GRIFFITH COLLEGE DUBLIN

LLM Dissertation Submission Cover Sheet

Student name:	**Maria Eduarda Ramalho Queiroz**
Student number:	**3128377**
Dissertation title:	**The extraterritorial influence of GDPR : The Brazilian Case**
Supervisor's name:	**Elletra Bargellini**
Supervisor's signature:	

Plagiarism disclaimer:

I understand that plagiarism is a serious offence and have read and understand the college's policy on plagiarism and that my dissertation will be checked for plagiarism through TURNITIN. I also understand that I may receive a mark of zero if I have not identified and properly attributed sources which have been used, referred to, or have in any way influenced the preparation of this dissertation, or if I have knowingly allowed others to plagiarise my work in this way.

I hereby certify that this dissertation is my own work, based on my personal study and/or research, and that I have acknowledged all material and sources used in its preparation. I also certify that the dissertation has not previously been submitted for assessment and that I have not copied in part or whole or otherwise plagiarised the work of anyone else, including other students.

Maria Eduarda R. Queiroz **09/08/2024**

Signature of student: **Date:**

Note to LLM students: You **MUST** submit TWO HARD-BOUND COPIES + A COPY ON MOODLE. You MUST retain the receipt issued to you as proof of submission.

FOR OFFICE USE ONLY:

No. of copies received (please tick):	2 x hard-bound
Confirmation from student that soft copy submitted on Moodle:	Yes
Date:	
Received by: **Name:**	
Signature:	

The extraterritorial influence of GDPR : The Brazilian Case

Research dissertation presented in partial fulfilment of the requirements for the degree of LLM in International Commercial Law (QQI)

Law School, Griffith College Dublin

Maria Eduarda Ramalho Queiroz

2024

Candidate Declaration

Candidate Name : Maria Eduarda Ramalho Queiroz

I certify that the dissertation entitled: **The extraterritorial influence of GDPR : The Brazilian Case**

Submitted for the degree of: LLM in International Commercial Law is the result of my own work and that where reference is made to the work of others, due acknowledgement is given.

Candidate Signature: Maria Eduarda R Queiroz

Date: 09/08/2024

Supervisor Name: Elettra Bargellini

Supervisor Signature:

Date:

Acknowledgements

I would like to express my deepest gratitude to my supervisor, Elettra Bargellini for her kindness, intelligent guidance and understanding support during this process of research, her constant gentle approach, was noticed and profoundly appreciated.

I also would like to thank my family whose love and encouragement have been a constant source of strength. Their ability to help me see life through a lens of grace and resilience has provided me with the motivation I needed.

Dedication

This work is dedicated to all of those that challenge themselves to do something outside their comfort zone, thousands of kilometres away from home and to my mom that taught me kindness, courage and how to pray.

Table of Contents

Title Page ..... **ii**
Candidate Declaration ..... **iii**
Acknowledgements ..... **iv**
Dedication ..... **v**
Abstract ..... **viii**

Introduction **9**
Chapter 1 - GDPR and LGPD **10**
1. Introduction 10
2. Convention for Human Rights and Fundamental freedoms 11
3. European Union - GDPR 14
3.1 Introduction 14
3.2 GDPR - Historical Background 15
3.3 GDPR - Aim 16
3.4 GDPR - Key Concepts 17
4. Brazil - LGPD 21
4.1. Introduction 21
4.2 LGPD - Historical Background 22
4.3 LGPD- Aim 23
4.4 LGPD - Key concepts 24
5. Comparative analysis 26

Chapter 2 - Principles and Rights **27**
1. Introduction 27
2. European Union 28
2.1 Introduction 28
.2.2 GDPR - Key Principles 28
2.3 GDPR – Legal Bases for processing personal data 31
2.4 GDPR- Rights of the Data Subject 34

3. Brazil 39
3.1 Introduction 39
3.2 LGPD - Key Principles 39
3.3 LGPD – Legal Bases for processing personal data 43
3.4 LGPD- Rights of the Data Subject 46
4. Comparative analysis 50

Chapter 3 - Enforcement and Remedies 51
Introduction 51
2. European Union 52
2.1 Introduction 52
2.1 Obligations for Controller and Processor 52
2.1.2 Controller and Processor Penalties 55
2.3 DPO duty 56
2.4 DPA - National Data Protection Authority 58
2.5 GDPR - Enforcement Mechanisms 61
2.6 GDPR - Remedies Measures 63
3. Brazil 64
3.1 Introduction 64
3.1 Obligations for Controller and Processor 64
3.1.2 Controller and Processor Penalties 67
3.2 DPO duty 68
3.3 DPA - National Data Protection Authority (ANPD) 69
3.4 LGPD - Enforcement Mechanisms 71
3.5 LGPD- Remedies Measures 72
4.Comparative analysis 73

Propositions 75
Conclusion 77
References 78

Abstract

The primary objective of this dissertation was to assess the influence of the General Data Protection Regulation (GDPR) on Brazilian legislation concerning data protection, specifically the Lei Geral de Proteção de Dados (LGPD). Through a comparative analysis, this research examined the key elements of both regulatory frameworks, highlighting their similarities and differences. Employing historical, doctrinal, and comparative methodologies, the study uncovered that the GDPR significantly shaped the development of the LGPD, serving as a foundational model for Brazil's approach to data protection. However, it also demonstrated that the LGPD incorporated specific adaptations to align with the realities of Brazilian society and legal culture. These adaptations ensured that the LGPD addressed unique national concerns while striving to meet international standards for data protection. The findings contributed to the understanding of how global regulatory frameworks can influence local legislation, shedding light on the complexities of implementing data protection laws in diverse sociocultural contexts.

Keywords: General Data Protection Regulation, data protection, comparative analysis, Brazilian legislation.

The extraterritorial influence of GDPR : The Brazilian Case

Introduction

In my practice as a commercial lawyer in Brazil, I've seen the challenge of enforcing the new data protection law, I have noticed the big resistance of clients to the necessary adjustments prevenient from the legislation. I've also comprehended the difficulty law professionals have in designing plans for companies in a way that allows them to adapt to the new norms. The changes in the data protection norms, required companies to change their practices, aiming to result in a real transformation in the business culture and to further the companies' perception of the importance of data protection.

This leads me to the main issue in this work: **How has GDPR influenced the Brazilian legislation for data protection?** Therefore, this dissertation provides a comprehensive examination of data protection laws, focusing primarily on the General Data Protection Regulation (GDPR) implemented in the European Union and the General Data Protection Law (LGPD) adopted in Brazil. It examines the General Aspects, Principles and Rights, and finally, Enforcement and Remedies across three chapters.

The first chapter starts by explaining the basis of the Right to Privacy in the Convention for Human Rights, going through the historical evolution, aim, and key concepts of General Data Protection Regulation (GDPR) and the Brazilian data protection legislation, the Lei de Proteção de Dados (LGPD). In the second chapter, the key principles are discussed in more detail, and the biggest difference between the legislations is the right to be forgotten. The third chapter discusses Enforcement and Remedies and will include an examination of the obligations placed on data controllers and processors, the penalties for non-compliance, the duties of Data Protection Officers (DPOs), and the roles of Data Protection Authorities (DPAs) in both the EU and Brazil, explaining how both legislations can be enforced and which remedies are available in case of a breach of personal data rights.

The methodology used in this research is historical, using textbooks and articles prior to the current Data Protection law to understand the development of data protection rights. Moreover, it uses a doctrinal methodology, focusing primarily on the General Data Protection Regulation (GDPR) and the Lei de Proteção de Dados (LGPD) as the main sources of study. Using the current norms for Data Protection, academic articles, and analysing the key provisions, principles, and requirements outlined in these legislations, this dissertation aims to understand the extent of the influence that the General Data Protection Regulation (GDPR) performed over the Brazilian data protection legislation, LGPD. The last method applicable to this dissertation is the comparative, which is used, in each chapter, to review how these legislations approach and differ from each other.

Chapter 1

GDPR and LGPD

1. Introduction

This chapter traces the development of laws that have had a major impact on international data privacy standards, giving a detailed overview of the historical evolution of data protection legislation in both the EU and Brazil. For that, it is necessary to comprehend the concept of the Right to Privacy in the Convention for Human Rights which is a pillar for both GDPR and LDPD.

This study reviews the objectives of these regulations, highlighting their aim of harmonizing data protection laws across different jurisdictions and preserving peoples' fundamental rights to privacy and data security. Furthermore, this chapter explores key concepts that are necessary to comprehend the GDPR and LGPD, such as the definitions of data processing, controllers and processors, and personal data. Through an examination

of these components, comprehending the parallels and divergences between these two data protection laws and their data privacy standards.

2. Convention for Human Rights and Fundamental freedoms

Before we can discuss GDPR and LGPD it's important to understand where both legislations were grounded. This section will assess the importance of the Convention for Human Rights with the recognition of the Right to Privacy and understand the development of data protection legislation in four generations.

The Convention for Human Rights and Fundamental Freedoms brought into the legal framework the Right to Private Life, which is the base for the legislation we will discuss. The vital part of the right to liberty and self-determination is the right to privacy, it provides protection from unlawful interference by public authorities and other aspects of personal life, such as correspondence, home, and family life. These protections make it feasible to uphold private boundaries and authority over their own personal data. It is a powerful way to protect identity and integrity from misuse, illegal access, and unjustified surveillance. [1]

The right to privacy and protection of personal data is not absolute and may face situations where it's legally admissible to have it mitigated for the greater good. Topics of national security, public safety, crime prevention, and public interest are possibilities to have these rights diminished legally.[2] Finding the equilibrium its for sure the challenge of the GDPR legislation, where the public interest begins and where the individual rights hit a barrier, what is justified and proportionate. The Convention for Human Rights and Fundamental freedoms recognizes the right for privacy as outlined in Article 8: [3]

> Right to respect for private and family life
>
> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.

[1] Voronova Sofija, 'Understanding EU Data Protection Policy'.
[2] Maria Lilla Montagnani and Mark Verstraete, 'What Makes Data Personal?' (2022) 56 UC Davis Law Review 1165.
[3] 'European Convention on Human Rights'.

> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

From that established right through the years, that right was recognized and incorporated in many national legislations with different degrees of protection.[4] As a reflection of that, the Charter of Fundamental Rights of the European Union furthers these rights with the provision not only for private life but a fundamental protection of personal data:

> Charter of Fundamental Rights of the European Union (2007/C 303/01) [5]
>
> Article 7 – Respect for private and family life
>
> Everyone has the right to respect for his or her private and family life, home and communications.
>
> Article 8 – Protection of personal data
>
> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.

[4] Sofija (n 1).
[5] Charter of Fundamental Rights of the European Union 2012 (OJ C).

It is common practice to categorize the development of data protection laws into four generations. Each generation reflects the increasing intricacy and the evolving focus of these laws that over time reflect the increasing complexity and changing concerns of society and technology.

In the 1960s the First Generations of laws was more technical, with the primary focus on regulating the creation and management of large centralized databases, particularly those operated by the government. By using computer terms, without any concern for the social repercussions and the privacy of individuals, these laws quickly became outdated due to the rapid development of multiple processing centres and the spread of computer technology beyond government control. [6]

In the 1980s, the Second Generation of laws began to recognize the importance of protecting personal data in all sectors. These legislations were more centred around the protection of individual's rights, introducing the possibility of bigger control over personal data. These laws also created instruments to make it possible to identify the misuse of your data, as well as to propose its protection.[7]

In the 2000s the Third Generation of laws adopted a more neutral approach regarding the technology, as a strategy to stay relevant throughout the evolution in this field. These legislations emphasize the accountability of data controllers and processors and aim to expand the rights of second-generation laws.[8]

Currently, we are in the Fourth Generation of legislation, which takes into account technological advances and social evolution. These legislations aim to establish a more balanced framework worldwide, protecting individual rights, holding data controllers and processors accountable, and allowing a safe environment for the free exchange of data.[9]

The journey from the first to the fourth generation of data protection laws reflects a significant shift from a narrow, technical focus to a broad, user-centric approach that considers both technological advancements and the social implications of data

[6] Cinthia Obladen de Almendra Freitas, Lucas Bossoni Saikali and Rafael Almeida Oliveira Reis, 'Adoption of the Regulation Model by the Code Architecture and Privacy by Design and by Default Practices for the Regulatory Scenario of Personal Data Protection in Brazil National Doctrine' (2022) 46 Direitos Fundamentais & Justica 363.
[7] ibid.
[8] ibid.
[9] ibid.

processing. As technology continues to evolve, so too will data protection laws, striving to balance innovation with the fundamental rights and freedoms of individuals.[10]

Knowing the basis for the GDPR and LGPD and considering the fourth generation of data protection rights, this work will now offer an analysis of both legislation, exploring their historical background, aim, and key aspects.

3. European Union - GDPR

3.1 Introduction

GDPR is the General Data Protection Regulation, 2016/679 created by the European Parliament and the Council on 27 April 2016. It applies to all Member States and has extraterritorial reach. But most importantly it inspired and influenced legislation all over the world. This section explains the historical evolution until the current GDPR, its aim, and key concepts.

The current regulation has a goal to harmonize the protection of the freedom and rights of natural persons while at the same time providing a free flow of personal data between Member States. The GDPR aims to guarantee a consistent level of protection throughout the European Union regarding personal data for data subjects. Considering the free movement of data within the internal market, demanding accuracy, fairness, and transparency in the processing of data from micro, small, and medium-sized enterprises. The legislation also ensures the same level of enforceable rights and obligations for controllers and processors, providing a tool for consistent oversight of the data protection framework between Member States as well as the possibility of effective cooperation between supervisory authorities.[11]

The principles of data protection must be applied to all data pertaining to a natural person who is identifiable or identified. The principles of data protection also apply to personal data that went through pseudonymization but it can lead to the identification of a natural person with the help of additional information. In order to determine if a natural person is identifiable, it must be considered if the means are reasonable and likely to be used to

[10] ibid.
[11] 'Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR)' (*General Data Protection Regulation (GDPR)*) <https://gdpr-info.eu/> accessed 10 May 2024.

identify the natural person, such as costs and amount of time that would take to identify the person, also considering the technology available.[12]

With that understanding, the principles of data protection do not apply to anonymous information, namely information that could not identify or lead to a natural person identification.

