LATEST EDITION

Comparing privacy laws:
GDPR v. LGPD

September 2022

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

BLUZ ADV

About the authors

OneTrust DataGuidance provides a suite of privacy solutions designed to help organisations monitor regulatory developments, mitigate risk and achieve global compliance.

The OneTrust DataGuidance platform includes focused guidance around core topics (i.e. GDPR, data transfers, breach notification, among others), Cross-Border Comparisons which allow you to compare regulations across multiple jurisdictions at a glance, a daily customised news service and expert analysis.

These tools, along with our in-house analyst service to help with your specific research questions, provide a cost-effective and efficient solution to design and support your privacy programme.

Baptista Luz Advogados was founded in 2004 and covers most areas of corporate law. Its clients include companies and economic groups, both domestic and international, investment funds, angel investors and entrepreneurs. It also operates in other sectors of the economy, particularly advertising, technology, financial institutions, aeronautics, telecommunications, e-commerce, logistics and health. Baptista Luz has a dedicated team for Privacy and Data Protection, with outstanding professionals, who are directly involved with the most important discussions in the area and which deal with data protection compliance on a global and national level. The firm has offices in four different Brazilian cities (São Paulo, Porto Alegre, Florianópolis and Londrina) as well as a unit in Miami.

Contributors

OneTrust DataGuidance: Alexis Kateifides, Iana Gaytandjieva, Victoria Ashcroft

Baptista Luz Advogados: Renato Leite Monteiro, Fernando Bousso, Odélio Porto Junior, Gabriela Moribe

Image production credits:

Cover/p.5/p.51: cnythzl / Signature collection / istockphoto.com
Scale key p6-49: enisaksoy / Signature collection / istockphoto.com
Icon p.12-21: Moto-rama / Essentials collection / istockphoto.com
Icon p.22-23: AlexeyBlogoodf / Essentials collection / istockphoto.com
Icon p.25, 29-37: zak00 / Signature collection / istockphoto.com
Icon p.38-45: AlexeyBlogoodf / Essentials collection / istockphoto.com
Icon p.47-51: cnythzl / Signature collection / istockphoto.com

Table of contents

Introduction

On 25 May 2018, the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') went into effect. In August 2018, Brazil approved Law No. 13.709 of 14 August 2018, General Personal Data Protection Law ('LGPD'), which was further amended by Law No. 13.853 of 8 July 2019. In April 2020, the President of Brazil, Jair Bolsonaro, issued Provisional Measure 959/2020 which provided that the LGPD would be postponed until 3 May 2021 due to the Coronavirus pandemic. Also, on 14 June 2020, Law No. 14,010 entered into force postponing the enforcement of LGPD sanctions until 1 August 2021, likewise due to the Coronavirus pandemic. However, on 26 August 2020, the Federal Senate rejected Provisional Measure 959/2020 and sent Conversion Bill 34/2020 to Bolsonaro, which caused the entry into force of the LGPD on September 2020 with the sanctions being postponed to August 2021. On 26 August 2020, Bolsonaro also signed Decree No. 10,474 of 26 August 2020 which approved the regulatory structure and the framework of the positions of the Brazilian data protection authority ('ANPD'). Finally, on 1 August 2021, the sanctions entered into force in Brazil.

Both laws are comprehensive in nature regarding personal, material and territorial scope. For example, both the GDPR and the LGPD apply to organisations that have a presence in the EU and Brazil respectively as well as to organisations that are not physically located, but which offer goods and services in the jurisdictions, or process personal data in these regions. Also, both laws apply to organisations 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.

In addition, 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 far-reaching 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 Constitution of the Federative Republic of Brazil ('the Constitution').

They also both provide special protection for the processing of sensitive personal data as well as for the processing of children's data. However, there are several nuances between the two laws, for example, regarding the applicable legal basis when sensitive data are processed.

In addition, both laws exclude from their scope the processing of anonymised data, 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.

Further similarities may be found in the rights individuals are entitled to, as well as the obligations controllers and processors are subject to. The exercise of rights must first be attempted directly to the data controller before reaching out to the national supervisory authority. However, under the GDPR, controllers and processors must appoint a data protection officer ('DPO') in specific circumstances as well as carry out a Data Protection Impact Assessment ('DPIA'). Under the LGPD, controllers must appoint a DPO, but does not explicitly establish this obligation for processors. This remains a possibility since the ANPD may create administrative rules demanding them to appoint a DPO. The concept of a DPO also refers to data processors.

This Guide is aimed at highlighting the similarities and differences between the two pieces of legislation in order to help organisations develop their compliance activities.

Structure and overview of the Guide

This Guide provides a comparison of the two pieces of legislation on the following key provisions:

1. Scope
2. Key definitions
3. Legal basis
4. Controller and processor obligations
5. Individuals' rights
6. Enforcement

Each topic includes relevant articles and sections from the two laws, a summary of the comparison, and a detailed analysis of the similarities and differences between the GDPR and the LGPD.

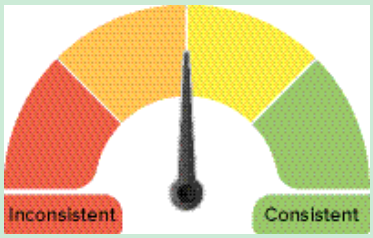
Key for giving the consistency rate

Consistent: The GDPR and LGPD bear a high degree of similarity in the rationale, core, scope, and the application of the provision considered.

Fairly consistent: The GDPR and LGPD bear a high degree of similarity in the rationale, core, and the scope of the provision considered; however, the details governing its application differ.

Fairly inconsistent: The GDPR and LGPD bear several differences with regard to scope and application of the provision considered, however its rationale and core presents some similarities.

Inconsistent: The GDPR and LGPD bear a high degree of difference with regard to the rationale, core, scope and application of the provision considered.



Usage of the Guide

This Guide is general and educational in nature and is not intended to provide, and should not be relied on, as a source of legal advice. The information and materials provided in the Guide may not be applicable in all (or any) situations and should not be acted upon without specific legal advice based on particular circumstances.

This analysis is based on the version of the LGPD as amended by Law No. 13.853 of 8 July 2019, as well as on an English translation of the law, as created by the law firm, Pereira Neto | Macedo Advogados, and accessible at https://www.pnm.adv.br/wp-content/uploads/2018/08/Brazilian-General-Data-Protection-Law.pdf. OneTrust DataGuidance and Baptista Luz Advogados would like to thank Pereira Neto | Macedo Advogados for their efforts and making this translation available for use.

1. Scope

1.1. Personal scope

Fairly consistent

Both the GDPR and the LGPD protect the processing of personal data of individuals. In addition, the GDPR states that the protection is provided regardless of the nationality or residency of the data subject, whilst the LGPD does not explicitly address this point. However, by providing an interpretation according to the Constitution, the protection applies to any person, regardless of the nationality or residency of the data subject. Both pieces of legislation apply to data controllers and processors.

