Legal Framework Analysis: A Comparative Study of GDPR and LGPD

Carlos Barbosa

Miami Dade College - North Campus

Ethics in Cybersecurity

Dr. Johnny Guimaraes

April, 2025

1 Introduction

Data privacy has become a critical concern worldwide, leading to the enactment of comprehensive data protection laws in various jurisdictions. Two landmark regulations in this paper are the European Union's General Data Protection Regulation (GDPR) and Brazil's Lei Geral de Proteção de Dados (LGPD). The GDPR, effective since May 2018, set a global standard for personal data protection and inspired many countries to strengthen their privacy frameworks (TermsFeed, n.d.). Brazil's LGPD, which came into force in 2020, was largely modeled on the GDPR to protect Brazilian individuals' data and facilitate international data exchanges (TermsFeed, n.d.).

This paper provides a detailed comparative analysis of the GDPR and the LGPD. It first offers an overview of each regulation's objectives, scope, key principles, data subject rights, and penalties. It then presents a comparison table highlighting their similarities and differences in key areas. The impact of each law on data-protection practices is examined, focusing on how they strengthen individual rights and impose obligations on organizations, particularly in terms of consent, adherence to data-processing principles, and requirements for cross-border data transfers. The paper also discusses the responsibilities of cybersecurity professionals under each law, especially regarding compliance, security measures, and handling data breaches. A contrasts the safeguards that each regulation requires for data at rest and data in transit, clarifying how technical and organizational measures must protect personal information throughout its life cycle. Recent enforcement cases under both the GDPR and LGPD are reviewed to illustrate how these regulations are applied in practice and to draw lessons for organizations.

2 Overview of Each Regulation

2.1 GDPR Overview

2.1.1 Objectives & Scope. The GDPR's primary objective is to protect the fundamental rights and privacy of individuals in the European Union (EU) and European Economic Area (EEA) with respect to their personal data (Privacy.unc.edu, n.d.–a). It seeks to harmonize data protection laws across EU member states and give individuals greater control over their personal information (Privacy.unc.edu, n.d.–b). GDPR applies not only to organizations established in the EU/EEA but also to those outside the region that offer goods or services to, or monitor the behavior of, individuals in the EU/EEA, reflecting its extraterritorial scope (Privacy.unc.edu, n.d.–b).

2.1.2 Key Principles. The GDPR is built upon seven key principles of data processing, which form the framework for compliance (Privacy.unc.edu, n.d.–b):

- **Lawfulness, Fairness, and Transparency:** Personal data must be processed lawfully, fairly, and in a transparent manner.
- **Purpose Limitation:** Data should be collected for specified, explicit and legitimate purposes.
- **Data Minimization:** Only the minimum data necessary for the purpose should be collected.
- **Accuracy:** Personal data should be accurate and kept up to date.
- **Storage Limitation:** Personal data should be kept in an identifiable form only as long as necessary.
- **Integrity and Confidentiality:** Appropriate security measures must be applied to protect data against unauthorized access or disclosure, and against accidental loss or destruction.

- **Accountability:** Data controllers are responsible for compliance and must demonstrate adherence to these principles.

2.1.3 Legal Bases for Processing. In line with the above principles, the GDPR requires that all processing of personal data have a valid legal basis. The regulation provides six lawful bases: consent of the data subject, necessity for the performance of a contract, compliance with a legal obligation, protection of vital interests, performance of a task in the public interest, and legitimate interests (Privacy.unc.edu, n.d.–b). When relying on consent, it must be informed, freely given, specific, and unambiguous, and data subjects can withdraw consent at any time (Usercentrics, n.d.).

2.1.4 Data Subject Rights. The GDPR grants individuals a robust set of rights over their personal data (Privacy.unc.edu, n.d.–b):

- **Right to be Informed:** Clear and transparent information about data collection and use.
- **Right of Access:** The ability to request confirmation of processing and access to personal data.
- **Right to Rectification:** The ability to correct inaccurate or incomplete data.
- **Right to Erasure:** The "right to be forgotten," allowing data deletion under certain circumstances.
- **Right to Restrict Processing:** The ability to limit processing in specific situations.
- **Right to Data Portability:** The ability to obtain personal data in a machine-readable format and transmit it elsewhere.
- **Right to Object:** The ability to object to certain types of processing, including direct marketing.