A natural person should have the possibility of rectifying their data, and the possibility of demanding its rectification, once the data collected should be accurate. Another important right is the right to be forgotten, which limits the retention of such data, demanding its destruction if proven that is no longer relevant for the purpose collected and its existence can cause harm to the person.[13]

3.2 GDPR - Historical Background

After World War II, came an extensive number of treaties and legislations, in that context, the right to privacy became focus of discussion with the Universal Declaration of Human Rights[14] in 1948. That declaration presented the right to be free from unlawful interference in privacy, family, home, and correspondence. The 1950 comes into play the European Convention on Human Rights[15] a international treaty binding the signature countries with the right to respect for privacy and family life.[16]

In a direct reaction to the indiscriminate and unlimited surveillance regimes imposed by the German State in previous years, in 1970, the state Hessen in Germany introduced the first law in Europe to address especially the protection of personal data. That initiative was followed by Sweden in 1973, Germany in 1977, and France in 1978.[17]

---

[12] Yelena Smirnova Victoriano Travieso-Morales, 'Understanding Challenges of GDPR Implementation in Business Enterprises: A Systematic Literature Review' <https://www.researchgate.net/publication/377572957_Understanding_challenges_of_GDPR_implementation_in_business_enterprises_a_systematic_literature_review> accessed 13 May 2024.
[13] Idem.
[14] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR)
[15] 'European C Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR)
[16] Sofija (n 1).
[17] David Banisar and Simon Davies, 'Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments' (1999) 18 John Marshall Journal of Computer and Information Law 1.

In May 1975, the European Parliament adopted a resolution recognizing a right for data protection for individuals, but it was the responsibility of each Member State to determine how this right would be protected. In the 1980's there was an attempt to harmonize the different legislations of Member States with guidelines from the Organisation for Economic Co-operation and Development (OECD) and with the Convention 108 from the Council of Europe. This convention was the first binding instrument to protect individuals against breaches of their right to data protection. [18]

The Convention 108 was signed by all Council of Europe members, all EU Member States, and also Argentina, Cabo Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia, and Uruguay. That convention was later updated by Protocol CETS 223 in October 2018.[19]

In 1995, the Data Protection Directive 95/46/EC(DPD) became the main European instrument for data protection and it was the predecessor to GDPR, that directive already came with many of the key concepts adopted in the current legislation and aimed to improve the internal market addressing gaps on the legislation for the Member States regarding the protection of fundamental rights. In 2000 the Charter of Fundamental Rights of the European Union was proclaimed and explicitly recognized as a fundamental right the right to data protection. [20]

All this background led to the GDPR legislation in 2016, designed to assess the new challenges regarding the protection of personal data. Guiding the process of data and all its forms and offering further protection for individuals subject to data protection. It became enforceable on May 25, 2018. [21]

3.3 GDPR - Aim

The GDPR aims to broaden the protection of personal data for individuals within the Member States of the EU, ensuring respect for the fundamental rights to privacy and data protection. The regulation, binding for all Member States, seeks to harmonize the

[18] Sofija (n 1).
[19] Jorg Ukrow, 'Data Protection without Frontiers? On the Relationship between EU GDPR and Amended CoE Convention 108 Reports: Practitioner's Corner' (2018) 4 European Data Protection Law Review (EDPL) 239.
[20] Sofija (n 1).
[21] ibid.

treatment of data across the European Union, providing a consistent legal framework, making possible the same level of protection in all Member States, and facilitating the free flow of data in a responsible and legitimate manner..[22]

The legislation aims to give individuals more control over their data, this goes through being able to reinforce the right to access personal data, but also the introduction of new rights such as The Right to be Forgotten and the right to data portability.[23]

As seen in the historical evolution of Data Protection, each country had its own legislation and methods of reinforcing it. The European Union's regulation on data protection binds them and sets parameters for a balanced framework throughout the European Union. This makes viable the high standards of protection in the right for privacy and data protection, while also facilitating the free flow of data within the internal market.

The legislation places emphasis on transparent methods in the processing of data while demanding accountability from the organizations responsible for processing personal data.[24] In that sense, it requires the institutions to explain how they are complying with the GDPR, keeping records of processing activities, also mandatory data protection officers in certain circumstances and introducing substantial fines in case of violations.

All actions demanded from institutions aim to mitigate data breaches and cyberattacks. The protection of personal data, not only benefits individuals but also creates trust in the market. Ensuring that personal data is handled with responsibility and care, and guaranteeing the correct processing of data boots the possibility of business within the EU and countries that uphold the same level of protection.

3.4 GDPR - Key Concepts

[22] IT Governance (Organization) (ed), *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide* (Third edition, IT Governance Publishing 2019)
[23] Wenlong Li, 'A Tale of Two Rights: Exploring the Potential Conflict between Right to Data Portability and Right to Be Forgotten under the General Data Protection Regulation' (2018) 8 International Data Privacy Law 309.
[24] 'Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR)' (n 11).

In order to best comprehend the legislation in the study, it is relevant to learn the key concepts drafted in the GDPR (Article 4), so this work will approach the concepts of Personal Data, Processing data, Controller, Data Processor, Data Subject, Data Protection Officer and Pseudonymisation:[25]

a) Personal Data

Personal data is any information related to a natural person that can identify it or make it identifiable. Identifiability can be direct or indirect. Maria Lilla Montagnani and Mark Verstraete argue that personal data is not a natural concept but in reality, a policy choice that is determined by social, political, and ethical principles. To put it another way, nothing in the world is inherently personal data and should, therefore, be subject to a particular set of legal regulations. A more comprehensive normative vision of privacy and data protection law should inform legal categories that determine when people should have control over information instead of deciding this based on an abstract concept of personal data. [26]
Examples: Names, addresses, email addresses, IP addresses

There is a special category of personal data that has special attention by the GDPR, sensitive data.

Sensitive data: It's the personal data that are particularly sensitive, processing these data could create significant risks to the fundamental rights and freedoms. Such personal data should not be processed, unless processing is allowed in specific cases and if its processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject or processing is necessary for reasons of substantial public interest as explained by Article 9. Paragraph 2 of the GDPR. [27]

[25] Maria Lilla Montagnani and Mark Verstraete, 'What Makes Data Personal?' (2022) 56 UC Davis Law Review 1165.
[26] ibid.
[27] 'Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR)' (n 11).

Examples : Religion, Race or ethnic origin, Political opinions, Sexuality, biometrical, genetical data.

b) Processing Data

Processing data is any operation which is done with personal data collected. Whether manually or automated, the collection, recording, structuring, storage, organizing, adapting, altering, retrieval, consulting, using, disclosing by transmission, transferring, dissemination, making available, rectifying, alignment or combining, restricting, erasing or destroying, all these actions are processing data and as such, under the scope of the GDPR. Examples**:** Storing customer information in a database, analysing user behaviour on a website, or sharing employee details with a payroll service provider. [28]

c) Controller

Controller is a natural or legal person, public authority, agency or any other body that defines the purpose and means of processing personal data. [29]

Examples: Companies, government agencies, non-profit organizations, and other entities that decide why and how personal data is processed.

d) Data Processor

A data processor is a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller. Processors must

[28] ibid.
[29] ibid.

follow the instructions of the controller and are also subject to data protection obligations. [30]

Examples: Cloud service providers, payroll companies, and third-party marketing firms that handle data on behalf of another organization.

e) Data Subject

The data subject is the individual to whom the personal data relates. Data subjects have rights under the GDPR, such as the right to access, rectify, erase, and object to the processing of their data. [31]

Examples: Customers, employees, website users, and any other individuals whose data is being processed.

f) Data Protection Officer

A DPO is an individual appointed by an organization to ensure compliance with data protection laws and regulations. The DPO acts as a point of contact between the organization and supervisory authorities and advises on data protection obligations. [32]

Examples: An in-house privacy expert or an external consultant responsible for overseeing data protection strategies and practices.

g) **Pseudonymisation**

Pseudonymisation (Article 4 and Recital 26) means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject

[30] ibid.
[31] ibid.
[32] ibid.

without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person, these data are still in the scope of GDPR. [33]

> Its relevant to note that anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. The GDPR does not concern the processing of such anonymous information. [34]

By observing these principles, organizations can make sure they respect to privacy rights and maintain compliance with one of the world's most rigorous data protection regulations. The GDPR's influence continues to shape data protection policies globally, emphasizing the importance of safeguarding personal data in a progressively more digital world.

4. Brazil - LGPD

4.1. Introduction

In light of the GDPR, and all the developments made with that legislation, the LGPD, the Brazilian legislation for data protection comes to the Brazilian legal framework in recognition of necessary adjustments to be up to date with best practices in regard to the protection of fundamental rights of data protection and right for privacy.

This section will delineate the historical evolution of the protection of data in the Brazilian ordainment until the current LGPD, the Aim of this legislation, and its key concepts.

---

[33] ibid.
[34] ibid.

In light of the year 2010's revelations of Edward Snowden and the Cambridge Analytica breach, it became noticeable the vital role of legislation that protects individuals from abuse in surveillance and misuse of their data. In that perception, the LGPD came to establish an organized framework to protect personal data and ensure the lawful treatment of data.

4.2 LGPD - Historical Background

Brazil went through a process of democratization in 1985, so the historical evolution of data protection will only consider democratic years. In 1988 the current constitution was promulgated.

In that 1988 Constitution, the inviolability of intimacy and private life was stablished, later on the year 1990 the Brazilian Consumer Protection Code guaranteed the communication in writing in case of use of personal data of the consumer.[35]

In the years 2002, a new Civil Code came into place, and also had a provision of inviolability of the private life of the natural person. In 2011 was instated the law for access to information (n 12.527/2011) ensuring a natural person the access to information that the Government or public entity would have from them. [36]

In 2012 came the law 12.737/2012 that criminalized the access and obtaining personal data via electronic accounts or devices, so it became a crime to hack or illegally access someone`s email for instance. [37]

In 2013, the Federal Decree 7, 962/2013 entered in the ordainment, which deals with contracting in electronic commerce, (Article 4, VII), requires suppliers to use effective security mechanisms for payment and processing of consumer data. [38]

In the years following Edward Snowden's exposure to NSA illegal surveillance and the depth of beach of fundamental rights, the world was highly impacted and it clearly

[35] Freitas, Saikali and Reis (n 6).
[36] ibid.
[37] ibid.
[38] ibid.

reflected on the 2014 Brazilian's legislation and also affected EU with the end of the Safe Harbour between EU and USA and beginning of Model clauses.

In 2014, the law No. 12,965 coming into effect, establishing principles, guarantees, rights, and duties for using the Internet in Brazil. It expressly protects privacy (Article 3, 11) and personal data (Article 3, IHI).

Although the topic has been addressed by laws such as the Consumer Protection Code and the Marco Civil da Internet, in addition to the 1988 Constitution, the real milestone in the protection of personal data occurred in 2020 with the General Data Protection Law Personnel (LGPD) and the creation of the National Data Protection Authority (ANPD), the entity responsible for the application, supervision and regulation of the LGPD.[39]

4.3 LGPD- Aim

The LGPD aims to protect the fundamental rights and guarantees of the natural person, in a balanced way, through the harmonization and updating of concepts in order to mitigate risks and establish well-defined rules on the processing of personal data.

The Brazilian General Data Protection Law deals only with the processing of data personal data. That is, it does not directly affect the data of a legal entity, confidential or confidential documents, business secrets, plans algorithms, formulas, software, or patents, among other documents or information that are not related to a natural person identified or identifiable.[40]

All these other types of information or documents are protected by different legal acts, such as the Industrial Property Law (Law 9.279/1996), the Industrial Rights Law Copyright (Law 9.610/1998), and the Software Law (Law 9.609/1998), only for cite a few examples. Nevertheless, whenever such documents and information not directly touched by the law under study contains data, only these data, will be protected by it. This

[39] ibid.
[40] Viviane Nóbrega Maldonado and Renato Opice Blum, 'LGPD: Lei geral de proteção de dados: comentada' <https://bdjur.stj.jus.br/jspui/handle/2011/132481> accessed 20 July 2024.

is why the analysis of the applicability of the LGPD, from this point of view, should deepen the mapping and inventory of both structured personal data and unstructured.[41]

The central idea addressed by the new legislation is to guarantee, through the processing of personal data, respect for the fundamental rights of freedom and privacy. In short, an innovative way for our society to relate to personal data and the privacy of its individuals. The point of contact between these individuals, their rights, their data, and those responsible for processing this data is the so-called Data Controller.

The role of the controller most of the LGPD was inspired by European data protection legislation, the General Data Protection Regulation (GDPR), which calls this role Data Protection Officer (DPO), it was one of the biggest innovations of this law.[42]

4.4 LGPD - Key concepts

In order to see the differences and similarities of the GDPR and LGPD, its relevant to learn the key concepts drafted in the LGPD (Article 5), so this section will approach the concepts of Personal data, Processing data, Controller, Data Processor, Data Subject, Data Protection Officer and Pseudonymisation[43]:

a) **Personal Data:**

It's the data connected to a natural person's sphere, acquiring the characteristic of being personal, means safeguarding one's own personality of the human being, since this constitutes "the characteristics or set of characteristics that distinguish a person".[44] Brazil has adopted the expansionist concept of personal data, whereby not only the information relating to the directly identified person will be protected by the Law, but also that information that can, has the potential to, make the person identifiable. The LGPD also provides a more restrictive protection on Sensitive

[41] ibid.
[42] Lara Rocha Garcia, *Lei Geral de Proteção de Dados (LGPD): Guia de Implantação* (Editora Blucher 2020).
[43] 'LEI Nº 13.709 Lei Geral de Proteção de Dados Pessoais (LGPD)' <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> accessed 2 June 2024.
[44] Maldonado and Blum (n 39).