GDPR	LGPD
Articles 3, 4 Recitals 2, 14, 22-25	Articles 1-5

Similarities

The GDPR **only** protects living individuals. Legal persons' personal data is not covered by the GDPR. The GDPR does not protect the personal data of deceased individuals, this being left to Member States to regulate.

The LGPD **only** explicitly protects the personal data of natural persons. Therefore, legal persons' data is also not covered.

Article 4(1) of the GDPR clarifies that a **data subject** is 'an identified or identifiable natural person.'

Article 5(V) of the LGPD clarifies that a **data subject** is a natural person to whom the personal data that are the object of processing refers to.

The GDPR applies to data controllers and data processors, who may be **businesses, public bodies, institutions as well as not-for-profit organisations**.

The LGPD applies to data controllers and data processors, together referred to as **processing agents**, who may be **businesses, public bodies, institutions as well as not-for-profit organisations**.

The GDPR defines a **data controller** as 'the natural and legal person, public authority, agency or other body which, alone or jointly, with others, determines the purposes and means of the processing of personal data.'

The LGPD defines a **controller** as the natural or legal person that is in charge of making decisions regarding the processing of personal data.

The GDPR defines a **data processor** as 'natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.'

The LGPD defines a **processor** as the natural person or legal entity, of public or private law, that processes personal data in the name of the controller.

Differences

The GDPR provides that it 'should apply to natural persons, **whatever their nationality or place of residence**, in relation to the processing of their personal data.'

The LGPD does **not** explicitly state whether it applies to natural persons, **irrespective of their nationality or place of residence**.

1.2. Territorial scope

Fairly consistent

Both the GDPR and the LGPD apply to entities which have a presence in the jurisdiction. The GDPR applies to organisations that have an 'establishment' in the EU, whilst the LGPD applies to data processing operations which are carried out in Brazil.

Both pieces of legislation also have an extraterritorial scope. In particular, they apply to organisations that offer goods and services to data subjects in Europe and Brazil, respectively, regardless of where they are located. It has to be noted that only the GDPR applies to organisations that, although do not have not any presence in the EU, monitor the behaviour of individuals in the EU.

GDPR	LGPD
Articles 3-4 Recitals 2, 14, 22-25	Articles 3-4

Similarities

The GDPR applies to organisations that have a presence in the EU, notably entities that have an '**establishment**' in the EU. Therefore, the GDPR applies to the processing of personal data by organisations **established** in the EU, regardless of **whether the processing takes place in the EU or not**.

With regard to the notion of establishment, there is no equivalent provision in the LGPD defining it. However, the LGPD applies to **data processing operations carried out in Brazil**. The LGPD applies, irrespective of the location of an entity's headquarters, or the location of the data being processed, if the data being processed **belongs to individuals located in Brazil or if the personal data being processed was collected in Brazil**. Data collected in Brazil is defined as data **belonging to a data subject who was in Brazil at the time of collection**.

In relation to the **extraterritorial scope**, the GDPR applies to the processing activities of organisations that **are not established in the EU**, where processing activities are related to the **offering of goods, or services to individuals in the EU**.

The LGPD also applies, **irrespective of the location of an entity's headquarters, or the location of the data being processed**, if the **purpose** of an entity's processing activity is to **offer or provide goods or services to individuals located in Brazil**.

Differences

In relation to **extraterritorial scope**, the GDPR applies to organisations that are not established in the EU, but **monitor the behaviour of individuals**, as far as their behaviour takes place in the EU.

In relation to **extraterritorial scope**, the LGPD **does not** include any specific provisions in relation to processing activities which have the purpose of monitoring the behaviour of individuals in Brazil. However, it mentions that it applies to the processing of personal data of natural persons who are in the national territory, which may be interpreted as monitoring of behaviour the people in the territory regardless of where the data is processed.

GDPR	LGPD
Differences (cont'd)	
There is no equivalent provision in the GDPR.	Article 4(IV) provides that the LGPD will not apply to data processing operations, where the data being processed **originated outside of Brazil**, and are not the object of communication, shared use of data with Brazilian processing agents, or the object of international transfer of data with a country other than Brazil, **provided that the country of origin provides a level of protection adequate to that under the LGPD**.
The GDPR applies to natural persons, **whatever their nationality or place of residence**, in relation to the processing of their personal data.	The LGPD **does not** explicitly provide that it will apply regardless of an individual's nationality or place of residence. However, by providing an interpretation according to the Constitution, the protection applies to any person, regardless the nationality or residency of the data subject. In addition, Article 3 sets out that the LGPD will apply if the personal data being processed belongs to a person who was in Brazil at the time of its collection.

1.3. Material scope

Both pieces of legislation apply to personal data defined as information regarding an identified or identifiable natural person. The GDPR excludes from its application the processing of anonymous data. Similarly, the LGPD excludes from its application 'anonymised data', since it is not considered personal data, unless the anonymisation process has been reversed. According to the LGPD, data can also be considered personal when used to formulate behavioural profiles of a particular natural person, if that person is identified.

The GDPR applies to the processing of personal data by automated means or non-automated means if the data is part of a filing system, whilst the LGPD applies to any processing operation.

GDPR	LGPD
Articles 2-4, 9 Recitals 15-21, 26	Articles 3-5, 11-12

Similarities

The GDPR applies to the '**processing**' of personal data. The definition of 'processing' covers 'any operation' performed on personal data 'such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.'	The LGPD applies to any **processing operation**, which is defined as any operation carried out with personal data, such as collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, deletion, evaluation or control of the information, modification, communication, transfer, dissemination or extraction.
The GDPR applies to the **processing** of personal data. '**Personal data**' is defined as 'any information' that directly or indirectly relates to an identified or identifiable individual.	The LGPD applies to any **processing operation** of personal data. '**Personal data**' is defined as information regarding an identified or identifiable natural person.
The GDPR defines '**special categories of personal data**' as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. The GDPR provides specific requirements for its processing.	The LGPD defines '**sensitive personal data**' as personal data concerning racial or ethnic origin, religious belief, political opinion, trade union or religious, philosophical or political organisation membership, data concerning health or sex life, genetic or biometric data, when related to a natural person. The LGPD provides specific requirements for its processing.
The GDPR excludes from its application the processing of personal data **by individuals for purely personal or household purposes**. This is data processing that has 'no connection to a professional or commercial activity.'	The LGPD excludes from its application the processing of personal data **by natural persons for purely private and non-economic purposes**.