- **Rights related to Automated Decision-Making:** The right not to be subject to decisions based solely on automated processing when it significantly affects the individual.

2.1.5 Security and Breach Notification. The GDPR obliges organizations to implement "appropriate technical and organizational measures" to secure personal data, such as encryption, pseudonymization, and access controls (Privacy.unc.edu, n.d.–b). In the event of a personal data breach, data controllers must notify the relevant supervisory authority within 72 hours unless the breach is unlikely to result in risk to individuals (Privacy.unc.edu, n.d.–b; UpGuard, n.d.).

2.1.6 Enforcement and Penalties. GDPR is enforced by independent Data Protection Authorities (DPAs) in each EU member state, coordinated by the European Data Protection Board (EDPB). Fines can reach up to €20 million or 4% of the organization's worldwide annual turnover, whichever is higher (UpGuard, n.d.). For less severe violations, fines can be up to €10 million or 2% of turnover.

2.2 LGPD Overview

2.2.1 Objectives & Scope. Brazil's General Data Protection Law (Lei Geral de Proteção de Dados, LGPD) was enacted to protect the personal data and privacy of individuals in Brazil and to regulate data processing in line with fundamental rights (TermsFeed, n.d.). It applies to any processing operation carried out in Brazil, or involving personal data of individuals located in Brazil, or aimed at offering goods/services to people in Brazil (TermsFeed, n.d.), mirroring the GDPR's extraterritorial approach.

2.2.2 Key Principles. LGPD sets out ten fundamental principles that guide all personal data processing (OneTrust, 2020; TermsFeed, n.d.):

- Purpose

- Adequacy (Suitability)
- Necessity
- Free Access
- Data Quality
- Transparency
- Security
- Prevention
- Non-Discrimination
- Accountability

2.2.3 Legal Bases for Processing. LGPD Article 7 provides ten legal bases for processing personal data, encompassing all those in GDPR plus additional ones for research, legal proceedings, health protection, and credit protection (UpGuard, n.d.). Consent, when used, must be free, informed, and specific; it can be withdrawn at any time (Usercentrics, n.d.).

2.2.4 Data Subject Rights. LGPD grants rights similar to GDPR, including (Terms-Feed, n.d.):

- Confirmation of Processing
- Access
- Correction
- Anonymization, Blocking, or Deletion of Unnecessary or Unlawful Data
- Data Portability

- Deletion of Data Processed with Consent
- Information about Sharing
- Information about Consent Options and Consequences
- Withdrawal of Consent

Additionally, individuals can request a review of decisions made solely by automated means.

2.2.5 Security and Breach Notification. LGPD Article 46 explicitly requires data security measures to protect personal data from unauthorized access or incidents (IAPP, n.d.; UpGuard, n.d.). In the event of a breach that may result in risk or harm to data subjects, the controller must inform the ANPD (National Data Protection Authority) and, in some cases, the affected individuals within a "reasonable time period" (UpGuard, n.d.).

2.2.6 Enforcement and Penalties. The LGPD is enforced by ANPD (TermsFeed, n.d.). Sanctions include warnings, fines of up to 2% of a company's Brazilian revenue (capped at R$50 million), public disclosure of the infraction, deletion of data, and suspension of processing activities (TermsFeed, n.d.; Littler Mendelson PC, 2023).