Data, due its nature representing significant risks to the fundamental rights and liberty, such as data on political views, sexuality, religious background and other data that could be used to retaliate against the Data Subject.[45]

b) Processing data

Any operation performed on personal data, such as collection, storage, use, transfer, or deletion. [46]

c) Controller

The natural or legal person, public authority, agency, or other body that determines the purposes and means of processing personal data. [47]

d) Data Processor

A natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller. [48]

e) Data Subject

The individual to whom the personal data refers. [49]

f) Data Protection Officer

An individual appointed by the data controller to oversee compliance with the LGPD, act as a point of contact for data subjects and the data protection authority, and manage data protection policies. [50]

g) Pseudonymisation

---

[45] 'LEI Nº 13.709 Lei Geral de Proteção de Dados Pessoais (LGPD)' (n 42).
[46] ibid.
[47] ibid.
[48] ibid.
[49] ibid.
[50] ibid.

> It’s the processing of personal data in such a way that it can no longer be attributed to a specific individual without the use of additional information (Article 4 and Article 5 II). While pseudonymised data remains classified as personal data under the LGPD, its use significantly mitigates risks and strengthens the protection of data subjects' rights while maintaining the data's utility for analysis or other legitimate purposes.[51]

5. Comparative analysis

The GDPR was adopted by the European Union and came into effect in 2018, It targets to unify and strengthen data protection for individuals within the EU and the European Economic Area. The GDPR replaced the Data Protection Directive 95/46/EC and aimed to respond to technological developments and shifts in data practices. Meanwhile, the Lei Geral de Proteção de Dados (LGPD) was enacted in Brazil and came into effect in 2020. The LGPD aimed to establish similar protections tailored to the Brazilian legal context, addressing the need for more stringent controls and transparency concerning personal data processing.[52]

The LGPD is also a response to the desire for greater legal security in the Brazilian digital environment, by updating and consolidating concepts that were previously scattered across various regulations. Since the LGPD largely follows a more robust and current standard in terms of data protection, which is the General Data Protection Regulation (GDPR), by ensuring a consistent, high, and homogeneous level of general and horizontal protection, it tends to eliminate obstacles to the circulation of personal data with other countries and, consequently, generate a higher likelihood of investments and economic activities in Brazil.[53]

Both law seeks to balance the maintenance of economic and technological development of innovative business models with the inviolability of citizens' constitutional rights (Article 3 GDPR and Article 3 LGPD). The laws are comprehensive in nature regarding

[51] ibid.
[52] Garcia and others (n 41).
[53] Maldonado and Blum (n 39).

personal, material, and territorial scope. For example, both the GDPR and the LGPD apply to organizations that have a presence in the EU and Brazil respectively as well as to organizations that are not physically located, but offer goods and services in the jurisdictions, or process personal data in these regions. Also, both laws apply to organizations that, although do not have any presence in the EU, monitor the behaviour of individuals in the EU. For example, the LGPD applies to the processing of people who are in Brazil, regardless of where the data is processed. [54]

Both pieces of legislation apply to the processing of natural persons' data as carried out by controllers and processors. In particular, their scope of application appears wide as they both protect individuals regardless of their nationality or residency status. This principle is explicitly included in the GDPR, while in Brazil it is provided for by the combined interpretation with the Federal Constitution of Brazil.

In addition, both laws exclude from their scope the processing of anonymized data(Articles 4 and Recital 26 GDPR and Article 4 and 5 II LGPD), although the LGPD states that data can be considered personal when used to formulate behavioural profiles of a particular natural person if that person is identified.

Chapter 2

Principles and Rights

1. Introduction

[54] 'LEI Nº 13.709 Lei Geral de Proteção de Dados Pessoais (LGPD)' (n 42).

Both the GDPR and the LGPD create strong frameworks for data protection that are built around fundamental rights and principles that give people power and guarantee the responsible handling of personal data. Organizations by complying with these legislations can build trust with data subjects and better manage the complexities of data privacy by being aware of these rights and principles.

In this chapter the key principles, the legal bases for processing data and the rights of the data subject for both legislations will be examined. Additionally, one of the biggest differences between the legislations will be addressed, specifically their differing approaches to the Right to be forgotten.

2. European Union

2.1 Introduction

The GDPR it's an important milestone in the development of data protection legislation in the European Union. In addition to outlining a thorough framework for the processing of personal data, focusing on protecting fundamental rights.

This section dives into the key principles guiding the GDPR, the legal bases for processing personal data, and the rights granted to data subjects. By examining these fundamental elements, gaining insight into the regulation objectives and their implications for businesses, governments, and individuals

.2.2 GDPR - Key Principles

In the core of GDPR are principles that guide the lawful processing of personal data in article 5 and 6: Lawfulness, Fairness, Transparency, Purpose limitation, Data Minimization, Accuracy, Storage Limitation, Integrity and Accountability. These principles are designed to foster responsible data handling and reinforce the significance of trust between organizations and individuals, they serve as guidelines for the general

handling of personal data and are meant to guarantee that data processing is carried out in a way that is fair, legal, and transparent. [55]

a) Lawfulness:

Any processing of data must have a legitimate legal foundation, such as consent, fulfilling a contract, or adhering to a mandate. [56]

b) Fairness:

When processing data, care must be taken to treat the individuals involved fairly. This calls for integrity and refraining from data misuse. [57]

c) Transparency:

It is the right of individuals to know how their data is being used. This entails being open and honest about the purposes behind data processing, the duration of data retention, and the individuals who will have access to the data. [58]

d) Purpose Limitation:

Personal data should not be processed in a way that is inconsistent with its intended uses; rather, it should only be gathered for clear, explicit, and legal purposes. This guarantees that personal information is only utilized for purposes that the person would reasonably expect. [59]

e) Data Minimization:

[55] IT Governance (Organization) (n 21).
[56] ibid.
[57] ibid.
[58] ibid.
[59] ibid.

Only information required to fulfil the stated goals should be gathered and handled. This lowers the possibility of misuse by only gathering the information necessary to fulfil the stated goal. [60]

f) Accuracy:

Personal data must be accurate and, when needed, kept current. As soon as possible, inaccurate data should be removed or corrected to maintain the accuracy of the data processing. [61]

g) Storage Limitation:

Personal data should only be retained in a format that allows for identification of the individual for as long as is required to fulfil the objectives for which it is processed. This restricts the amount of time that can be spent using and storing the data. [62]

h) **Integrity:**

Processing of personal data must be done in a way that guarantees adequate security, including defence against improper or illegal processing as well as against unintentional loss, damage, or destruction. To do this, appropriate organizational and technical measures must be put in place. [63]

i) **Accountability:**

Requires the demonstration of how the organization has been compliant with the GDPR principles and practices. In order to demonstrate that, data controllers are

[60] ibid.
[61] ibid.
[62] ibid.
[63] ibid.

required to maintain records of data processing activities, impact assessments and ensure the proper treatment of data within the organisation. [64]

By following these principles, organizations can guarantee that personal data is managed in a manner that is not only legal and transparent but also respectful of individuals' rights. In the end, embracing these guidelines fosters a culture of accountability and trust, which is vital in today's society.

Furthermore, when organizations prioritize these principles, they demonstrate a commitment to ethical practices that extend beyond mere compliance. This proactive approach helps build a strong relationship with customers, enhancing loyalty and encouraging positive engagement. Organizations that embrace a culture of accountability not only protect themselves from potential legal repercussions but also position themselves as ethical organizations, increasing their trust in the market.

2.3 GDPR – Legal Bases for processing personal data

The six legal bases listed in Article 6 of the GDPR, provide the legal justification necessary for processing activities. The Legal Bases for processing personal data are specific conditions defined in the GDPR that justify why an organization is allowed to process personal data.

The GPDR enumerates six legal bases for processing personal data: Consent, Contractual Performance, Legal Obligation, Vital Protection, Public Interest, and Legitimate Interest [65]. Each of these bases serves distinct purposes and requirements, making it imperative for organizations to carefully assess which provision applies to their specific processing activities:

[64] ibid.
[65] 'Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR)' (n 11).

a) Consent:

Consent is an essential aspect of the GDPR. Under the GDPR, consent must be provided voluntarily, specific, informed and unambiguous reflecting the individual's preferences. There needs to be a clear affirmative action on the part of the individual—essentially, a positive opt-in—meaning that consent cannot be assumed from a lack of response, pre-selected checkboxes, or inaction. Additionally, consent should be distinct from other terms and conditions, and organizations must offer straightforward methods for individuals to revoke their consent. Public authorities and employers must take extra precautions to ensure that consent is truly voluntary. Consent should be easily verifiable, and individuals typically have enhanced rights if their data processing relies on their consent.[66]
Consent under the GDPR can be given but can also be withdrawn, at which point the data would no longer be able to be processed. Although consent is not always required for processing, there are specific operations that do necessitate it. Notably, it's mandatory to obtain consent if intended to market to an individual, so it's important to distinguish between general processing activities—such as managing orders or operating an online account—and marketing. Other legal bases besides consent can be utilized, such as when processing is essential for organization's or a third party's legitimate interests. [67]

b) Contractual Performance:

Processing is permitted if it is necessary for the performance of a contract to which the data subject is a party, or to take steps at the request of the data subject prior to entering into a contract. This ensures that data processing is essential for fulfilling contractual obligations.[68]

c) Legal Obligation

---

[66] Mark Foulsham, Brian Hitchen, and Andrew Denley, GDPR : How To Achieve and Maintain Compliance (Routledge 2019) <https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1996589&site=ehost-live> accessed 26 May 2024.
[67] ibid.
[68] 'Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR)' (n 11).

Organizations may process personal data if it is necessary for compliance with a legal obligation to which the data controller is subject. This ensures that data processing can occur to fulfil legal requirements, such as tax obligations or employment law standards. [69]

d) Vital Protection:

This basis allows for data processing that is necessary to protect the vital interests of the data subject or another individual. This typically pertains to cases where someone's life or physical safety is at risk, such as in medical emergencies. [70]

e) Public Interest:

Data processing may be justified if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller. This basis is often invoked for public agencies and institutions when processing data for societal or governmental purposes. [71]

f) Legitimate Interest:

This basis allows for processing when it is necessary for the purposes of the legitimate interests pursued by the data controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. This legal basis requires a careful balancing test between the organization's interests and the rights of individuals. [72]

[69] ibid.
[70] ibid.
[71] ibid.
[72] ibid.

In reality, companies must choose a valid legal justification for processing personal data and disclose to data subjects how they rely on those justifications. Organizations need to carefully assess and clearly communicate the specific reasons they are using, ensuring that individuals understand how their data is being handled. It is important to select the right legal basis and to inform people about this. By doing this, companies show respect for individuals' rights and build trust in how they manage personal information. As data protection rules change, being aware of the reasons for processing personal data will help organizations stay in compliance and practice ethical data management.

2.4 GDPR- Rights of the Data Subject

The acknowledgment of the Rights of the Data Subject empowers individuals to take control of their personal information and ensure its responsible use. These rights, protected in the GDPR, prioritize individual privacy and foster a culture of transparency and accountability in data processing practices.

In this section, will assess GDPR articles 15 to 22 covering the following rights: The right to Access, Right to Rectification, Right to Restriction of Processing, Right to Data Portability, Right to Object, Rights Related to Automated Decision-Making and Profiling, and the Right to be Forgotten[73]:

a) Right to Access

Right to Access (Article 15) gives individuals the right to request and receive a copy of their personal data held by a data controller. This right allows individuals to confirm

[73]ibid.

whether their data is being processed, understand the purpose of the processing, and know the types of data being processed. Data controllers must respond to such requests promptly, typically within one month, and provide the information in a concise, transparent, and easily accessible format.[74]

This right allows data subjects to check the processing of their information, comprehend its purpose, and identify the types of data being handled. However, exercising this right presents difficulties for both data subjects and data controllers. Controllers need to securely verify the identity of those making requests, but many currently employ unsafe methods, such as sending identity documents through unprotected channels. By collectively exercising the right of access, data subjects may help to correct power imbalances between citizens and organizations, thereby promoting more transparent data practices.[75]

b) Right to Rectification

Right to Rectification (Article 16) allows individuals to request the correction of inaccurate or incomplete personal data. If a data subject identifies that their personal data is incorrect or outdated, they can ask the data controller to amend this information. The data controller must ensure the rectification is made without unnecessary delay, ensuring that the data remains accurate and up to date. [76]

Accuracy is defined by Article 29 Working Party as data that is "correct regarding a matter of fact." Inaccurate factual data refers to information that is not objectively true and does not align with reality. Additionally, legal statutes and case law have determined that the concept of accuracy depends on the purpose and context of the data usage. This

[74] ibid.
[75] Coline Boniface and others, 'Security Analysis of Subject Access Request Procedures: How to Authenticate Data Subjects Safely When They Request for Their Data' in Maurizio Naldi and others (eds) (Springer International Publishing 2019) <http://link.springer.com/10.1007/978-3-030-21752-5_12> accessed 20 July 2024.
[76] 'Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR)' (n 11).

implies that data must be sufficiently accurate for its intended purpose without exceeding the necessary level of accuracy.[77]

c) Right to Restriction of Processing

The Right to Restriction of Processing (Article 18) enables individuals to limit how their personal data is used. This right can be exercised under certain circumstances, such as when the accuracy of the data is contested by the individual or if the processing is unlawful, and the individual requests restriction instead of erasure. During the restriction period, the data can still be stored, but not processed, unless the individual gives consent or there are legal obligations that require processing. [78]

d) Right to Data Portability

The Right to Data Portability allows data subjects the possibility to obtain their personal data, which they have shared with a controller. They also have the right to transfer that data to another controller without interference from the original controller. It enables individuals to obtain and reuse their personal data across different services (Article 20). It means that individuals can request to receive their data in a structured, commonly used, and machine-readable format, allowing them to transfer it to another data controller without obstruction. This right enhances individuals' autonomy over their data and promotes competition among service providers. [79]

One effective way to enhance informational self-determination is by enabling data portability. Data subjects should have the right to control their information, deciding when and with whom it can be shared, without losing the ability to reuse it for personal purposes. With data portability, individuals are more encouraged to utilize their data and