GDPR	LGPD

Similarities (cont'd)

The GDPR excludes **anonymous data** from its application, which is defined as information that 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 LGPD excludes from its application **anonymised data**, which is defined as data related to a data subject who cannot be identified, considering the use of reasonable and available technical means at the time of the processing.
The GDPR excludes from its application data processing in the context of **law enforcement or national security**.	The LGPD excludes from its application data processing done **exclusively for purposes of law enforcement and national security**.
The GDPR provides specific requirements for certain processing situations, including processing for **journalistic purposes and academic, artistic or literary expression**.	The LGPD generally does not apply to processing of personal data done exclusively for **public safety, journalistic, artistic or academic purposes**.

Differences

The GDPR applies to the processing of personal data **by automated means or non-automated means if the data is part of a filing system**.	The LGPD applies to **any processing operation**.
The GDPR does **not** specifically address the processing of anonymised data for profiling purposes.	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.

2. Key definitions

2.1. Personal data

Both the GDPR and the LGPD provide definitions of personal data, sensitive personal data and anonymised data that present a high degree of similarity.

In relation to anonymised data, in order to determine whether reasonable efforts were made to anonymise the data, the LGPD provides for objective criteria for analysis, such as time and cost, but also includes the controller or processor's use of its 'own resources'. Moreover, according to the LGPD, anonymised data can be considered personal when used to formulate behavioural profiles of a particular natural person, if that person is identified.

GDPR	LGPD
Articles 4, 9 Recitals 26-30	Articles 5, 12

Similarities

The GDPR, defines 'personal data' as '**any information relating to an identified or identifiable natural person**' ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.'

The LGPD defines 'personal data' as **information related to an identified or identifiable natural person**.

The GDPR does **not** apply to **anonymised data**, notably data 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 is identifiable. Recital 26 of the GDPR provides that 'to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.' Therefore, all objective factors should be considered, such as the cost and the time required for identification,

The LGPD does **not** apply to **anonymised data**, which is defined as data concerning a subject who cannot be identified, directly or indirectly, considering the use of reasonable technical means available at the time of processing. Under the LGPD, data is not considered anonymised when the anonymisation process to which they were submitted is reversible, considering reasonable efforts. However, besides the objective criteria (cost, time and available technology), the LGPD also adopts a subjective concept, which is the controller or processor's 'use of its own resources' to determine whether the efforts made for the process of anonymisation were reasonable.

GDPR	LGPD

Similarities (cont'd)

taking into consideration the available technology at the time of processing and technological developments.

The GDPR defines **special categories of personal data (or 'sensitive data')** as 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.' The processing of this category of personal data is prohibited unless exceptions apply. See 'Legal Basis' below.

The LGPD defines '**sensitive data**' as personal data on racial or ethnic origin, religious belief, political opinion, union membership or religious, philosophical or political organisation, health or sexual life, genetic or biometric data, when connected to a natural person. The LGPD does not prohibit the processing of sensitive data, but the legal bases for such processing are more restricted. See 'Legal Basis' below.

Differences

The GDPR does not specifically address the processing of anonymised data in the context of profiling.

The LGPD states that if anonymised data is used to create or enhance a behaviour profiling of a natural person, it may be deemed as personal data when the data subject can be identified.

2.2. Pseudonymisation

Fairly consistent

The definition of 'pseudonymisation' included in both pieces of legislation is quite similar. However, the GDPR states that pseudonymised data should be regarded as personal data, while the LGPD is not explicit on this. However, considering that under the LGPD the concept of personal data includes data that might indirectly identify a data subject, pseudonymised data may be considered personal data. In addition, 'pseudonymisation' is only provided for in the LGPD when the processing purpose relates to health research.

Both pieces of legislation mention the process of pseudonymisation as a safeguard that should be taken for reducing risks to the rights of data subjects. Nonetheless, the LGPD only explicitly provides for the use of pseudonymised data in the context of public health research.

GDPR	LGPD
Articles 4, 11 Recitals 26, 28-29	Article 13

Similarities

'**Pseudonymisation**' is defined in the GDPR as 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject 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.'

'**Pseudonymisation**' is defined in the LGPD as the process by which data can no longer be directly or indirectly associated with an individual, except by using additional information kept separately by the controller in a controlled and secure environment.

Differences

The GDPR clearly states that 'personal data that have undergone pseudonymisation, and which could be attributed to a natural person by the use of additional information should be considered as information on an identifiable natural person.'

The LGPD does **not** explicitly state that pseudonymised data should be regarded as personal data, however, it could be interpreted as such, since the definition given indicates the possibility of reidentification.

The LGPD provides that in public health-related studies, research entities which have access to personal data, must process the data exclusively within the entity and strictly for the purpose of conducting studies and surveys in a controlled and safe environment, including, **whenever possible, the anonymisation or pseudonymisation of the data**. A 'research entity' is defined in the LGPD as a body or legal entity of the direct (federal, state and

GDPR	LGPD

Differences (cont'd)

	local government, and their related bodies without a legal personality) or indirect (agencies, foundations, state-owned companies, etc. which have a legal personality of its own) government bodies or a not-for-profit legal entity of private law, legally established under the Brazilian law, with headquarters and jurisdiction in Brazil, that includes in its institutional mission or in its statutory purposes an objective to do basic or applied research of historic, scientific, technological, or statistical nature.

2.3. Controllers and processors

The definitions of controller and processor under the GDPR and the LGPD bear a high degree of similarity.

The GDPR requires that the relationship between the controller and the processor is governed by a contract or other legal act. On the contrary, the LGPD simply states that the processor must conduct the processing pursuant to the instructions provided by the controller, which is responsible for verifying compliance with the same.

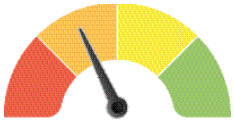
GDPR	LGPD
Articles 4, 28, 30, 82	Articles 5, 37-40, 42-43

Similarities

A **data controller** is defined in the GDPR as 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, **determines the purposes and means of the processing of personal data**; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.'	A **data controller** is defined in the LGPD as the natural or legal person, whether public or private, which is responsible for decisions concerning the processing of personal data.
A **data processor** is defined in the GDPR as 'a natural or legal person, the public authority, agency or any other entity which processes personal data on behalf of the controller.'	A **data processor** is defined in the LGPD as the natural or legal person, whether public or private, which performs the processing of personal data on behalf of the controller.
Under the GDPR, the controller and the processor shall maintain a record of the processing activities under their responsibility.	Under the LGPD, the controller and the processor must keep a record of the personal data processing operations they perform, especially when based on legitimate interest.
Under the GDPR, 'any controller involved in the processing shall be liable for the damage caused by the processing which infringes this Regulation [the GDPR]. A processor shall be liable for the damage caused by the processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to the legal instructions of the controller.'	The controllers who are directly involved in the processing from which the data subject has suffered damages are jointly and severally liable. A processor is jointly and severally liable for the damage caused by the processing when it fails to comply with the obligations of the LGPD or when it has not followed the legal instructions of the controller, in which case the processor equals the controller for liability. Processors are also jointly and severally liable for the damage caused by the processing in cases where they have failed to comply with the obligations and instructions of the controller.