3 Comparison of GDPR and LGPD

Table 1. *Comparison of GDPR and LGPD*

Aspect	**GDPR (EU)**	**LGPD (Brazil)**
Data-protection requirements	• Six lawful bases (consent, contract, legal obligation, vital interests, public interest, legitimate interests) (Privacy.unc.edu, n.d.–b) • Seven principles (lawfulness … accountability) • High-standard consent; easy withdrawal (Usercentrics, n.d.) • DPO mandatory in certain cases (Arts.37–39) • Detailed controller–processor contracts (OneTrust, 2020)	• Ten lawful bases (GDPR + research, legal proceedings, health, credit) (UpGuard, n.d.) • Ten principles (purpose … accountability) (OneTrust, 2020; TermsFeed, n.d.) • Comparable consent rules (Usercentrics, n.d.) • DPO (*encarregado*) generally required (Littler Mendelson PC, 2023) • Contract duties less prescriptive but recommended
Enforcement mechanisms	• National DPAs + EDPB coordination (European Data Protection Board, 2023) • Fines up to €20 million / 4 % global turnover • Individuals may seek judicial remedies	• ANPD (federal) (TermsFeed, n.d.) • Fines up to 2 % Brazil revenue (max R$50 million) (Littler Mendelson PC, 2023) • Other sanctions: public disclosure, data blocking, suspension
Territorial scope	Applies to controllers/processors in the EU or processing EU-resident data (extraterritorial)	Applies to data processed in Brazil or about individuals in Brazil, incl. offering goods/services or collecting data there (TermsFeed, n.d.)
Data-subject rights	Access, rectification, erasure, restriction, portability, objection, automated-decision review (Privacy.unc.edu, n.d.–b)	Confirmation, access, correction, anonymization / blocking / deletion, portability, withdrawal of consent, automated-decision review (TermsFeed, n.d.)

Aspect	GDPR (EU)	LGPD (Brazil)
Penalties	Up to €20 million / 4 % global turnover; plus warnings, bans, civil liability	Up to 2 % Brazil revenue (max R$50 million); warnings, public disclosure, processing suspension (Littler Mendelson PC, 2023)

4 Impact on Data Protection

Both the GDPR and LGPD have significantly enhanced the protection of personal data worldwide. By granting robust rights to data subjects and mandating accountability, these laws have shifted the power balance toward individuals and compelled organizations to adopt stronger data governance. Companies must document their data flows, ensure they have valid legal bases, and implement robust security measures. Consent and fair processing rules have reshaped marketing and advertising models, as users have more say in how their data is collected, shared, and retained. Furthermore, both regulations restrict cross-border data transfers unless adequate safeguards exist, prompting multinational entities to adopt standardized data protection clauses and higher security practices (Privacy.unc.edu, n.d.–b; TermsFeed, n.d.; UpGuard, n.d.).

5 Data at Rest vs. Data in Transit Under GDPR and LGPD

Neither GDPR nor LGPD explicitly distinguishes "data at rest" from "data in transit" by name; however, both require comprehensive protection of personal data throughout its life-cycle (European Union, 2016; Federative Republic of Brazil, 2018). Under GDPR Article 32, organizations must implement technical and organizational measures—such as encryption, pseudonymization, and access controls—to secure data wherever it resides or moves. LGPD likewise mandates that "processing agents shall adopt security measures able to protect personal data" at all stages of handling (UpGuard, n.d.; IAPP, n.d.).

5.1 Data at Rest

GDPR emphasizes "storage limitation" and the use of measures like database encryption and strict role-based permissions (Privacy.unc.edu, n.d.–b). Similarly, LGPD focuses on preventing unauthorized access and limiting data retention to what is necessary for the stated purpose (TermsFeed, n.d.). In practice, organizations often deploy encryption solutions, secure backups, and strict access policies to safeguard stored data.

5.2 Data in Transit

During data transfers, GDPR Recital 83 requires confidentiality, commonly achieved through TLS/SSL or other secure channels (OneTrust, 2020). LGPD has no explicit "72-hour rule," but demands breach notification "in a reasonable time period" if data in transit is compromised (UpGuard, n.d.). Organizations generally use end-to-end encryption, VPNs, and monitoring tools to protect data in motion under both frameworks.

6 Responsibilities of Cybersecurity Professionals

Cybersecurity professionals are central to complying with data protection laws:

6.1 Ensuring Compliance with Data Protection Principles

- Collaborate with privacy/legal teams to implement the principles of minimization, transparency, and accountability.
- Maintain documentation (e.g., records of processing, DPIAs) to demonstrate compliance (Privacy.unc.edu, n.d.–b).

6.2 Implementing Technical and Organizational Measures

- Enforce encryption, pseudonymization, and secure configurations.

- Set up identity and access management systems to ensure only authorized personnel handle personal data.
- Secure networks and endpoints (firewalls, anti-malware, patching) (Privacy.unc.edu, n.d.–b).

6.3 Risk Management and Privacy by Design

- Conduct risk assessments and incorporate privacy from the outset of system design.
- Evaluate and select vendors with appropriate security and contractual safeguards (OneTrust, 2020).