---

[77] 'Article 29 Working Party - Guidelines on Transparency under Regulation 2016/679 | European Data Protection Board' <https://www.edpb.europa.eu/our-work-tools/our-documents/article-29-working-party-guidelines-transparency-under-regulation_en> accessed 2 July 2024.
[78] 'Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR)' (n 11).
[79] Paul De Hert and others, 'The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services' (2018) <https://papers.ssrn.com/abstract=3447060> accessed 25 July 2024.

move easily between various services, selecting those that align best with their preferences and policies. These systems enable data subjects to oversee and regulate their online identity. This fosters a human-centred approach, safeguarding against illegal tracking and profiling methods that seek to bypass essential data protection principles.[80]

Additionally, on Recital 68 of the GDPR, data controllers should be encouraged to develop interoperable formats that enable data portability. However, the imposition upon data controllers towards a full interoperability of digital systems is considered minor once they should be encouraged but are not obliged to develop these interoperable formats.[81]

e) Right to Object

The Right to Object (Article 21) gives individuals the ability to challenge the processing of their personal data based on specific conditions. For example, individuals can object to their data being processed for direct marketing purposes or when processing is based on legitimate interests. Upon receiving an objection, the data controller must stop processing the data unless it can demonstrate compelling legitimate grounds for its processing that override the individual's rights. [82]

f) Rights Related to Automated Decision-Making and Profiling

This right protects individuals from decisions based solely on automated processing, including profiling, (Article 22) which can significantly affect them. GDPR states that individuals should not be subject to decisions that are based solely on automated processing unless specific conditions are met, such as explicit consent or necessity for entering into or performance of a contract. This right emphasizes the importance of human oversight and accountability in automated processes. [83]

---

[80] Daniela Copetti Cravo, 'How to Make Data Portability Right More Meaningful for Data Subjects?' (2022) 8 European Data Protection Law Review (EDPL) 52.
[81] 'The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services' (2018) 34 Computer Law & Security Review 193.
[82] 'Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR)' (n 11).
[83] ibid.

g) Right to be forgotten

The Right to be Forgotten (Article 17) allows individuals to request the deletion of their personal data when specific conditions are met. This right can be exercised, for example, when the personal data is no longer necessary for the purposes for which it was collected, when the individual withdraws consent, or when the data has been unlawfully processed. Data controllers must assess these requests and delete data unless there are overriding legal obligations or legitimate grounds for retaining it. [84]

This right has multiple cases of relevance, with the most significant being the 2014 Google Spain[85] ruling. This judgment acknowledged individuals' right to request that search engines remove links to webpages containing personal data that is inaccurate, irrelevant, inadequate, or excessive from search results associated with their names. This right to de-referencing or delisting is interpreted in the CJEU jurisprudence on the basis of the applicable legislation. Its purpose is to safeguard individuals from extended exposure to past embarrassments or inaccuracies online, as well as other potentially harmful information. This was notably demonstrated in the Google Spain case[86], where searching for an individual's name continually brought up their previous financial difficulties.[87]

This right is one of the most important innovations from the GDPR. This right is grounded on the notions of privacy and data protection but at the same time is criticized for being in conflict with freedom of expression. The right to be forgotten has been well received by the masses, however, the criticisms and the concerns against such a right remain valid in the current scenario. It directly contradicts the freedom of speech and the right of the public to know."[88]

---

[84] ibid.
[85] *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECJ Case C-131/12.
[86] ibid.
[87] Nina Gumzej, 'Google Me and Tell Me Who I Am (Not): The Legal Intricacies of Global Delisting Orders in the "Right to Be Forgotten" Cases' (2024) 12 South East European Law Journal (SEE Law Journal) 133.
[88] Shreya Bansal and Deboleena Dutta, 'Right to Be Forgotten: A Critical and Comparative Analysis Special Edition on Intellectual Property, Entertainment and Media Laws' (2018) 5 RGNUL Financial and Mercantile Law Review (RFMLR) 81.

3. Brazil

3.1 Introduction

The LGPD is a remarkable legislative measure in Brazil designed to safeguard the personal information of its people. The LGPD, which addresses privacy and data protection is modelled after the European GDPR and provides extensive guidelines and principles for organisations that process data.

This section will examine the key principles guiding the LGPD, the legal bases for processing personal data, and the rights of data subjects. Companies need to be aware of these rights and put procedures in place that make it possible for data subjects to use them successfully and build a strong ethical perception of the Controllers and Data Processors.

3.2 LGPD - Key Principles

LGPD in it`s Article 6 brings the key principles that guide the processing of data and guarantee a proper way to handle data in the Brazilian ordainment.[89] This section will focus on analysing the following principles: Purpose, Adequacy, Necessity, Free Access, Data Quality, Transparency, Security, Prevention, Non-Discrimination and Accountability.[90]

a) **Purpose:**

   Personal data must be processed for specific, legitimate purposes that are informed to the data subject at the time of data collection. This principle emphasizes that data should not be used for purposes that go beyond what was communicated to the data subject.[91]

[89] Vítor Boas, Gustavo Oliveira and Rodrigo Sampaio, 'Data Protection: An Analysis of the Principle of Purpose: Proteção de Dados: Uma Análise Sobre o Princípio Da Finalidade' (2023) 23 Concilium 456.
[90] 'LEI Nº 13.709 Lei Geral de Proteção de Dados Pessoais (LGPD)' (n 42).
[91] Boas, Oliveira and Sampaio (n 88).

Even data that is publicly accessible (including via the internet) may only be processed if the following principles are adhered to:

- **Purpose**: That is, the purpose for which the data was made public must be respected in any subsequent use by third parties;
- **Good Faith**: There must be no use that distorts the legitimate expectations of the data subjects; and
- **Public Interest**: The public interest that justified the availability of the data must be identified, and the data must be processed specifically within those situations.

It is clear, therefore, that the existence of data for broad access does not remove the protection that must be granted to it, and it is mandatory to comply with all the key principles of the LGPD.

Its relevant to note that in situations where users make their personal data public themselves, it will not be necessary to obtain their consent for the processing of their personal data. However, it is essential to observe that, even in this case, the use of the data will not be entirely unrestricted; it must be conducted in a manner that safeguards the rights and principles outlined in the law.[92]

b) Adequacy:

The data processing must be compatible with the purposes disclosed to the data subject. The relevance of the data being processed in relation to the stated purpose is crucial, ensuring that only necessary data for the intended purpose is collected and used.

While the principle of purpose is concerned with the legitimacy of the purpose of processing, the principle of adequacy analyses legitimacy from the perspective of the data subject's expectations.[93]

[92] Maldonado and Blum (n 39).
[93] ibid.

c) Necessity:

Data processing should be limited to what is strictly necessary for the fulfilment of its purposes. Compliance with this principle requires that, in doing so, the criterion of minimal collection, or the minimization of the database collected, be applied, and that it includes only data that is relevant, proportional to the purpose of the operation, and not excessive. This principle promotes data minimization, demanding that organizations should collect and process only the personal data that is necessary to achieve their objectives. [94]

d) Free Access:

Data subjects have the right to freely access their personal data held by organizations. This principle ensures transparency and that individuals can exercise their rights regarding their data, including knowledge about how their data is being processed. [95]

e) Data Quality:

Personal data must be accurate, complete, and up to date. Organizations have the responsibility to ensure the quality of data and to take steps to update or rectify any inaccurate data to protect the rights of data subjects.[96]

f) Transparency:

Individuals must be informed about the processing of their personal data in a clear and accessible manner. This principle is crucial for building trust and ensuring that data subjects are aware of how their data will be used. [97]

[94] ibid.
[95] ibid.
[96] ibid.
[97] ibid.

g) **Security:**

Organizations must adopt technical and administrative measures to protect personal data from unauthorized access, destruction, alterations, and any form of unlawful processing. This principle focuses on the importance of implementing adequate security measures to safeguard personal data. [98]

h) Prevention:

Organizations should adopt measures to prevent the occurrence of damage to data subjects resulting from the processing of their personal data. This principle emphasizes proactive approaches to data protection, promoting practices that mitigate risks and prevent privacy breaches. [99]

i) Non-Discrimination:

The processing of personal data must not discriminate against individuals based on their personal attributes. This principle is vital for promoting fairness and protecting the rights of all individuals against misuse of their data. [100]

j) Accountability:

Data controllers and processors are responsible for demonstrating compliance with LGPD. This principle emphasizes that organizations must be able to show that they are adhering to the principles and provisions set forth in the law. [101]

The LGPD provides a strong foundation for the protection of personal data in Brazil, based on its main principles, together, these principles create a comprehensive approach to data protection, improving privacy, building trust between Data Subjects and companies, and promoting ethical data practices. The LGPD not only aligns Brazil with

[98] ibid.
[99] ibid.
[100] ibid.
[101] ibid.

global data protection standards but also sets a high bar for the responsible handling of personal data.[102]

3.3 LGPD – Legal Bases for processing personal data

The legal bases for processing personal data are specific conditions defined in the LGPD that justify why an organization is allowed to process personal data. The LGPD Article 7 enumerates ten legal bases, which will be studied bellow: Consent, Contractual Necessity, Legal Obligation, Protection of Life or Physical Safety, Public Interest, Legitimate Interests, Regular Exercise of Rights, Health Protection, Historical, Statistical, Scientific Research, and Tutorship or Guardianship.[103]

a) Consent:

Processing is lawful if the data subject has given their explicit consent for a specific purpose. Consent must be informed, clear, and provided freely, and individuals can withdraw their consent at any time. In this sense, it is argued that the interpretation of consent should be restrictive, and the agent should not extend the authorization granted to them for data processing to other means beyond those agreed upon, to a later time, or for a different purpose.

It's important to consider that there are situations where the agent is allowed to process, the data necessary for the contract, without consent, as long as the data subject is a party to or is in negotiations for a contract. It is possible to consider examples such as situations where the data subject acquires products or services for delivery, requiring knowledge of their full name, address, and other necessary details for the completion of the contract.[104]

---

[102] Boas, Oliveira and Sampaio (n 88).
[103] 'LEI Nº 13.709 Lei Geral de Proteção de Dados Pessoais (LGPD)' (n 42).
[104] Chiara Spadaccini de Teffé and Mario Viola, 'Tratamento de dados pessoais na LGPD: estudo sobre as bases legais' (2020) 9 Civilistica.com 1.

b) Contractual Necessity:

Processing is permissible if it is necessary for the fulfilment of a contract to which the data subject is a party or for taking pre-contractual steps at the request of the data subject.

c) Legal Obligation:

Organizations may process personal data to comply with a legal obligation that the data controller is subject to, such as tax obligations or labour laws.

The processing can also be based on the regular exercise of rights in judicial, administrative, or arbitral proceedings, a broad legal basis that authorizes the use of personal data in processes to ensure the right to produce evidence by one party against another. The regular exercise of rights includes actions by ordinary citizens authorized by the existence of a right defined by law and conditioned by the regularity of exercising that right. It is understood that it would not be reasonable for a party to be deprived of legitimately defending itself, having to depend on the consent of the opposing party to present certain evidence or information to defend its interests. Therefore, this protects the right to a full defence and the due process.[105]

d) Protection of Life or Physical Safety:

This basis allows for processing that is necessary to protect the life or physical safety of the data subject or another individual, such as in emergency situations.

e) Public Interest:

[105] ibid.

Processing is lawful when necessary for performing a task carried out in the public interest or in the exercise of official authority vested in the data controller. This often pertains to public bodies or institutions.

f) Legitimate Interests:

Organizations may process personal data for legitimate interests pursued by the data controller or a third party, provided that such interests do not override the rights and freedoms of the data subject.

g) Regular Exercise of Rights:

Processing is allowed when necessary for the regular exercise of rights in judicial, administrative, or arbitration proceedings.

h) Health Protection:

Processing is lawful when necessary for protecting the health of the data subject or third parties, especially in the context of healthcare and public health.

i) Historical, Statistical, or Scientific Research:

Personal data may be processed for purposes of research, development, or statistical analyses, provided that this processing is carried out in accordance with sufficient safeguards.

j) Tutorship or Guardianship :

Processing can occur if it is necessary for the tutorship or guardianship of individuals who cannot fully express their will, ensuring that their rights are respected.

LGPD offers flexibility while maintaining strict data subject protection measures. Every legal basis is made to reach a compromise between the necessity of processing data and people's fundamental rights, guaranteeing that data is managed in an ethical and responsible manner. This legal framework fosters transparency, accountability, and trust between data subjects and organizations in addition to improving the protection of

personal data. Because of this, the LGPD is an essential tool for promoting a safe environment in the processing of data in Brazil.