GDPR	LGPD
Similarities (cont'd)	
A controller or processor is exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.	Processing agents shall not be held liable when they are able to prove: (i) they were not involved in the processing of the data; (ii) when, despite the damage, the processing is conducted in accordance with the LGPD; and (iii) the damage is due to the exclusive fault of the data subject or other third parties.
Differences	
The GDPR requires processing by a processor to be governed by a contract or another legal act, 'that is binding on the processor with regard to the controller and that sets out the subject matter and the duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects and the obligations and rights of the controller.'	The LGPD simply states that the operator must conduct the processing according to the instructions provided by the controller, who is responsible for verifying compliance. Under the LGPD there is no obligation to execute a contract or another legal act for the processing conducted by a processor.
The GDPR does not specifically address this point.	Processing agents shall be held jointly liable when the processing consists of a consumer-based service, since it triggers the application of the Law No. 8078 of 11 September 1990, Consumer Protection Code.

2.4. Children



Both the GDPR and the LGPD grant special protection to children's personal data.

With regard to consent to information society services, the GDPR sets the minimum age at 16 years old, though Member States may set a lower age, abiding by the minimum of 13 years of age. Under that age, consent must be given by a parent or legal guardian.

Under the LGPD, consent might be given by a 13 to 18 year old natural person, as long as the processing of their personal data is undergone in their best interest. In cases where children are younger than 13 years old, specific and prominent consent must be given by a parent or person responsible for the child. The age definition of children and adolescents is provided by the Federal Children's and Adolescents Statute 8069/1990 ('the Children's and Adolescent's Statute').

GDPR	LGPD
Articles 6, 8, 12, 40, 57 Recitals 38, 58, 75	Article 14

Similarities

The GDPR states that any information and communication, addressed to a child, should be provided in such a **clear and plain language** that the child can easily understand.

The LGPD states that the information on the processing of children's data should be provided in a **simple, clear and accessible way**, using audio-visual resources when appropriate, in order to provide the information needed by the parents or legal representative and appropriate to the child's understanding.

The GDPR requires controllers to make **reasonable efforts** to verify if consent has been given or authorised by a parent or person responsible for the child, taking available technology into consideration.

The LGPD states that the controller shall make every **reasonable effort** to verify that the consent has been given by the child's representative, considering the available technologies.

Differences

The GDPR explicitly addresses children's consent **only in the context of the offering of information society services**.

Under the GDPR, the minimum age to consent to information society services is **16**, but Member States may provide for a lower age for those purposes, provided that such lower age is not below **13 years**.

The LGPD addresses children's and adolescents' consent with regard to **any processing of their personal data**.

The LGPD does not explicitly state what is the age for consent, although, by interpreting the Children's and Adolescent's and Statute and the Brazilian Civil Code, it is possible to argue that consent might be given by a 12 to 18 year-old natural person (legal definition of adolescents), as long as the processing of their personal data complies with the LGPD's

GDPR	LGPD
Differences (cont'd)	
	requirement that it pursues their best interest. In the case of children younger than **12 years old**, specific and prominent consent must be given by a parent or person responsible for the child. The age for full contractual capacity is 18 years old in Brazil.
Under the GDPR, the consent of a parent or legal representative shall not be necessary in the context of preventive or counselling services offered directly to a child.	Under the LGPD, it is possible to collect children's data without consent when necessary to contact the parents or legal representatives, used once and without storing, or for their protection, and in no case may be shared with a third party without the proper consent.
The GDPR states that specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.	Under the LGPD, controllers shall not condition the participation of children in games, internet applications or other activities upon the provision of personal information beyond what is strictly necessary for the activity.

2.5. Research

The GDPR provisions on research are more flexible than those of the LGPD. In particular, the LGPD provides for a restrictive definition of a 'research body', while the GDPR states that scientific research should be interpreted in a 'broad manner'.

Rules concerning processing for public health research are quite similar, however, the LGPD provisions are more restrictive than the GDPR, since it prohibits the transfer of data to a third party, stating that processing should be conducted within the research body.

GDPR	LGPD
Articles 5, 9, 14, 17, 89 Recitals 33, 159-161	Articles 5, 7, 11, 13, 16

Similarities

According to the GDPR, **the processing of sensitive data is not prohibited when 'necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.'

Under the LGPD, **sensitive data may be processed in order for a research body to conduct its studies**. In this case, the LGPD also recommends the anonymisation of sensitive personal data.

According to the GDPR, special categories of personal data which deserve higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, for example, in the context for studies conducted in the public interest in the area of public health.

Under the LGPD, the processing of personal data for the purpose of public health research shall be conducted exclusively within the body of research and strictly for the purpose of conducting studies and surveys and kept in a controlled and safe environment in accordance with security practices including the anonymisation or pseudonymisation of the data.

Differences

Under the GDPR, the processing of personal data for scientific research purposes should be interpreted 'in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research.'

Scientific research is not defined in the LGPD. Under the LGPD, a 'research body' is defined as the body or entity of the public administration or legal entity of a non-profit private organisation, with headquarters and jurisdiction in Brazil, which includes in its institutional mission or its corporate or statutory objective basic or applied research of historical, scientific, technological, or statistical nature. The legal basis of 'research' is only valid for studies conducted by research bodies that meet the definition mentioned above. Therefore, entities that undergo research to obtain economic advantages cannot rely on the research legal basis to process personal data.

GDPR	LGPD
Differences (cont'd)	
Under the GDPR, where personal data are processed for archiving purposes in the public interest and research purposes, it is possible for Member States to derogate from some data subjects' rights, insofar as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.	Under the LGPD, there are no derogations for data subjects' rights when the processing is for research purposes.
The GDPR provides that 'further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.'	There is no equivalent provision in the LGPD.

3. Legal basis

Both the GDPR and the LGPD require a legal basis to be identified in order to process personal data. Some legal bases are similar, however, both pieces of legislation provide for different legal bases as well.

GDPR	LGPD
Articles 5-10 Recitals 39-48	Articles 7-13

Similarities

Under the GDPR, the legal bases for **the processing of personal data are:** (i) **consent** given by the data subject for one or more specific purposes; (ii) where necessary for the **performance of a contract** to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract; (iii) where necessary for **compliance with a legal obligation** to which the controller is subject; (iv) where necessary in order to **protect the vital interests** of the data subject or of another natural person; (v) where necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller; and (vi) where necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. The processing of personal data strictly necessary for the **purposes of preventing fraud** also constitutes a legitimate interest of the data controller concerned. The processing of personal data for **direct marketing purposes** may be regarded as carried out for a legitimate interest.

