.** Gaithersburg: National Institute of Standards and Technology, 2022. (NIST Special Publication 800-161, rev. 1). DOI: 10.6028/NIST.SP.800-161r1.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Year VII, v.2 2026 | Submission: 06/11/2026 | Accepted: 11/11/2026 | Publication: 16/11/2026

BRAZIL. **Law No. 13.709, of August 14, 2018.** General Law on the Protection of Personal Data (LGPD). Brasilia, DF: Presidency of the Republic, 2018.

CAVOUKIAN, Ann. **Privacy by design:** the 7 foundational principles. Toronto: Information and Privacy Commissioner of Ontario, 2009.

NATIONAL MONETARY COUNCIL (Brazil). **CMN Resolution No. 4,893, of February 26, 2021.** Establishes the cybersecurity policy and the requirements for contracting data processing and storage services and cloud computing. Brasília, DF: Central Bank of Brazil, 2021.

NATIONAL MONETARY COUNCIL (Brazil). **CMN Resolution No. 5,274, of December 18, 2025.** Amends CMN Resolution No. 4,893, of February 26, 2021. Brasília, DF: Central Bank of Brazil, 2025.

DANEZIS, George; DOMINGO-FERRER, Josep; HANSEN, Marit; HOEPMAN, Jaap-Henk; LE MÉTAYER, Daniel; TIRTEA, Rodica; SCHIFFNER, Stefan. **Privacy and data protection by design:** from policy to engineering. Heraklion: European Union Agency for Network and Information Security (ENISA), 2014.

DATA PROTECTION COMMISSION (Ireland). **Data Protection Commission announces decision in Facebook "Data Scraping" inquiry.** Dublin: DPC, 28 Nov. 2022.

DATA PROTECTION COMMISSION (Ireland). **Irish Data Protection Commission fines Target €251 million.** Dublin: DPC, 17 Dec. 2024.

DONEDA, Danilo. **From privacy to the protection of personal data:** elements of the formation of the General Data Protection Law. 2nd ed. São Paulo: Thomson Reuters Brasil, 2019.

EDELMAN, Lauren B. **Working law:** courts, corporations, and symbolic civil rights. Chicago: University of Chicago Press, 2016.

EUROPEAN DATA PROTECTION BOARD (EDPB). **Guidelines 4/2019 on Article 25:** data protection by design and by default. Version 2.0. Brussels: EDPB, 2020.

FEDERAL BUREAU OF INVESTIGATION (FBI); CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA). **#StopRansomware:** CL0P ransomware gang exploits CVE-2023-34362 MOVEit vulnerability. Washington, DC: CISA, 2023. (Cybersecurity Advisory AA23-158A).

FIERCE HEALTHCARE. UnitedHealth estimates 190M people impacted by Change Healthcare cyberattack. **Fierce Healthcare,** [S. l.], 24 Jan. 2025.

GIL, Antonio Carlos. **Methods and techniques of social research.** 6th ed. São Paulo: Atlas, 2008.

HOEPMAN, Jaap-Henk. Privacy design strategies. In: IFIP INTERNATIONAL INFORMATION SECURITY CONFERENCE, 29., 2014, Marrakech. **ICT Systems Security and Privacy Protection.** Berlin: Springer, 2014. p. 446-459. DOI: 10.1007/978-3-642-55415-5_38.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Year VII, v.2 2026 | Submission: 06/11/2026 | Accepted: 11/11/2026 | Publication: 16/11/2026

IBM. **Cost of a data breach report 2024.** Armonk: IBM Corporation, 2024.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO/IEC 27701:** information security, cybersecurity and privacy protection, privacy information management systems, requirements and guidance. Geneva: ISO, 2025.

MEYER, John W.; ROWAN, Brian. Institutionalized organizations: formal structure as myth and ceremony. **American Journal of Sociology,** Chicago, vol. 83, no. 2, p. 340-363, 1977.

MOBILE TIME. ANPD applies its first sanction with a fine to Telekall. **Mobile Time,** São Paulo, July 6, 2023.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **NIST Privacy Framework:** a tool for improving privacy through enterprise risk management. Version 1.0. Gaithersburg: NIST, 2020.

OFFICE OF THE COMPTROLLER OF THE CURRENCY (United States). **OCC assesses $80 million civil money penalty against Capital One.** Washington, DC: OCC, 6 Aug. 2020. (News Release 2020-101).

POWER, Michael. **The audit society:** rituals of verification. Oxford: Oxford University Press, 1997.

ROTHER, Edna Terezinha. Systematic review vs. narrative review. **Acta Paulista de Enfermagem,** São Paulo, v. 20, n. 2, p. v-vi, 2007.

SPIEKERMANN, Sarah; CRANOR, Lorrie Faith. Engineering privacy. **IEEE Transactions on Software Engineering,** [New York], v. 35, no. 1, p. 67-82, 2009.

EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. **Official Journal of the European Union,** Luxembourg, L 119, p. 1-88, 4 May 2016.

UNITED STATES. Government Accountability Office. **Data protection:** actions taken by Equifax and federal agencies in response to the 2017 breach. Washington, DC: GAO, 2018. (GAO-18-559).

UNITED STATES. Department of Health and Human Services. HIPAA Security Rule to strengthen the cybersecurity of electronic protected health information: proposed rule. **Federal Register,** Washington, DC, vol. 90, no. 3, p. 898-1022, 6 Jan. 2025.

VERIZON. **2025 data breach investigations report.** Basking Ridge: Verizon Business, 2025.

WALDMAN, Ari Ezra. Privacy law's false promise. **Washington University Law Review,** St. Louis, vol. 97, no. 3, p. 773, 2020.

WALDMAN, Ari Ezra. **Industry unbound:** the inside story of privacy, data, and corporate power. Cambridge: Cambridge University Press, 2021.

WITTY, Andrew. **Testimony before the United States Senate Committee on Finance:** hacking America's health care, assessing the Changing Healthcare cyberattack and what's next. washington,

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 06/11/2026 | Accepted: 11/11/2026 | Publication: 16/11/2026

DC: US Senate, May 1, 2024.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.