3.4 LGPD- Rights of the Data Subject

The LGPD grants specific rights to individuals, known as data subjects, concerning their personal data. These rights are designed to give individuals greater control over the handling of their personal information, similar to protections established by the GDPR. Below are the essential rights recognized by the LGPD (Article 18) that empower individuals to manage their data and ensure transparency in its use. They are: Right to Access, Right to Confirmation of Existence of Processing, Right to Correction, Right to Data Portability, Right to the Security of Personal Data, Right to Information, Right to Revoke Consent, Right to Object, and Right to be Forgotten.[106]

a) Right to Access:

Individuals have the right to access their personal data that the data controller holds. This includes information about the processing purpose, data categories, storage periods, among other relevant information. The right to access data presupposes prior knowledge or confirmation of the existence of processing. Indeed, if the existence of personal data processing is undisputed, the data subject can access the data and also obtain a range of information processed regarding himself.[107]

b) Right to Confirmation of Existence of Processing:

Data subjects have the right to obtain confirmation from data controllers about whether their personal data is being processed. They can request information regarding the

[106] 'LEI Nº 13.709 Lei Geral de Proteção de Dados Pessoais (LGPD)' (n 42).
[107] Maldonado and Blum (n 39).

processing activities involving their data. In this sense, and without requiring justification, every data subject has the right to simply confirm the existence of the processing of their personal data. This specific right is related to the principle of transparency.[108]

c) Right to Correction:

Data subjects have the right to request the correction of incomplete, inaccurate, or outdated personal data. Individuals can also provide additional information to supplement their data. Seeking to give effect to the principle of informational self-determination, the LGPD provides for the rights to correct incomplete, inaccurate, or outdated data.[109]

d) Right to Data Portability

Data subjects have the right to receive their personal data in a structured, commonly used, and machine-readable format. They can also request the transfer of their data to another data controller when technically feasible. The LGPD provides the right to data portability, but the legal provision was extremely brief about this right establishing that data portability will be performed among a direct transfer of data, upon express requisition, according to the national authority provided regulation, respecting trade secrets. The possibility to receive a copy of the data (and to transfer this data to another data controller, in the present or the future) in Brazil is inside the right of access."[110]

e) Right to the Security of Personal Data:

Individuals have the right to be informed about any security incidents that may affect their personal data, particularly if such incidents may result in significant risk to their rights and freedoms. This right also provides for the use of technical and administrative

[108] ibid.
[109] ibid.
[110] Cravo (n 79).

measures capable of protecting personal data from unauthorized access, as well as from accidental or unlawful destruction, loss, alteration, communication, or dissemination.[111]

f) Right to Information:

Data subjects are entitled to be informed about the option to consent to the processing of their personal data and the consequences of declining to provide consent. This right is also approached in the doctrine as Informational self-determination consists of the data subject's personal control over the handling of their information. It is interpreted as an extension of individual freedoms. It is the right that ensures every data subject can be aware of the storage and use of their information by third parties, as well as control, question, correct, block, withdraw, or rectify their data.[112]

g) Right to Revoke Consent:

Individuals have the right to revoke their consent for the processing of their personal data at any time, and the data controller must provide a simple and free method for this revocation. It is also essential to emphasize that the legislator was concerned with ensuring that revocation could be made at any time, free of charge and facilitated, through a declaration by the data subject. The importance given to the data subject's consent for actions involving their information is evident, as they not only give or revoke the consent for the processing to begin but also decide if the processing should be terminated if they do not agree with the steps to be taken by those handling their information.[113]

h) Right to Object:

---

[111] Maldonado and Blum (n 39).

[112] 'O Direito à Autodeterminação Informativa Na Lei Geral de Proteção de Dados: Empoderar Para Efetivar / Semantic Scholar' <https://www.semanticscholar.org/paper/O-direito-%C3%A0-autodetermina%C3%A7%C3%A3o-informativa-na-Lei-de-Pereira/a9ffbf5b2265bfb67f2c07b846c1dfca690918fa> accessed 27 July 2024.

[113] Lys Nunes Lugati and Juliana Evangelista De Almeida, 'Da Evolução Das Legislações Sobre Proteção de Dados: A Necessidade de Reavaliação Do Papel Do Consentimento Como Garantidor Da Autodeterminação Informativa', *Revista de Direito* (2020) <https://periodicos.ufv.br/revistadir/article/view/10597> accessed 27 July 2024.

Data subjects have the right to object to the processing of their personal data in certain circumstances, such as when they believe their fundamental rights are being violated.

i) Right to be forgotten

The law does not explicitly establish for the "right to be forgotten," only regulating cases of consent withdrawal and data deletion. To avoid any doubts, it should be understood that what Brazilian law predicts is the possibility of "eliminating unnecessary, excessive, or unlawfully processed data." [114] From a Brazilian perspective, this prerogative is not related to the right to be forgotten and is concerned solely with the possibility of data deletion under these circumstances, as personal data, clearly, must always be necessary, adequate, and lawful.[115]

STF (Highest Court in Brazil) when judging the matter on RE nº 1.010.606, Tema 786, excluded from Brazilian ordainment the Right to be Forgotten due to incompatibility with the Constitution:

> It`s incompatible with the Federal Constitution the idea of the right to be forgotten, understood as a power to prevent the dissemination of truthful and lawfully obtained facts or data and published in analogue or digital media due to the passage of time. Any excesses or abuses in the exercise of freedom of expression and information must be analysed case by case, based on constitutional parameters, especially those relating to the protection of honour, image, privacy and personality in general, and express and specific legal provisions in the criminal and civil spheres.[116]

[114] Maldonado and Blum (n 39).
[115] ibid.
[116] 'RE 1010606 Tema 786 STF' <https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5091603&numeroProcesso=1010606&classeProcesso=RE&numeroTema=786> accessed 4 July 2024.

Individuals may request the deletion of their personal data when it is no longer needed for the purposes for which it was collected, or if they withdraw their consent. However, this right is subjected to a thorough analysis in case by case.

The LGPD aligns Brazilian data protection standards with global practices, in special the GDPR in Europe and also provides balance between the processing of data and the right for privacy of the individuals.

4. Comparative analysis

While both regulations share a commitment to protecting personal information, they exhibit distinct approaches, the GDPR and LGPD emphasizes the importance of transparency, accountability, and fairness in data processing. The LGPD, while reflecting the idea of the same principles as GDPR, uses slightly different terminology and structure. Both frameworks emphasize the need for responsible data handling, the LGPD adds nuance to the principles by stressing adequacy and necessity, suggesting a more contextual approach to data processing.[117]

When analysing their take on legal bases to process personal data, the LGPD extends the list beyond the GDPR, recognizing specific contexts like credit protection and research, which highlights Brazil's approach to balancing data protection with specific societal needs.[118]

Both regulations grant extensive rights to data subjects, empowering them to control their personal information actively, but the LGPD also highlights the design of its rights in a manner tailored to Brazilian cultural and legal landscapes. This is a coherent difference to be expected the GDPR has to accommodate provisions for a big block of countries and the LGPD can only focus on Brazil. The main difference in their take on the rights of subjects is the Right to be Forgotten, the Brazilian legislation does not recognize it as

[117] Maiara Rogalewski and Nelson Vidal, 'Lei Geral de Proteção de Dados: Uma Análise Frente Aos Direitos e Garantias Fundamentais' (2023) 5 Academia de Direito 261.
[118] Teffé and Viola (n 103).

compatible with their Federal Constitution, even though in a case-by-case analysis it can support the erase of data supported in other rights.[119]

Both GDPR and LGPD share core principles and the aim of protecting personal data and ensuring individual rights, even though they have differences in their terminology and specific rights reflect the unique contexts of the European and Brazilian regulatory environments. The alignment of both frameworks illustrates a global trend toward more robust data protection, emphasizing the importance of privacy rights.

Chapter 3

Enforcement and Remedies

Introduction

Enforcement is mechanisms and procedures established by regulatory bodies to certify compliance with data protection laws. Remedies refer to the corrective actions or compensatory measures available to individuals who have experienced violations of their rights under data protection laws. Considering the framework established by the GDPR and LGPD, the mechanisms for remedies and enforcement are essential. They empower data subjects and ensure that organizations adhere to data protection principles. This chapter explores the Obligations of Controller and Processor, Controller and Processor Penalties, the duties of the Data Protection Officer, the independence of the Data Protection Authorities to better understand and the enforcement mechanisms employed

[119] Renato Opice Blum, Rony Vainzof and Henrique Fabretti Moraes, ‘ Teoria e Prática de acordo com a LGPD e o GDPR’ <https://bdjur.stj.jus.br/jspui/handle/2011/150187> accessed 28 July 2024.

by the authorities and the remedies available for individuals in case of a breach in their right for data protection in the GDPR and LGPD.

2. European Union

2.1 Introduction

This section will explore the obligations that data controllers and processors must obey under GDPR, as well as the penalties they may incur for non-compliance. It will highlight the critical role of the Data Protection Officer (DPO) in ensuring that entities meet their legal duties and maintain compliance with data protection laws. Additionally, will examine the functions of Data Protection Authorities (DPAs), which play a central role in overseeing compliance with the GDPR, along with the various mechanisms of enforcement available to address violations. Finally, will discuss the remedies and measures that individuals can pursue in cases of non-compliance, understanding how these elements work together to protect personal data and uphold individuals' rights throughout the EU.

2.1 Obligations for Controller and Processor

The GDPR imposes specific obligations on both data controllers and data processors to safeguard the protection of personal data and the rights of individuals. These obligations create a framework of accountability and transparency that organizations must follow while processing personal information. This section highlights key obligations: Conducting Data Protection Impact Assessments, Designation of Data Protection Officers, Reporting Data Breaches, among others. Understanding these responsibilities is crucial for compliance and fostering trust in data handling practices.

a) Data Protection Impact Assessment

A significant aspect of the GDPR lies in its focus on proving compliance with its reinforced data protection principles and encouraging increased accountability for any non-compliance. The Data Protection Impact Assessment (DPIA) it's an assessment to determine how personal data will be processed, the necessity and proportionality of the processing, and measures taken to mitigate risks. Controllers are required to conduct DPIAs under certain circumstances when initiating new projects or processing activities that could pose risks to the rights and freedoms of data subjects.[120]

The DPIA serves as an evaluation of how the suggested processing operations will impact the protection of personal data. It is designed to outline the processing activities, evaluate their necessity and proportionality, and assist in managing risks to individuals' rights and freedoms by assessing those risks and determining appropriate measures to mitigate them. Certain types of processing that are included under this requirement involve sensitive personal data, automated "profiling" of individuals, or processing activities conducted on a large scale. The idea is identifying potential impacts, so organizations can take steps to protect data subjects and ensure legal compliance. [121]

b) Designation of the Data Protection Officer

The appointment of a Data Protection Officer (DPO) is mandatory for certain organizations under the GDPR. The main responsibilities of the DPO are to supervise compliance with data protection laws, act as a liaison between individuals and regulatory bodies, and offer advice on data protection-related issues. Organizations can show their dedication to data protection and guarantee accountability throughout their operations by appointing a DPO. In addition to providing training, the DPO is in charge of keeping an eye on compliance and

[120] Arturo J Carrillo and Matías Jackson, 'Follow the Leader? A Comparative Law Study of the EU's General Data Protection Regulation's Impact in Latin America' (7 June 2022) <https://papers.ssrn.com/abstract=4130437> accessed 15 July 2024.
[121] ibid.

offering advice on Data Protection Impact Assessments and breach notifications.[122]

c) Notification of Personal Data Breaches

On GDPR articles 33 and 34, it was introduced the obligation of notifying the national supervisory authority and data subjects must be informed in the event of a data breach,. A breach is any security event that leads to the unintentional or intentional loss, alteration, disclosure, or access to personal information. The extent of personal data breaches can vary, from small ones with no repercussions to large ones that could seriously jeopardize people's rights and liberties.[123]

It is required from controllers to notify supervisory authority about the breach within 72 hours, if the reporting is not made within that timeline, the reasons for the delay should be explained. The notification must contain comprehensive and relevant details to the nature of the breach, the categories and approximate number of persons and files involved, the contact information for the Data Protection Officer or other point of contact for further information, a description of the likely consequences of the breach and a description of the steps taken or proposed to be taken to address the breach, including any mitigation measures.[124]

d) Standard for Consent

The legislation establishes a higher standard for obtaining consent from individuals to process their personal data. Consent must be informed, specific, and unambiguous, provided through clear affirmative action. Organizations must ensure that individuals are fully aware of their right to withdraw consent and that such a process is straightforward and accessible.[125]

---

[122] Aurimas Šidlauskas, 'The Role and Significance of the Data Protection Officer in the Organization' (2021) 44 Socialiniai tyrimai 8.
[123] 'Breach Notification in the General Data Protection Regulation' (2023) 09 Voice of the Publisher 334.
[124] ibid.
[125] Mark Foulsham, Brian Hitchen, and Andrew Denley (n 65).

e) Governance and Accountability

Organizations must also provide training to staff involved in data processing to ensure that everyone understands their responsibilities under the GDPR. Requiring organizations to implement measures that demonstrate their compliance with data protection laws, this includes maintaining detailed records of processing activities, conducting regular audits, and ensuring that appropriate data protection policies and procedures are in place.

2.1.2 Controller and Processor Penalties

Non-compliance with the GDPR carries severe consequences, with fines of up to €20 million or 4% of the organization's annual global proceeds. The significance of obeying data protection rules and upholding strong compliance procedures is emphasized by these possible fines. Regulators have the authority to fine an organization depending on a variety of criteria, including the type of violation, how serious it is, and how cooperative the company was during the investigation.[126]

The major causes fall into the following major groups of infractions:

- Insufficient legal basis for data processing;
- Non-compliance with general data processing principles;
- Insufficient technical and organizational measures to ensure information security.

An insufficient legal basis for data processing describes a scenario where an organization lacks a valid legal justification for collecting, storing, or utilizing personal data. This

[126] Josephine Wolff and Nicole Atallah, 'Early GDPR Penalties: Analysis of Implementation and Fines Through May 2020' (14 December 2020) <https://papers.ssrn.com/abstract=3748837> accessed 22 July 2024.

situation may arise when an organization has not obtained the required consent from the individual whose data is being processed or when there is no valid legal rationale for processing the data, such as a legitimate interest or a legal obligation. Non-compliance with general data processing principles indicates that an organization fails to adhere to the fundamental data processing principles established in the regulation. Lastly, insufficient technical and organizational measures to ensure information security signifies that an organization lacks the necessary safeguards to protect personal data from unauthorized access, disclosure, alteration, or destruction.[127]

2.3 DPO duty

The GDPR also introduced the role of DPOs, under Article 37, there are certain situations where a DPO must be designated, but a DPO is not required under all circumstances. The DPO (Data Protection Officer) has the responsibility of overseeing the organization's compliance to data protection regulations. Making sure the company abides by the guidelines provided in the GDPR. The DPO assists in avoiding possible infractions that might result in the need for remedies or enforcement actions. [128]

According to Article 37(1) of the GDPR, the DPO must be appointed when: 1. The processing is carried out by a public authority or body, except for courts acting in their judicial capacity, 2. When the core activities of the organization consist of processing operations that require regular and systematic monitoring of data subjects on a large scale; 3. When the core activities involve large-scale processing of special categories of personal data or data related to criminal convictions and offenses.[129]

The DPO can either be an internal employee of the organization or an external third party. The DPO has at least the following responsibilities as instated in Article 39[130]:

---

[127] 'An Analysis of Infractions and Fines in the Context of the GDPR' [2023] International Journal of Marketing, Communication and New Media <http://u3isjournal.isvouga.pt/index.php/ijmcnm/article/view/758> accessed 22 July 2024.
[128] Abigayle Erickson, 'Comparative Analysis of the EU's GDPR and Brazil's LGPD: Enforcement Challenges with the LGPD Notes' (2018) 44 Brooklyn Journal of International Law 859.
[129] 'Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR)' (n 11).
[130] ibid.