Under the LGPD, the legal bases for **the processing of personal data are:** (i) the provision of **consent** by the data subject; (ii) where necessary for the **execution of a contract** or preliminary procedures related to a contract to which the holder is a party, at the request of the data subject; (iii) for the **fulfilment of a legal or regulatory obligation** by the controller; (iv) for the **protection of the life or physical safety** of the data subject or third party; (v) **by the public administration**, for the processing and shared use of data necessary for the execution of public policies provided for in laws and regulations or supported by contracts, agreements or similar instruments; and (vi) where necessary to meet the **legitimate interests** of the controller or third party, except in the case of the fundamental rights and freedoms of the data subject that require the protection of personal data.

Under the GDPR, the legal bases for **the processing of sensitive personal data are:** (i) the data subject has given **explicit consent**; (ii) where necessary for the purposes of **complying with the obligations and exercising specific rights** of the controller or of the data subject in the field of employment and social security and social protection; (iii) where necessary to protect the **vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; (iv) where necessary for the **establishment, exercise or defence of legal claims** or

Under the LGPD, the legal bases for **the processing of sensitive personal data are:** (i) when the data subject or their legal representative **consents**, specifically and distinctly, in a separate manner, for specific purposes, (ii) where necessary for compliance with a **legal or regulatory obligation** by the controller; (iii) where necessary for the **protection of the life or physical safety** of the data subject or third party; (iv) where necessary for the **regular exercise of rights, including in contract and in judicial**, administrative and arbitration proceedings, the latter under the terms of Law No. 9,307

GDPR	LGPD

Similarities (cont'd)

whenever courts are acting in their judicial capacity; (v) where necessary for reasons of substantial **public interest**, on the basis of the Union or Member States law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; (vi) where necessary for the **purposes of preventive or occupational medicine**, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of the Union or Member States law or pursuant to contract with a health professional; (vii) where necessary **for reasons of public interest in the area of public health**, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of the Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; and (viii) where necessary for archiving purposes in the **public interest, scientific or historical research purposes or statistical purposes** based on the Union or Member States law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

of 23 September 1996, (Arbitration Law); (v) shared processing of data necessary for the execution, by the Government, of **public policies** provided for in laws or regulations; and (vi) '**health protection**', in a procedure conducted by health professionals, and by health entities (e.g. agencies responsible for protecting the public health), or a procedure performed in the context of health services.

Differences

There are no further legal bases under the GDPR for the processing of personal data.

Legal bases that only the LGPD provides regarding the processing of personal data include: (i) to conduct **studies by a research body**, guaranteeing, whenever possible, the anonymisation of personal data; (ii) for the regular exercise of rights in **judicial, administrative or arbitral proceedings**; (iii) for the **protection of health**, in a procedure conducted by health professionals or by health entities; (iv) when necessary for **'credit protection' (credit analyses)**.

GDPR	LGPD

Differences (cont'd)

Legal bases that only the GDPR provides for regarding the processing sensitive data include: (i) where the processing is conducted in the course of its **legitimate activities** with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects; and (ii) where the processing relates to **personal data which are manifestly made public by the data subject**.

Legal bases that only the LGPD provides for regarding the processing of sensitive data include: (i) **ensuring the prevention of fraud and to promote the security of the data subject**, in the processes of identification and authentication of registration in electronic systems, safeguarding the rights mentioned in Article 9, and except where fundamental rights and liberties of the data subject which require protection of personal data prevail.

4. Controller and processor obligations

4.1. Data transfers

Fairly consistent

Both the GDPR and the LGPD provide for the transfer of personal data to third countries or international organisations only on specific grounds. Both pieces of legislation recognise the concept of adequacy, as well as other legal grounds for the basis of the international transfer of personal data.

Despite the high level of similarity in the core of the provision, the GDPR includes more prescriptive requirements on legal conditions for transferring personal data.

GDPR	LGPD
Articles 44-50 Recitals 101, 112	Articles 33-35

Similarities

The GDPR **permits the international transfer of personal data** to a third country, a territory or one or more specified sectors within that third country, or an international organisation which ensures an adequate level of protection, as assessed by the European Commission. In the absence of an adequacy decision, the transfer is allowed when the controller or processor has provided appropriate safeguards by means of: (i) binding corporate rules; (ii) standard data protection clauses adopted by the European Commission or by a supervisory authority; (iii) an approved code of conduct; and (iv) an approved certification mechanism.

Other legal grounds on the basis of which data transfers are allowed are: (i) judicial cooperation by means of international agreements; (ii) when the data subject has explicitly consented; (iii) when the transfer is necessary for the performance or conclusion of a contract; (iv) when the transfer is necessary for important reasons of public interest; (v) when the transfer is necessary for the establishment, exercise or defence of legal claims; and (vi) when the transfer is necessary in order to protect the vital interests of the data subject or of other persons.

The LGPD **permits the international transfer of personal data** to countries or international organisations that provide an adequate level of protection of personal data, or when the controller ensures compliance with the regime of data protection by means of: (i) specific contractual clauses for a given transfer; (ii) standard contractual clauses; (iii) global corporate rules; and (iv) valid seals of quality, certificates and codes of conduct.

Other legal grounds on the basis of which data transfers are allowed are: (i) when the transfer is necessary for international legal cooperation among law enforcement agencies, in accordance with instruments of international law; (ii) when the transfer is necessary to protect the life or physical safety of the data subject or of a third party; (iii) when the data subject has given a specific and outstanding consent for the transfers; (iv) when the transfer is necessary for the execution of a contract or preliminary procedures related to a contract; (v) when the transfer is necessary for the regular exercise of rights in judicial, administrative or arbitration procedures; and (vi) when the transfer is necessary for the execution of a public policy or legal attribution of public service.

GDPR	LGPD

Similarities (cont'd)

Further grounds on the basis of which data transfers are permitted are: (i) legally binding and enforceable instruments between public authorities or bodies; and (ii) subject to the authorisation from the competent supervisory authority by either: (a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or (b) provisions to be included into administrative arrangements between public authorities or bodies.

Further grounds on the basis of which data transfers are permitted are: (i) specific contractual clauses for a particular transfer; (ii) when the supervisory authority authorises the transfer; (iii) when the transfer results from a commitment made in an international cooperation agreement; and (iv) when the transfer is necessary for compliance with a legal or regulatory obligation by the controller.

Differences

Other grounds under the GDPR include: (i) the transfer is made from a register which according to the Union or Member States law is intended to provide information to the public and which is open to consultation; and (ii) based on the legitimate interest of the controller if the transfer is not repetitive, concerns only a limited number of data subjects and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data.

The LGPD does not provide for the international transfer of data on the basis of a register which is intended to provide information to the public, nor based on the legitimate interest of the controller.