6.4 Incident Response and Breach Reporting

- Continuously monitor for potential breaches; investigate promptly.
- Notify supervisory authorities (under GDPR within 72 hours; under LGPD in a "reasonable time") (Privacy.unc.edu, n.d.–b; UpGuard, n.d.).
- Provide affected individuals with guidance to mitigate harm if a breach poses high risk.

6.5 Training and Culture

- Conduct regular security awareness training for all staff.
- Foster a privacy-first culture and ensure top management is informed of compliance statuses.

7 Recent Cases and Enforcement

7.1 GDPR Enforcement Cases

Over the years, GDPR has been actively enforced, resulting in significant fines:

- **Meta (Facebook) – €1.2 Billion Fine (2023):** For illegal data transfers to the United States despite the invalidation of the EU–US Privacy Shield (European Data Protection Board, 2023).
- **Amazon – €746 Million Fine (2021):** Alleged violations in personalized advertising (Reuters, 2021).
- **Google – €50 Million Fine (2019):** Lack of transparency in obtaining valid consent for personalized ads.
- **British Airways – £20 Million Fine (2020):** Security lapses leading to a data breach.
- **Marriott – £18.4 Million Fine (2020):** Failing to secure data acquired via merger.
- **H&M – €35 Million Fine (2020):** Excessive employee profiling and data collection.

7.2 LGPD Enforcement Cases

LGPD enforcement began more recently:

- **Telekall (2023):** The ANPD's first fines for processing data without a valid legal basis and failing to appoint a Data Protection Officer (Littler Mendelson PC, 2023).
- **Threads App Investigation (2023):** ANPD examined data collection practices of Meta's new social platform (UpGuard, n.d.).
- **Additional Investigations:** Ongoing scrutiny in banking, telecom, and e-commerce. While early fines have been modest, ANPD can impose larger penalties for serious or repeated violations.

These cases highlight that regulators on both sides actively enforce data protection laws. Non-compliance can result not only in financial penalties but also reputational damage and strict corrective orders.

8 Conclusion

The GDPR and LGPD together form a robust legal framework for data protection, each grounded in transparency, accountability, and respect for individual rights. Both laws require organizations to establish valid legal bases for processing personal data, honor data subjects' rights, and adopt strong security measures to mitigate breaches. While the GDPR has a longer track record and can levy extremely high fines, the LGPD is rapidly gaining momentum, ensuring that Brazilian residents' data is handled responsibly. For cybersecurity professionals, these regulations underscore the importance of comprehensive data governance—covering everything from privacy-by-design strategies to incident response plans. Ultimately, the GDPR and LGPD reflect a global trend toward stronger data protection regimes that balance technological innovation with the safeguarding of fundamental privacy rights.

References

European Data Protection Board. (2023, May 22). *1.2 billion euro fine for Facebook as a result of EDPB binding decision*. https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en

European Union. (2016). *General Data Protection Regulation* (Regulation (EU) 2016/679). https://privacy.unc.edu/

Federative Republic of Brazil. (2018). *Lei Geral de Proteção de Dados Pessoais* (Law No. 13 709/2018, as amended). https://termsfeed.com/

IAPP. (n.d.). *LGPD Overview and Guidance*. https://iapp.org/

Littler Mendelson PC. (2023, July). *Brazil ANPD Issues its First Sanction*. https://www.littler.com/news-analysis/asap/brazil-data-protection-agency-anpd-issues-its-first-sanction-against-non

OneTrust. (2020, September). *LGPD vs. GDPR: Key Differences Explained*. https://www.onetrust.com/blog/lgpd-vs-gdpr/

Privacy.unc.edu. (n.d.–a). *GDPR Overview*. https://privacy.unc.edu/

Privacy.unc.edu. (n.d.–b). *GDPR Principles and Compliance*. https://privacy.unc.edu/

Reuters. (2021, July 30). *Amazon hit with record EU data privacy fine*. https://www.reuters.com/business/retail-consumer/amazon-hit-with-886-million-eu-data-privacy-fine-2021-07-30/

TermsFeed. (n.d.). *Brazil's LGPD: Everything You Need to Know*. https://www.termsfeed.com/blog/lgpd/

UpGuard. (n.d.). *What is the LGPD? Brazil's General Data Protection Law*. https://www.upguard.com/blog/lgpd

Usercentrics. (n.d.). *Consent Under GDPR & LGPD*. https://usercentrics.com/