1. To inform and advise the controller or processor and their employees about their obligations under the GDPR and other relevant data protection laws of the European Union or individual Member States.
2. To oversee compliance with the GDPR, other applicable data protection laws, and the policies of the controller or processor regarding personal data protection. This includes defining responsibilities, raising awareness, training staff involved in processing activities, and conducting related audits.
3. To offer advice when requested concerning Data Protection Impact Assessments (DPIAs) and to monitor their implementation.
4. To engage with the supervisory authority.
5. To serve as the primary contact for the supervisory authority on processing-related issues, including prior consultations as mentioned in Article 36, and to consult on additional matters when necessary.

Additionally, in carrying out these responsibilities, the DPO must consider the risks associated with processing operations while taking into account the nature, scope, context, and purposes of the data processing. If the organization chooses not to follow any advice given by the DPO, it should document the decisions made and the reasons behind them, as this may help demonstrate accountability. It is crucial to note that even though the DPO monitors compliance with the GDPR within an organization does not make the DPO personally responsible for any regulatory violations. The responsibility for GDPR compliance lies with the data controller or data processor, not with the DPO.[131]

Appointing a DPO can enhance compliance and serve as a competitive advantage, signalling that the organization values data as a key asset essential to its success. As corporate responsibility grows, it is acknowledged that businesses and public services are guided by values and cannot be evaluated solely on quantifiable performance metrics.

[131] Aurimas Šidlauskas, 'The Role and Significance of the Data Protection Officer in the Organization' (2021) <https://www.semanticscholar.org/paper/The-Role-and-Significance-of-the-Data-Protection-in-%C5%A0idlau skas/5d407c710da2174b5e9deec9935357598bb85dd9> accessed 25 July 2024.

Responsibility means thinking about the consequences of the organization in relation to others and clear lines on how to reach accountability.[132]

2.4 DPA - National Data Protection Authority

The GDPR and it's right to the protection of personal data its based on three main points: the obligations of data controllers, the rights of data subjects and the role of data protection authorities. Data Protection Authorities are independent public authorities established by each EU Member State to oversee the enforcement of data protection laws, ensure compliance with the GDPR, and protect individuals' rights regarding their personal data. [133]

DPAs are responsible for monitoring compliance with the GDPR within their respective jurisdictions. They have the authority to investigate complaints, conduct audits, and impose fines for non-compliance. Their Key Functions are Advisory, Handling Complaints, Cooperation with Other DPAs, Public Awareness and Education, and Issuing Guidelines as an institute.[134]

- **Advisory Role:**

They provide guidance and advice to organizations about their obligations under the GDPR, helping them understand how to implement data protection measures effectively. (Article 57(1)(a)

- **Handling Complaints**:

DPAs receive and address complaints from individuals who believe their data protection rights have been violated(Article 77). They investigate these complaints and take appropriate action.

---

[132] Thomas Kahler (ed), Turning Point in Data Protection Law: Two Years GDPR on DPOblog.Eu (1st edition, Nomos 2020).
[133] A Giurgiu and T A Larsen, 'Roles and Powrs of National Data Protection Authorities' (2016) 2 European Data Protection Law Review 342.
[134] 'Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR)' (n 11).

- **Cooperation with Other DPAs:**

Under the One-Stop-Shop mechanism of the GDPR, (Article 60) DPAs cooperate with each other, especially in cross-border cases involving data processing activities that affect individuals in multiple EU countries. [135]

- **Public Awareness and Education:**

DPAs work to raise public awareness about data protection rights and responsibilities(Article 57(1)(b). They provide resources and information to help both individuals and organizations understand the GDPR.

- **Issuing Guidelines:**

DPAs issue guidelines and recommendations(Article 70) on various aspects of data protection, including data processing activities, consent requirements, and Data Protection Impact Assessments (DPIAs).

Although Data Protection Authorities (DPAs) are national organizations set up under local law, they perform their duties based on EU law. The GDPR introduces two types of responsibilities for DPAs: Single and Collaborative.

Single competence means that a DPA can handle a case by itself, which is typically based on where the data processing takes place. This means that the DPA has exclusive authority, especially when the processing is done by public authorities or involves courts acting in their official roles. In these situations, no other DPA can interfere.[136]

However, to ensure consistent decision-making, if a case has broader implications beyond local concerns, the DPA must inform the DPA that oversees the main establishment of the data controller or processor. This DPA will then decide whether to get involved in the case. If it chooses to engage, the responsibility becomes Collaborative, meaning multiple DPAs work together on the issue.[137]

Article 52 emphasizes the importance of independence for Data Protection Authorities (DPAs). Not only must a DPA operate independently in its functions, but its individual members must also act without outside influence. For companies operating in multiple

[135] ibid.
[136] Giurgiu and A Larsen (n 132).
[137] ibid.

Member States, they must comply with the national rules enforced by different DPAs, each responsible for supervising the company's processing activities.[138]

However, under the new regulations, such companies will have a single DPA as their main point of contact. If a company operates in more than one Member State and has at least one establishment in the EU, it will interact with one primary DPA, known as the lead DPA. Through the new 'one-stop-shop' mechanism, the lead DPA will oversee the company's processing activities across the EU, working together with other relevant DPAs. Additionally, the regulations outline specific timelines and responsibilities for this cooperative approach among DPAs. In cases involving multiple countries, the lead DPA must consult all concerned DPAs before taking any actions.[139]

The lead DPA is responsible for sharing all relevant information and sending draft decisions to the other involved DPAs. These other DPAs have four weeks to raise any objections to the draft. If the lead DPA agrees with any objections, it must revise the draft decision and submit it again for feedback within two weeks. Once an agreement is reached, the lead DPA will adopt the decision and notify the company's main establishment. It must also inform the other relevant authorities and the European Data Protection Board (EDPB), as well as the authority that handled the complaint, if needed.[140]

The Consistency Mechanism is crucial for ensuring that data protection laws are applied uniformly across the EU in cases that involve multiple countries. The EDPB plays a central role in this process, alongside the concerned and lead DPAs. The EDPB replaces the previous Article 29 Working Party (A29 WP) and, unlike its predecessor, has legal authority and the power to issue binding decisions. The European Data Protection Supervisor has investigative powers, corrective powers, authorisation and advisory powers, and power to refer the matter to the CJEU. This change makes the EDPB a much stronger entity in enforcing EU data protection regulations. [141]

The Consistency Mechanism must be followed in two specific situations. First, it is required when a Data Protection Authority (DPA) intends to issue a decision that will have legal effects on processing activities significantly impacting a large number of

[138] ibid.
[139] ibid.
[140] ibid.
[141] Paul Lambert, *Data Protection, Privacy Regulators and Supervisory Authorities* (2020).

individuals in several Member States. Article 64(1) of the Regulation lists certain measures that require a DPA to send a draft decision to the European Data Protection Board (EDPB) for its prior opinion. These measures include things like establishing a list of processing operations that need a data protection impact assessment or approving binding corporate rules. In these cases, consistency is essential for the legality of these measures. While the Regulation does not explicitly grant the EDPB direct binding authority, it does allow for concerned authorities or the Commission to raise issues with the EDPB if a DPA disregards its opinion, which can trigger consistency and give the EDPB the final say. [142]

Second, if the concerned DPAs cannot agree under the one-stop-shop mechanism, or if there are disagreements about which DPA should be the lead authority for the main establishment, the EDPB should step in and make binding decisions. The Regulation allows any supervisory authority, the Chair of the EDPB, or the Commission to request that a matter be reviewed under the consistency mechanism when it broadly affects multiple Member States. [143]

It is important to note that when the EDPB exercises its binding powers, national DPAs lose some of their authority in overseeing EU data protection rules. As a result, DPAs may prefer to resolve issues through cooperation within the one-stop-shop mechanism instead of relying on the consistency mechanism and potentially giving up their decision-making power to the EDPB. [144]

2.5 GDPR - Enforcement Mechanisms

Understanding Enforcement Mechanisms as the procedures established by regulatory bodies to certify compliance with data protection laws. The GDPR establishes several enforcement mechanisms to ensure compliance among organizations that process personal data. The legislation passes to each DPA, the responsibility to enforce the GDPR within their jurisdiction. These independent bodies monitor compliance with the GDPR and have the authority to take various actions to ensure that organizations adhere to data

[142] Giurgiu and A Larsen (n 132).
[143] ibid.
[144] ibid.

protection laws. DPAs can investigate complaints filed by individuals who believe their data rights have been violated, conduct audits of organizations, and impose fines for non-compliance, which can be substantial. [145]

The DPA's can issue fines, warnings, reprimands, and compliance orders, requiring organizations to take specific corrective actions. In cases of severe violations, DPAs may also impose temporary restrictions on data processing activities. The European Data Protection Board (EDPB) supports this process by fostering cooperation between DPAs and ensuring consistent application of the GDPR across Europe. [146]

One of the most significant measures is the imposition of fines and penalties. DPAs can impose substantial fines on organizations that violate GDPR rules. This financial consequence serves as a strong deterrent against non-compliance and emphasizes the importance of adhering to data protection laws.[147]

In addition to fines, DPAs can issue notices and reprimands for less severe breaches. These are intended to inform organizations of their non-compliance, encouraging them to correct their practices without incurring immediate financial penalties. This approach allows organizations a chance to rectify issues before more severe actions are taken. [148]

If an organization continues to disregard GDPR requirements, the DPA can issue orders to comply and corrective measures. This authority allows DPAs to demand that organizations take specific actions to correct their practices and align them with regulatory standards. In cases of severe violations, DPAs may also impose temporary bans on the processing of data, effectively stopping operations until compliance is achieved. [149]

Additionally, the DPAs can work together with the European Data Protection Board (EDPB) to resolve cross-border issues, ensuring that decisions are consistent across Member States. This collaboration is essential for addressing cases where data processing impacts individuals in multiple countries, as the EDPB provides legal support and guidance.[150]

---

[145] Lambert (n 140).
[146] ibid.
[147] ibid.
[148] ibid.
[149] ibid.
[150] ibid.

2.6 GDPR - Remedies Measures

Considering Remedies as the measures that an individual can take in the face of a breach of their Data Protection right, according to the GDPR, the actions possible are: to file a complaint with a Data Protection Authority (DPA) or seek legal action.[151]

If a Data Subject believes their data has been mishandled, they have the right to lodge complaints with Data Protection Authorities from where they live, where they work or in the Member State where the alleged infringement occurred, if they believe their personal data has been mishandled or their rights under GDPR have been infringed.

If they are not satisfied with the DPA's response, they have the right to seek legal action in court against the organization that is responsible for the violation. Individuals can also claim compensation for any damages they have suffered as a result of the violation, whether it's financial loss or emotional distress. Additionally, they may ask a court to issue an injunction to stop the organization from continuing any unlawful processing of their data. [152]

Without affecting any other administrative or non-judicial remedies, not only they can seek legal action against organizations that breached their rights, but also can seek an effective judicial remedy against any legally binding decision made by a data protection supervisory authority that pertains to them. This ensures that both data subjects and organizations can challenge such decisions and seek redress in a court of law, reinforcing their rights in the context of data protection. [153]

These measures empower individuals to assert their rights and obtain compensation when their data is not protected properly.

---

[151] *Privacy and Data Protection Based on the GDPR* (2020) <https://www.hive.co.uk/Product/Leo-Besemer/Privacy-and-Data-Protection-based-on-the-GDPR/25332019> accessed 20 July 2024.
[152] Lambert (n 140).
[153] *Privacy and Data Protection Based on the GDPR* (n 150).

3. Brazil

3.1 Introduction

When examining Enforcement and Remedies in the Brazilian data protection legislation, central to the enforcement is the National Data Protection Authority (ANPD), which is responsible for overseeing compliance, issuing guidelines, and imposing penalties for violations. The law also outlines specific remedies available to individuals the LGPD aims to promote accountability among data controllers and processors.

This section will explore the obligations that data controllers and processors must obey under LGPD, as well as the penalties they may incur for non-compliance. It will highlight the critical role of the Data Protection Officer (DPO) in ensuring that entities meet their legal duties and maintain compliance with data protection laws. Furthermore, will examine the functions of the Brazilian DPA, the ANPD. To conclude, this section will discuss the remedies and measures that individuals can pursue in cases of non-compliance.

3.1 Obligations for Controller and Processor

Under LGPD, both data controllers and processors are subject to specific obligations designed to ensure the responsible handling of personal data. . This section pays closer attention to the key obligations for Data Controllers and Data Processors.

Data controllers, who determine the purposes and means of processing personal data, are required to obtain explicit consent from individuals before collecting and processing their information, unless other legal bases for processing are applicable. They must provide clear and transparent information regarding data processing activities, including the purposes for which the data is collected and how it will be used. Moreover, controllers are responsible for implementing measures to ensure the security and confidentiality of personal data, and they must notify data subjects and the National Data Protection Authority (ANPD) in the event of a data breach.

On the other hand, data processors, who process data on behalf of controllers, must operate under a written contract that stipulates their responsibilities in relation to the personal data being processed. This contract should include provisions that require the processor to implement appropriate security measures and to assist the controller in fulfilling their obligations under the LGPD. Additionally, under Article 29 and 30, processors are expected to ensure that they only process data in accordance with the instructions provided by the controller and must implement measures to avoid unauthorized access to the data.