4.2. Data processing records

Fairly consistent

Both the GDPR and the LGPD establish a legal obligation for controllers and processors to maintain a record of the processing activities under their responsibility. The GDPR details the information that needs to be recorded, whilst the LGPD does not provide such detail.

GDPR	LGPD
Article 30 Recital 82	Article 37

Similarities

Under the GDPR, controllers and processors must maintain a record of their processing activities.

Under the LGPD, controllers and processors must keep records of personal data processing operations carried out by them, especially when based on legitimate interest.

Differences

Under the GDPR, organisations employing fewer than 250 persons need not maintain such a record unless 'the processing is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.'

Under the LGPD, all organisations regardless of their size, number of employees or type of data, need to comply with the record processing obligation. Nonetheless, exemptions can be established by the supervisory authority.

The GDPR establishes that **data controllers must record**: a) the name and contact details of the controller; b) the purposes of the processing; c) a description of the categories of data subjects and of the categories of personal data; d) the categories of recipients to whom the personal data will be disclosed; e) international transfers of personal data, with the identification of third countries or international organisations, and the documentation of suitable safeguards adopted; f) the estimated time limits for erasure of the categories of data; and g) a general description of the technical and organisational security measures adopted.

The LGPD does not detail the information that controllers need to record.

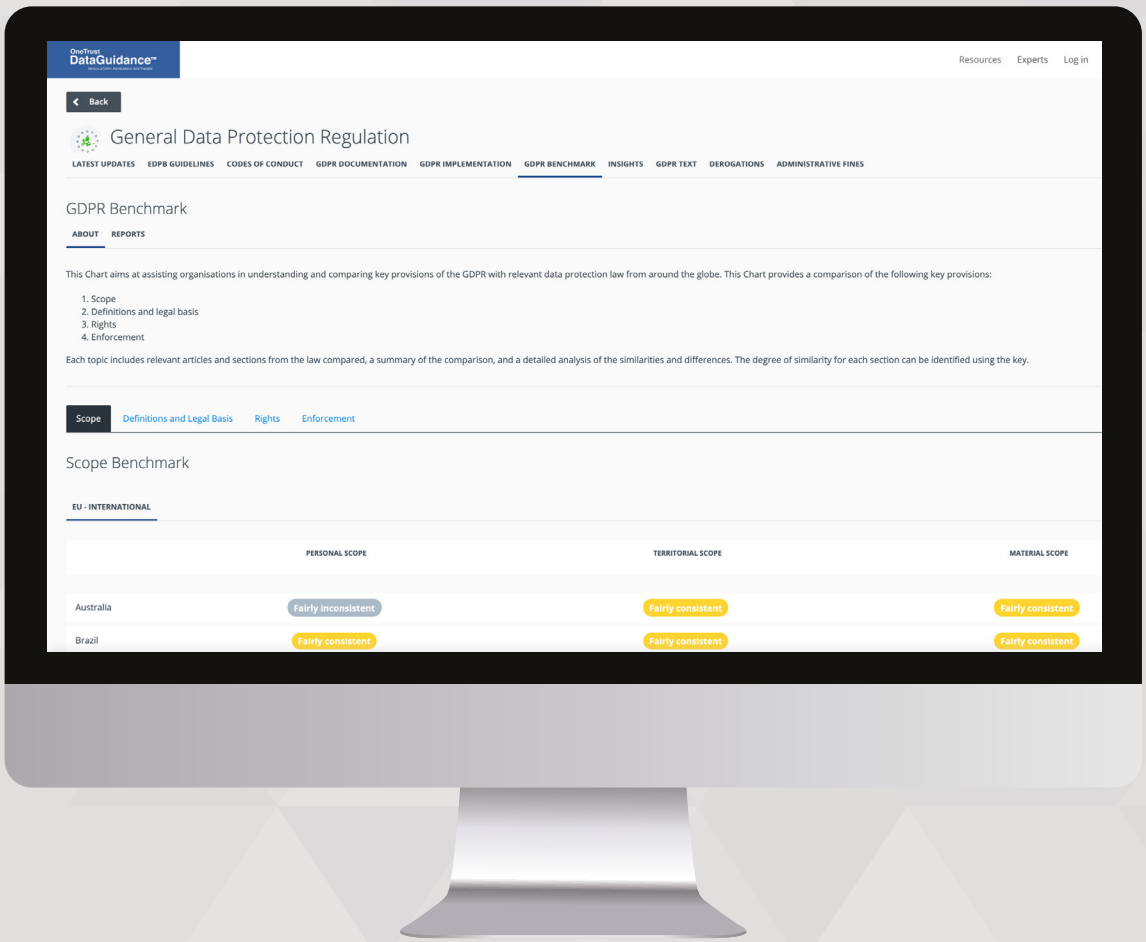
The GDPR establishes that **data processors must record**: a) the name and contact details of the processor; b) the categories of processing conducted on behalf of each controller; c) international transfers of personal data, with the

The LGPD does not detail the information that processors need to record.

Global Regulatory Research Software

40 In-House Legal Researchers, 500 Lawyers Across 300 Jurisdictions

Monitor regulatory developments, mitigate risk, and achieve global compliance



OneTrust

DataGuidance™

REGULATORY RESEARCH SOFTWARE

Build a global privacy program by comparing key legal frameworks against the GDPR

CCPA | Russia | Thailand | Brazil | Japan | China
and 20+ other global laws & frameworks

Understand and compare key provisions of the GDPR with relivant data protection laws from around the globe

The GDPR Benchmarking tool provides comparison of the various pieces of legislation on the following key provisions


Scope


Rights


Definitions and legal basis


Enforcement

- Employ topic specific guidance to develop your compliance activities
- Monitor news and access written opinion pieces on the most recent developments

Start your free trial at

www.dataguidance.com

GDPR	LGPD

Differences (cont'd)

identification of third countries or international organisations, and the documentation of suitable safeguards adopted; and d) a general description of the technical and organisational security measures adopted.	
	The ANPD has developed a regulation for small data processing entities (e.g., small companies and startups) which requires only a simplified data processing record ('ANPD Regulation for Small Processing Entities').

4.3. Data Protection Impact Assessment

Fairly inconsistent

Both the GDPR and the LGPD establish the requirement for a DPIA to be performed in order to assess the risk of data processing activities to the rights and liberties of data subjects in specific circumstances.

The GDPR specifies the cases where a DPIA is required, whilst the LGPD sets fewer criteria than the GDPR as to when a DPIA must be carried out.

GDPR	LGPD
Articles 35-36 Recitals 75, 84, 89-93	Articles 5, 10, 38

Similarities

The GDPR **establishes the requirement for a DPIA** to be conducted in specific circumstances. Member States' supervisory authorities can further determine which processing operations require a DPIA.

The ANPD is empowered to create regulations to specify which processing operations require a DPIA.

Differences

The GDPR states that a DPIA is 'an assessment of the impact of the envisaged processing operations on the protection of personal data.'

The LGPD provides that a DPIA is the documentation from the controller that contains the description of the proceedings of processing of the personal data that could generate risks to civil liberties and fundamental rights, as well as measures, safeguards and mechanisms to mitigate the risk.

The GDPR states that a **DPIA is required**: a) when the processing is likely to result in a high risk to the rights and freedoms of natural persons; b) when a systematic and extensive evaluation of personal aspects relating to natural persons is involved, which is based on automated processing; c) processing on a large scale of special categories of data; and d) a systematic monitoring of a publicly accessible area on a large scale.

The LGPD **does not establish when a DPIA is required**, but the ANPD can request the controller to perform and provide a DPIA.

The GDPR states that a **DPIA must include** at least: (i) a systematic description of the estimated processing operations and the purposes of the processing; (ii) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; and (iii) an assessment of the risks to the rights and freedoms of data subjects.

According to the LGPD, the **DPIA must include** at least: (i) a description of the types of data processed; (ii) the methods used to collect the data; (iii) the methods of information security used; and (iv) the description of the mechanisms used to mitigate the risks related to the processing of the personal data involved.

GDPR	LGPD
Differences (cont'd)	
The measures contemplated for addressing the risks, include safeguards, security measures and mechanisms to ensure the protection of personal data and demonstrate compliance with the GDPR.	The LGPD does not include any explicit provisions on the measures to take to mitigate the risks.
Under the GDPR, the controller shall consult the supervisory authority prior to processing, where a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.	The LGPD does not establish a prior consultation process regarding DPIAs.

4.4. Data protection officer appointment


Fairly inconsistent

The GDPR and the LGPD provide for the appointment of a DPO. Although the tasks they are expected to perform are quite similar in both laws, the nature and scope of their role and responsibilities differ.

GDPR Articles 13-14, 37-39 Recital 97	LGPD Articles 5, 41

Similarities

The GDPR provides for the appointment of a DPO.	The LGPD provides for the appointment of a DPO.
The GDPR defines the tasks of a DPO, which include: (i) **inform and advise** the controller or processor of their obligations under the GDPR; (ii) **monitor compliance** with data protection law and raise awareness/training the staff involved in processing operations; (iii) **provide advice** on DPIAs when requested; and (iv) **act as the point of contact** for data subjects and supervisory authorities.	The LGPD defines the DPO's activities, which include: (i) **accepting complaints and communications** from data subjects, providing explanations and adopting measures; (ii) **receiving communications** from the supervisory authority, advising the entity's employees and contractors regarding data protection practices, and carrying out other duties as determined by the controller; (iii) **orienting the entity's** employees and contractors regarding practices to be taken in relation to personal data protection; and (iv) **carrying out other duties** as determined by the controller or set forth in complementary rules.
The data controller and/or the data processor must publish the contact details of the DPO as part of their privacy notice, and communicate them to the supervisory authority.	The identity and contact information of the DPO should be publicly disclosed, in a clear and objective manner, preferably on the controller's website.

Differences

The GDPR **does not include a definition** of a DPO.	The LGPD **includes a definition** of a DPO, notably a person designated by the controller or processor, that acts as a communication channel between the controller, data subjects and the supervisory authority.
Under the GDPR, **both controllers and processors** are under the obligation to appoint a DPO in specific circumstances.	The LGPD expressly states that **controllers** must appoint a DPO. The LGPD **does not** explicitly establish this obligation for processors, but it is a possibility since the ANPD may create administrative rules demanding them to appoint a DPO. The definition of a DPO also refers to data processors.
Under the GDPR, the obligation to appoint a DPO only applies	The LGPD does **not** limit the DPO appointment to specific

GDPR	LGPD
Differences (cont'd)	
to controllers and processors whose core activities consist either of processing operations which require **regular and systematic monitoring of data subjects on a large scale**, or **processing on a large scale of special categories of data** and personal data relating to criminal convictions.	circumstances; this being left to the ANPD to release complementary rules about the situations in which the appointment of such person may be waived, according to the nature and the size of the entity, or the volume of data processing operations.
A group of undertakings may appoint a DPO provided that the DPO is easily accessible from each establishment.	The LGPD does **not** explicitly mention whether a group of entities may appoint a single DPO.
The GDPR establishes the independence of the DPO.	The LGPD does **not** explicitly establish the independence of the DPO.
The GDPR states that the DPO must be provided with monetary and human resources to fulfil their tasks.	The LGPD does **not** include any provision providing for monetary and human resources to be given to the DPO to fulfil their tasks.
	The ANPD Regulation for Small Processing Entities exempts small data processing entities (e.g., small companies and startups) from appointing a DPO. Nevertheless, the appointment of a DPO is still considered a good practice by the ANPD regarding small data processing entities.

4.5. Data security and data breaches

Fairly consistent

Both the GDPR and the LGPD include an obligation for controllers and processors to adopt security measures to protect the personal data they are processing. The LGPD specifies that the ANPD is empowered to release guidance on which specific security measures are to be adopted.

With regard to data breach notification, both the GDPR and the LGPD include an obligation to notify the supervisory authority as well as data subjects affected in certain circumstances. However, whilst the GDPR includes a set timeline to notify in the LGPD, the timeframe is left to the ANPD to establish.

GDPR	LGPD
Articles 5, 24, 32-34 Recitals 74-77, 83-88	Articles 6, 46

Similarities

The GDPR recognises **integrity and confidentiality as fundamental principles** of data protection by stating that personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate **technical or organisational measures**.

The LGPD recognises **security as a fundamental principle** of data protection by stating that security means the use of **technical and administrative measures** which are able to protect personal data from unauthorised accesses and accidental or unlawful situations of destruction, loss, alteration, communication or dissemination.

The GDPR states that **data controllers and data processors must adopt technical and organisational security measures** that ensure a level of security appropriate to the risk taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

The LGPD states that **controllers and processors must adopt security, technical and administrative measures** able to protect personal data from unauthorised accesses and accidental or unlawful situations of destruction, loss, alteration, communication, or any type of improper or unlawful processing.

Under the GDPR, in case of a data breach, the **data controller must notify the competent supervisory authority** unless the personal data breach is unlikely to result in a risk for the data subject. The data controller must also notify the **data subjects involved**, without undue delay, when the personal data breach is likely to result in a high risk.

Under the LGPD, controllers **must communicate to the ANPD and to the data subject the occurrence of a security incident** that may create risk or relevant damage to the data subjects.