The highlight of key obligations are: Data Protection Impact Assessments, Designation of a Data Protection Officer, Notification of Personal Data Breaches, observing Lawful Basis for Processing and Governance and Accountability[154]:

Data Protection Impact Assessments (DPIAs)

The Data Protection Impact Report (Article 38) constitutes a risk management tool for privacy to be used by the controller to assess the impacts of data processing operations on the privacy of the data subjects, arising from the development of new technologies, the offering of products, or the provision of services, it must be conducted when processing operations present high risks to data subjects. This includes scenarios such as large-scale processing of sensitive data, systematic monitoring of publicly accessible areas, or processing involving new technologies that could impact data subjects significantly. [155]

Designation of a Data Protection Officer (DPO):

Appoint a DPO responsible for overseeing data protection strategies and ensuring compliance with the LGPD. The DPO will be responsible for receiving complaints and

[154] 'LEI Nº 13.709 Lei Geral de Proteção de Dados Pessoais (LGPD)' (n 42).
[155] Blum, Vainzof and Moraes (n 118).

communications from data subjects and the National Data Protection Authority providing clarifications, and taking appropriate measures. The DPO will also advise the company internally on practices for personal data protection and fulfil other functions as determined by complementary regulations.[156]

Notification of Personal Data Breaches

Notify the ANPD and, in certain cases, the data subjects about data breaches. The notification should include details on the nature of the data affected, the affected data subjects, measures taken to address the breach, and potential impacts, and also comply with the timeline for notification as defined by the ANPD.

In Article 48, the LGPD determines that the data controller must notify the national authority and the data subject of a security incident that may pose a relevant risk or harm to the data subjects. The national authority will assess the severity of the incident and may, if necessary for the safeguarding of the rights of the data subjects, instruct the controller to take measures. In determining the severity of the incident, any evidence that appropriate technical measures were adopted to render the affected personal data unintelligible within the scope and technical limits of their services, to unauthorized third parties, will be evaluated.[157]

Lawful Bases for Processing

Ensure that there is a legal bases for processing personal data, such as consent, performance of a contract, compliance with a legal obligation, protection of life, health, legitimate interests, or exercise of rights in legal proceedings(Article 6 and 7).

[156] ibid.
[157] 'LEI Nº 13.709 Lei Geral de Proteção de Dados Pessoais (LGPD)' (n 42).

Governance and Accountability

Maintain records of all categories of processing activities carried out on behalf of a controller, including the details of the controller, categories of processing, international transfers, and security measures.

It is important to consider that keeping the record up to date does not merely mean including new data processing operations(Article 37). It also means excluding operations and their respective personal data that can no longer be processed, even for the purpose of being included in the record.[158]

Overall, the LGPD emphasizes accountability, requiring both controllers and processors to establish practices that respect individuals' rights and maintain the integrity and confidentiality of personal data throughout the entire data processing lifecycle, in so doing, protecting the rights of individuals in Brazil.

3.1.2 Controller and Processor Penalties

Considering the LGPD, both data controllers and processors face specific penalties for non-compliance(Articles 52 and 53). The penalties are designed to ensure that organizations take their responsibilities seriously regarding the protection of personal data. The penalties can go from warnings, reprimands, administrative fines, suspension of data processing or even prohibitions.[159]

Authorities may issue warnings or reprimands for minor violations, may suspend or prohibit the processing of personal data entirely if the organization fails to comply with the LGPD or does not make necessary corrections. Controllers and Processors can incur fines that reach up to 2% of their revenue in Brazil, capped at R$50 million (about 8,200 million EUR) per violation. The fine should reflect the seriousness of the infringement, considering factors such as the nature and extent of the violation and any measures taken to mitigate damage.[160]

---

[158] Blum, Vainzof and Moraes (n 118).
[159] 'LEI Nº 13.709 Lei Geral de Proteção de Dados Pessoais (LGPD)' (n 42).
[160] Blum, Vainzof and Moraes (n 118).

Organizations must be aware of their obligations and potential repercussions for non-compliance, as the ANPD has the authority to impose significant penalties. By implementing proper data protection practices and fostering a culture of compliance, organizations can mitigate risks and maintain trust with their clients and data subjects. Sanctions can be applied either individually or cumulatively; however, the measures taken by the companies for the protection of personal data and privacy will be evaluated as a parameter for the penalty. [161]

With this understanding, there is a clear benefit arising from maintaining regulatory compliance, no only providing agility in identifying any discrepancies and solving, enhancing significantly adverse impacts. The privacy governance program can serve as a mitigating circumstance in the symmetry of administrative sanctions imposed by the ANPD, due to the good faith of the organization in (i) applying the principles and foundations of privacy and data protection to ensure the secure and appropriate handling of data, (ii) adopting corporate mechanisms and procedures capable of minimizing harm through effective corrective measures, and (iii) implementing a policy of good practices and governance. [162]

However, the organization must demonstrate the maturity level of its privacy governance program in order to benefit from the advantages conferred by the LGPD, as mentioned earlier. The mere formal existence of a privacy governance program, without its respective internal control mechanisms, will not meet the minimum requirements set by the LGPD and will therefore be disregarded in the calculation of the penalties. [163]

3.2 DPO duty

The Data Protection Officer (DPO) is the person designated by the controller and operator to act as a channel of communication between the controller, the data subjects, and the

[161] ibid.
[162] ibid.
[163] ibid.

National Data Protection Authority. In the first edition of the law, the term "natural person" was included; however, in the current version, the word "natural" has been removed. Consequently, there is a doctrinal discussion as to whether there was an intention to include legal entities as a possibility for the exercise of the DPO function. The doctrine engages in extensive discussion, and until now there is not a set position.[164]

The DPO will be responsible for receiving complaints and communications from data subjects and the ANPD, providing clarifications, and taking appropriate measures. The DPO will also advise the company internally on practices for personal data protection and fulfil other functions as determined by complementary regulations.[165]

This list of responsibilities is not exhaustive and should include collaboration in ensuring the controller adheres to the principles set in Article 6 of the LGPD. Among these principles is the principle of accountability, which corresponds to the obligation to demonstrate effective measures and compliance with data protection regulations, such as generating evidence in the form of impact reports, keeping records of data processing activities, training employees, and ensuring conformity with the LGPD.[166]

Additionally, the DPO is responsible for ensuring the implementation of internal policies created and for adapting them to new products and needs that may arise over time (Article 41).

3.3 DPA - National Data Protection Authority (ANPD)

The Brazilian Data Protection Authority, is actually named National Data Protection Authority (ANPD in Portuguese) and its an agency of the federal administration, part of executive power of the Presidency and is responsible for safeguarding, implementing, and overseeing compliance with the law throughout the national territory. The ANPD is managed by a Board of Directors that issues its decisions, the members of this board are

[164] Garcia and others (n 41).
[165] Blum, Vainzof and Moraes (n 118).
[166] ibid.

selected by the President of the Republic and appointed by him after approval from the Senate.[167]

In the Article 55 J, the LGPD, provides the key functions of ANPD as Oversight and Enforcement, Handling Complaints, Promoting Awareness, Education on Data Protection and Developing Policies. This article highlights that the ANPD is responsible for overseeing and ensuring compliance with the LGPD, which involves monitoring how personal data is processed across public and private sectors. One of the key responsibilities includes issuing guidelines and regulations that interpret the law, providing clarity to both individuals and organizations regarding their rights and obligations related to data protection.[168]

Additionally, the ANPD has the authority to carry out investigations into potential violations of the LGPD, which may include auditing data processing activities and assessing compliance measures implemented by data controllers and processors. The authority can impose administrative sanctions for non-compliance, such as warnings, fines, and even suspension of data processing activities, depending on the severity of the violation. Another important aspect of the ANPD's duties is to promote educational initiatives aimed at raising awareness about data protection rights among the public and organizations, ensuring that individuals understand their rights in relation to personal data. The last task of the ANPD is nurturing an environment of cooperation with other national and international data protection authorities, facilitating the exchange of information and best practices to enhance the overall framework of data protection.[169]

ANPD is the primary regulatory body for data protection in Brazil, established by the General Data Protection Law (LGPD). However, it's not the only entity involved in data protection matters, as explained bellow[170]:

Consumer Protection Agencies: Organizations like PROCON (Consumer Protection and Defence Program) can also address data protection issues when they intersect with

[167] 'LEI Nº 13.709 Lei Geral de Proteção de Dados Pessoais (LGPD)' (n 42).
[168] ibid.
[169] Garcia and others (n 41).
[170] Maldonado and Blum (n 39).

consumer rights

Public Prosecutor's Office: Can take legal action in cases involving data protection violations that affect collective or diffuse interests.

Judiciary: Courts play a role in interpreting the law and resolving disputes related to data protection.

Sectoral Regulators: Some industries have specific regulators that may also address data protection within their sectors , such as the Central Bank for financial institutions.

While the ANPD is the primary and specialized authority for data protection in Brazil, these other entities also contribute to the overall data protection ecosystem. The ANPD often collaborates with these entities to ensure comprehensive protection of personal data rights in Brazil.

3.4 LGPD - Enforcement Mechanisms

Considering Enforcement Mechanisms as the procedures established by regulatory bodies to certify compliance with data protection laws. The LGPD bring several enforcement mechanisms, the current legislation has as its primary enforcement tool the ANPD, National Data Protection Authority, that can investigate, establish fines, issue warnings, suspensions and prohibitions, analysing the extent of data breaches and the sanctions appropriated for the case.[171]

The administrative sanctions have a big range in value it can reach, but fall somewhat short considering the value possible to reach with the GDPR. These sanctions aim to serve as a barrier and encourage organizations, to have a responsible approach when processing data. By actively engaging in investigations and audits, the ANPD can identify violations and areas for improvement, serving as both a regulatory body and a resource for organizations seeking to align with best practices. The LGPD emphasizes the importance of self-regulation by organizations, encouraging them to establish internal policies and practices that comply with data protection principles. This includes appointing Data

[171] 'LEI Nº 13.709 Lei Geral de Proteção de Dados Pessoais (LGPD)' (n 42).

Protection Officers (DPOs) to ensure adherence to the law and facilitate communication with the ANPD and data subjects.[172]

The ANPD also plays a role in promoting public awareness and education regarding data protection rights. By informing individuals about their rights and how to exercise them, the ANPD strengthens the enforcement framework and empowers data subjects to hold organizations accountable for their data practices. The LGPD allows the ANPD to collaborate with other regulatory bodies and international data protection authorities to enhance enforcement efforts. This collaboration is essential for addressing cross-border data transfers and ensuring consistent application of data protection standards.[173]

The combination of regulatory oversight by the ANPD, judicial remedies for violations, and self-regulatory practices establishes a robust framework for data protection in Brazil. The ongoing collaboration between the ANPD, judicial systems, and organizations will be crucial in adapting to emerging challenges and ensuring that data protection remains a cornerstone of individual rights in Brazil.

3.5 LGPD- Remedies Measures

Remedies are the measures that an individual can take in the face of a breach of their Data Protection right, according to the LGPD, the actions possible are: file a complaint with the National Data Protection Authority or seek legal action.

The LGPD provides that civil damages may be sought through individual or collective legal instruments, such as collective actions triggered by consumer rights associations on behalf of data subjects. In the case of a breach beyond the complaint with the ANPD or

[172] José Jerônimo Nogueira de Lima, 'A estruturação da autoridade nacional de proteção de dados: desafios para a efetividade da LGPD' (*Conteúdo Jurídico*) <https://conteudojuridico.com.br/> accessed 27 July 2024.
[173] ibid.

legal action, its possible that the data subject just want to seek for rectification, deletion, or portability of the data.[174]

Article 42 of the LGPD states that data subjects who experience damage due to the processing of their personal data in violation of the law have the right to seek compensation. This right covers both material damages (quantifiable financial losses) and non-material damages (emotional distress or harm). Both data controllers and data processors can be held responsible for the damages caused by data processing, depending on their specific roles and whether they have adhered to the requirements of the LGPD.[175]

The burden of proof regarding the existence of damage and the causal link between the damage and the data processing typically lies with the data subject. However, if the data subject establishes a breach of the LGPD or lacks access to necessary evidence, courts may consider the circumstances of the case.[176]

4.Comparative analysis

In the fact of what was presented in this chapter, its noticeable how similar is LGPD to the GDPR. Both require controllers and processors to demonstrate accountability and implement appropriate technical and organizational measures to ensure compliance with data protection principles. Both the GDPR and LGPD impose significant penalties for non-compliance, with fines based on a percentage of the organization's annual revenue (GDPR up to 4%, LGPD up to 2%) or a capped amount (GDPR at €20 million, LGPD at R$50 million).

Both regulations encourage or require the appointment of a Data Protection Officer (DPO) to oversee data protection compliance. While GDPR mandates it for certain organizations specified in the law, based on specific criteria such as size and data processing activities, in the LGPD the appointment of a DPO is recommended but not mandatory for all organizations. However, public authorities and entities that process

[174] 'LEI Nº 13.709 Lei Geral de Proteção de Dados Pessoais (LGPD)' (n 42).
[175] Blum, Vainzof and Moraes (n 118).
[176] ibid.

sensitive data under the LGPD must appoint a DPO. [177] Both laws provide mechanisms for individuals to file complaints regarding violations of their data protection rights. Supervisory authorities have the power to investigate complaints and impose sanctions on non-compliant entities. Both GDPR and LGPD grant data subjects the right to seek compensation for damages resulting from violations of their rights.

When analysing the data breach reporting, LGPD requires data controllers to report data breaches to the ANPD and affected individuals, but the specifics around timing and criteria for notification can have some flexibility when compared to GDPR.

The European Data Protection Authorities (DPAs) are independent public authorities that supervise, enforce, and advise on data protection compliance in each EU Member State. They have the authority to investigate complaints and impose penalties. The National Data Protection Authority (ANPD) is established as the regulatory body to oversee and enforce the LGPD in Brazil. Similar to DPAs, the ANPD has the authority to issue guidelines, conduct investigations, and impose penalties for non-compliance."[178]

However, questions have arisen regarding the future efficiency and effectiveness of the ANPD due the technical and functional dependence of the ANPD, as it is linked to the Presidency of the Republic, the Authority could have the power to evade government scrutiny. It is important to note that the topic of data protection and privacy is extremely technical and requires a high degree of specificity and technicality—which would benefit from its own independent structural organization. Finally, the third problem refers to the lack of budgetary independence, due it's direct connection to the Executive Branch, the ANPD will be sustained by the federal budget and can be priority or not depending on the changes in government.[179]

[177] Renato Opice Blum, Rony Vainzof and Henrique Fabretti Moraes, 'Data Protection Officer (encarregado): teoria e prática de acordo com a LGPD e o GDPR' <https://bdjur.stj.jus.br/jspui/handle/2011/150187> accessed 28 June 2024.
[178] Erickson (n 127).
[179] Garcia and others (n 41).

Propositions

As with any legislation, there is always room for improvement, and that is the case of both GDPR and LGPD, for example the position of the Data Protection Officer (DPO), currently its expected to have enough independence to do its job, but there are not direct provisions demanding it. In practice, the Data Protection Officer (DPO) often finds themselves in a challenging position. In one hand, the DPO is an integral part of the system responsible for overseeing the controller's compliance with data protection laws, collaborating with data protection authorities in this capacity. However, on the other hand, the DPO is also an employee of the controller and is embedded within the controller's organization. This dual role can lead to situations where the controller may exert pressure on the DPO to make statements that favour the organization, potentially stretching beyond a legitimate legal interpretation of the GDPR. Furthermore, the controller might attempt to influence the DPO's audit findings, particularly if those findings are deemed to be high risk.[180]

This challenging situation can hold back the DPO's ability to transform the data protection culture within an organization, especially when faced with resistance from the management of the controller. Without the management's support, the successful implementation of the GDPR is unlikely. This applies to both middle and upper management levels of the controller. Nevertheless, the implementation of the GDPR necessitates both organizational and cultural changes within the controller, stemming from the regulation's stricter requirements and the documentation obligations outlined in the Accountability Principle. Since the controller must provide evidence of compliance with the GDPR, it is essential to monitor the organization's risk culture, transparently identify risks, and assess those risks adequately with regard to data subjects.[181]

Based on guidance from the German Federal Data Protection Authority , the DPO must not only report directly to top management but also be directly accountable to the highest management board. Therefore, the DPO should hold the same hierarchical status as, for example, the head of the legal department or the compliance department. This level of

[180] Kahler (n 131).
[181] ibid.

hierarchy will enable the DPO to issue valid legal opinions and conduct thorough audits to help protect the controller from potential fines, damages, and negative publicity.[182]Both legislations could benefit from a more secure structure for the DPO, this would empower DPOs to advocate for compliance initiatives more effectively and ensure that data protection is prioritized at the organizational level.

Different jurisdictions and organizations may define data portability in various ways, leading to confusion about what constitutes data that is portable, it is often confused with other related concepts, such as data access and data transfer. This variability can create challenges for businesses and data subjects attempting to understand their rights and obligations.[183] As such, it is essential to develop policies that promote awareness of this right and clarify its purpose, which is the reuse of data. Given the significant cross-border flow of data, harmonizing this right with international legal frameworks is necessary to facilitate its implementation.

Additionally, providing clearer guidelines on the scope of data covered by data portability will help controllers ensure compliance. Introducing reasonable restrictions or time limits on the exercise of this right could help balance the interests of both controllers and data subjects. Furthermore, promoting interoperability and the use of APIs is crucial for enhancing the efficient flow of data.[184]

The private sector and regulatory authorities should work together to define standards, formats, and appropriate techniques for authentication and security in the transfer of data more definitions and interpretative trajectories regarding the responsibility for carrying out portability, including the rights of third parties, may help in the effectiveness of this right "[185]

[182] ibid.
[183] Cravo (n 79).
[184] ibid.
[185] ibid.

Conclusion

This dissertation has thoroughly explored the significant influence of the General Data Protection Regulation (GDPR) on the development of Brazil's General Data Protection Law (LGPD). Through a comprehensive comparative analysis, the research highlighted the key components of both regulatory frameworks while illustrating how the GDPR served as the base point for the LGPD's creation.

The historical background of both regulations demonstrates that while the GDPR emerged from decades of European privacy legislation, the LGPD was developed more rapidly, drawing inspiration from the Human Rights Convention and the GDPR's framework. This influence is evident in the similar key concepts, principles, and rights afforded to data subjects in both laws. The LGPD's adoption of concepts such as data minimization, purpose limitation, and transparency closely mirrors the GDPR's approach, indicating a clear influence on Brazil's legislative process.

In terms of the rights granted to individuals, the LGPD closely follows the GDPR's model. Both laws provide for rights such as access, rectification, erasure, and data portability. However, the LGPD's interpretation of these rights, particularly the right to be forgotten, shows some nuanced differences, reflecting Brazil's unique legal and cultural context.

The GDPR's influence is also apparent in the LGPD's approach to enforcement and remedies. The establishment of a National Data Protection Authority (ANPD) in Brazil mirrors the role of Data Protection Authorities (DPAs) under the GDPR. Similarly, the concept of Data Protection Officers (DPOs) in the LGPD clearly draws from the GDPR, although with some differences in implementation.

Additionally, the legal bases for processing personal data in the LGPD closely resemble those outlined in the GDPR, demonstrating Brazil's effort to align its data protection standards with international best practices. This alignment facilitates a secure cross-border data transfers and enhances Brazil's position in the global market.

In conclusion, the GDPR's influence on the LGPD, in doing so, the LGPD not only aligned with global trends in data protection but also ensured that it addressed the practicalities of enforcement and compliance within Brazil. By drawing inspiration from the GDPR, Brazil has positioned itself as a country committed to robust data protection standards. This alignment not only benefits Brazilian citizens but also facilitates international data flows and business operations. As both laws continue to be implemented and enforced, their similarities and differences will likely shape the global conversation on data protection, potentially influencing future legislation in other countries. The challenge moving forward will be to maintain this high standard of data protection while allowing for innovation and economic growth in an increasingly data-driven world, assessing the independence in the role of DPO and more independence for the Brazilian National Data Protection Authority.

References

Legislation

‘Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR)’ (General Data Protection Regulation (GDPR)) <https://gdpr-info.eu/> accessed 30 May 202

‘LEI Nº 13.709 Lei Geral de Proteção de Dados Pessoais (LGPD)’ <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> accessed 2 June 2024

Charter of Fundamental Rights of the European Union 2012 (OJ C)

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR)

Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR)

Case Law

Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014] ECJ Case C-131/12

‘RE 1010606 Tema 786 STF’

<https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5091603&numeroProcesso=1010606&classeProcesso=RE&numeroTema=786> accessed 4 July 2024

Books

Blum RO, Vainzof R and Moraes HF, ‘Data Protection Officer (encarregado): teoria e prática de acordo com a LGPD e o GDPR’ <https://bdjur.stj.jus.br/jspui/handle/2011/150187> accessed 28 June 2024

Cravo DC, ‘How to Make Data Portability Right More Meaningful for Data Subjects?’ (2022) 8 European Data Protection Law Review (EDPL) 52

Garcia LR and others, Lei Geral de Proteção de Dados (LGPD): Guia de Implantação (Editora Blucher 2020)

José Jerônimo Nogueira de Lima, ‘A estruturação da autoridade nacional de proteção de dados: desafios para a efetividade da LGPD’ (Conteúdo Jurídico) <https://conteudojuridico.com.br/> accessed 22 July 2024

Maldonado VN and Blum RO, ‘LGPD: Lei geral de proteção de dados: comentada’ <https://bdjur.stj.jus.br/jspui/handle/2011/132481> accessed 20 July 2024

Kahler T (ed), Turning Point in Data Protection Law: Two Years GDPR on DPOblog.Eu (1st edition, Nomos 2020)

Lambert P, Data Protection, Privacy Regulators and Supervisory Authorities (2020)

Articles

‘An Analysis of Infractions and Fines in the Context of the GDPR’ [2023] International Journal of Marketing, Communication and New Media <http://u3isjournal.isvouga.pt/index.php/ijmcnm/article/view/758> accessed 22 July 2024

‘Article 29 Working Party - Guidelines on Transparency under Regulation 2016/679 | European Data Protection Board’ <https://www.edpb.europa.eu/our-work-tools/our-documents/article-29-working-party-guidelines-transparency-under-regulation_en> accessed 2 June 2024

Banisar D and Davies S, ‘Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments’ (1999) 18 John Marshall Journal of Computer and Information Law 1

Bansal S and Dutta D, ‘Right to Be Forgotten: A Critical and Comparative Analysis Special Edition on Intellectual Property, Entertainment and Media Laws’ (2018) 5 RGNUL Financial and Mercantile Law Review (RFMLR) 81

Besemer L, Privacy and Data Protection Based on the GDPR (2020) <https://www.hive.co.uk/Product/Leo-Besemer/Privacy-and-Data-Protection-based-on-the-GDPR/25332019> accessed 27 June 2024

Boas V, Oliveira G and Sampaio R, ‘Data Protection: An Analysis of the Principle of Purpose: Proteção de Dados: Uma Análise Sobre o Princípio Da Finalidade’ (2023) 23 Concilium 456

Boniface C and others, ‘Security Analysis of Subject Access Request Procedures: How to Authenticate Data Subjects Safely When They Request for Their Data’ in Maurizio Naldi and others (eds) (Springer International Publishing 2019) <http://link.springer.com/10.1007/978-3-030-21752-5_12> accessed 2 August 2024

Carrillo AJ and Jackson M, 'Follow the Leader? A Comparative Law Study of the EU's General Data Protection Regulation's Impact in Latin America' (7 June 2022) <https://papers.ssrn.com/abstract=4130437> accessed 16 July 2024

De Hert P and others, 'The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services' (2018) <https://papers.ssrn.com/abstract=3447060> accessed 22 July 2024

De-Yolande M, Doh-Djanhoundji T and Constant G, 'Breach Notification in the General Data Protection Regulation' (2023) 09 Voice of the Publisher 334

Erickson A, 'Comparative Analysis of the EU's GDPR and Brazil's LGPD: Enforcement Challenges with the LGPD Notes' (2018) 44 Brooklyn Journal of International Law 859

Freitas CO de A, Saikali LB and Reis RAO, 'Adoption of the Regulation Model by the Code Architecture and Privacy by Design and by Default Practices for the Regulatory Scenario of Personal Data Protection in Brazil National Doctrine' (2022) 46 Direitos Fundamentais & Justica 363

Giurgiu A and A Larsen T, 'Roles and Powers of National Data Protection Authorities' (2016) 2 European Data Protection Law Review 342

Gumzej N, 'Google Me and Tell Me Who I Am (Not): The Legal Intricacies of Global Delisting Orders in the "Right to Be Forgotten" Cases' (2024) 12 South East European Law Journal (SEE Law Journal) 133

IT Governance (Organization) (ed), EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide (Third edition, IT Governance Publishing 2019) <http://ezproxy.griffith.ie/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=2289418&site=ehost-live> accessed 10 May 2024

Li W, 'A Tale of Two Rights: Exploring the Potential Conflict between Right to Data Portability and Right to Be Forgotten under the General Data Protection Regulation' (2018) 8 International Data Privacy Law 309

Lugati LN and Almeida JED, 'Da Evolução Das Legislações Sobre Proteção de Dados: A Necessidade de Reavaliação Do Papel Do Consentimento Como Garantidor Da Autodeterminação Informativa', Revista de Direito (2020) <https://periodicos.ufv.br/revistadir/article/view/10597> accessed 2 June 2024

Mark Foulsham, Brian Hitchen, and Andrew Denley, GDPR : How To Achieve and Maintain Compliance (Routledge 2019) <https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1996589&site=ehost-live> accessed 30 May 2024

Montagnani ML and Verstraete M, 'What Makes Data Personal?' (2022) 56 UC Davis Law Review 1165

Pereira P 'O Direito à Autodeterminação Informativa Na Lei Geral de Proteção de Dados: Empoderar Para Efetivar / The Right to Informative Self-Determination in the General Data Protection Law: Empowering to Make Effective | Semantic Scholar' <https://www.semanticscholar.org/paper/O-direito-%C3%A0-

autodetermina%C3%A7%C3%A3o-informativa-na-Lei-de-Pereira/a9ffbf5b2265bfb67f2c07b846c1dfca690918fa> accessed 3 August 2024

Rogalewski M and Vidal N, 'Lei Geral de Proteção de Dados: Uma Análise Frente Aos Direitos e Garantias Fundamentais' (2023) 5 Academia de Direito 261

Šidlauskas A, 'The Role and Significance of the Data Protection Officer in the Organization' (2021) <https://www.semanticscholar.org/paper/The-Role-and-Significance-of-the-Data-Protection-in-%C5%A0idlauskas/5d407c710da2174b5e9deec9935357598bb85dd9> accessed 25 July 2024

——, 'The Role and Significance of the Data Protection Officer in the Organization' (2021) 44 Socialiniai tyrimai 8

Sofija V, 'Understanding EU Data Protection Policy'

Teffé CS de and Viola M, 'Tratamento de dados pessoais na LGPD: estudo sobre as bases legais' (2020) 9 Civilistica.com 1

'The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services' (2018) 34 Computer Law & Security Review 193

Ukrow J, 'Data Protection without Frontiers? On the Relationship between EU GDPR and Amended CoE Convention 108 Reports: Practitioner's Corner' (2018) 4 European Data Protection Law Review (EDPL) 239

Victoriano Travieso-Morales YS, 'Understanding Challenges of GDPR Implementation in Business Enterprises: A Systematic Literature Review' <https://www.researchgate.net/publication/377572957_Understanding_challenges_of_GDPR_implementation_in_business_enterprises_a_systematic_literature_review> accessed 12 July 2024

Wolff J and Atallah N, 'Early GDPR Penalties: Analysis of Implementation and Fines Through May 2020' (14 December 2020) <https://papers.ssrn.com/abstract=3748837> accessed 16 July 2024