GDPR	LGPD

Similarities (cont'd)

The notification **must include as a minimum**: (i) description of the nature of the breach including, where possible, the categories and the approximate number of the data subject concerned, and the categories and approximate number of personal data records concerned; (ii) contact details of the DPO or other contact point; (iii) the likely consequences of the breach; (iv) measures taken or proposed to be taken to mitigate the possible adverse effects; and (v) the reason of the delay.	**The communication must include as a minimum**: (i) a description of the nature of the affected personal data; (ii) information on the data subjects involved; (iii) an indication of the technical and security measures used to protect the data, subject to commercial and industrial secrecy; (iv) the risks related to the incident; (v) the reasons for delay, in cases in which communication was not immediate; and (vi) the measures that were or will be adopted to reverse or mitigate the effects of the damage.

Differences

The GDPR provides a list of security measures that the controller and processor may implement, which include: (i) the pseudonymisation and encryption of personal data; (ii) measures that ensure the ongoing confidentiality, integrity and availability and resilience of processing systems and services; and (iii) measures that restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.	**The ANPD may provide minimum technical standards** taking into account the nature of the processed information, the specific characteristics of the processing and the current state of technology, especially in the case of sensitive personal data, as well as the principles provided in the lead sentence of Article 6.
The GDPR sets a **timeframe** to notify the competent national authority as '**without undue delay** and, where feasible, not later than **72 hours** after having become aware of it.'	The LGPD states that the communication to the ANPD must be done in a **reasonable time period** to be defined.
The GDPR states that the controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless they are required to do so by Union or Member State law.	The LGPD states that processing agents or any other person that intervenes in one of the processing phases undertake to ensure the security of the information regarding personal data.
The GDPR includes specific provisions with regard to the notification of a personal data breach to data subjects.	The LGPD does not include further details with regard to the communication of a data breach directly aimed at data subjects. The ANPD Regulation for Small Processing Entities provides the following with regard to small data processing entities (e.g., small companies and startups): (i) grants them a prerogative to have a simplified information security policy; and (ii) duplicates the period to notify the ANPD and data subjects about an information security incident.

4.6. Accountability and good practice

Fairly inconsistent

Both the GDPR and the LGPD recognise accountability as a fundamental privacy principle. The LGPD states that controllers and processors may adopt privacy governance programs and good practices to achieve accountability, whilst the GDPR does not refer to such measures.

GDPR	LGPD
Articles 5, 24-25 Recital 39	Articles 6, 50

Similarities

The GDPR recognises **accountability** as a fundamental principle of data protection. Article 5 states that 'the controller shall be responsible and able to demonstrate compliance with data protection laws.'

The LGPD recognises **accountability** as a fundamental principle of data protection. Article 6 states that accountability is the demonstration by the processing agent of the adoption of measures which are efficient and capable of proving the compliance with the rules of personal data protection, including the efficacy of such measures.

Differences

The GDPR clarifies that the data controller must implement measures that ensure and demonstrate compliance. It refers to Data Protection by Design and by Default, the implementation of data protection policies, and the adherence to codes of conduct. **However, it does not specify which activities the data controller shall engage with**.

The LGPD clarifies that controllers and processors may adopt internal processes and policies that ensure broad compliance with rules and good practices, which include a **privacy governance program**, and measures demonstrating its effectiveness. The governance program may: (i) demonstrate the controller's commitment to adopt internal processes and policies that ensure broad compliance with rules and good practices regarding the protection of personal data; (ii) is applicable to the entire set of personal data under their control, irrespective of the means used to collect them; (iii) is adapted to the structure, scale and volume of their operations, as well as to the sensitivity of the processed data; (iv) establishes adequate policies and safeguards based on a process of systematic evaluation of the impacts on and risks to privacy; (v) has the purpose of establishing a relationship of trust with the data subject, by means of transparency, and that ensures mechanisms for the data subject to participate; (vi) is integrated into its general governance structure and establishes and applies internal and external mechanisms of supervision; (vii) has plans for response to incidents and solution; and (viii) is constantly updated based on information obtained from continuous monitoring and periodic evaluations. The ANPD Regulation for Small Processing Entities provides derogations and simplified obligations for small data processing entities (e.g. small companies, startups, etc.), which do not

GDPR	LGPD

Differences (cont'd)

	apply for high risk processing activities. Mainly, these entities are not required to appoint a DPO, they can use a simplified privacy policy and information security policy, and are subject to different deadlines for data subject requests and information security incident notifications. The definition of a small data processing entity refers to a series of criteria with reference to other laws (e.g. theCivil Code), the main ones being the type of legal personality and volume of profit.

5. Individuals' rights

5.1. Right to erasure

Fairly consistent

Both the GDPR and the LGPD allow individuals to request the deletion of their personal information unless exceptions apply.

It should be noted that the scope, applicability and exemptions to the right to erasure vary between the two pieces of legislation. Nevertheless, some exceptions are similar, such as where processing of personal data is done for research, journalistic, artistic or academic purposes, or where it is necessary to comply with a legal obligation.

GDPR	LGPD
Articles 12, 17 Recitals 59, 65-66	Articles 5, 16, 18

Similarities

GDPR	LGPD
The GDPR provides individuals with the **right to request that their data be erased**.	The LGPD provides individuals with the **right to request that their data be deleted**.
The right to erasure applies if **certain grounds** apply, such as where **consent is withdrawn** and there is no other legal ground for processing, or when **personal data is no longer necessary for the purpose for which it was collected**.	Under the LGPD, the right to request deletion applies to **unnecessary or excessive data, or data processed with the consent of the data subject**, except in the situations provided under Article 16.
The scope of this right is not limited to the data controller, but also impacts **third parties**, such as recipients, data processors and sub-processors that may have to comply with erasure requests.	The scope of this right is not limited to the data controller, but also impacts **processors** with whom the data was shared. Controllers must immediately inform the processing agents with whom the personal data was shared of the data subjects' deletion request, so that they can repeat the identical procedure.
This right can be exercised **free of charge**. There may be some instances, however, where a fee may be requested, notably when the requests are unfounded, excessive or have a repetitive nature.	This right can be exercised **free of charge**.
The data subject must be **informed** that they have the right to request for their data to be deleted.	The data subject must be **informed** that they have the right to request for their data to be deleted.
The GDPR includes some **exemptions** to the application of the right to erasure. Among the exceptions to the right of erasure provided by the GDPR include: (i) **freedom of expression** and **freedom of information**, including journalistic,	The LGPD includes some **exemptions** to the application of the right to erasure. Among the exceptions to the right of erasure provided by the LGPD include: (i) where storage of personal data was authorised for a **study by a research entity**; or (ii) to **comply**

GDPR	LGPD

Similarities (cont'd)

academic, artistic and or literary expression; (ii) processing for **research purposes** of personal data that, if erased, would impair the objectives of the research; and for (iii) **complying with a legal obligation**. In addition, the GDPR provides that restrictions may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard: **national security, defence, public security**, the **prevention, investigation and prosecution of criminal offenses** or the execution of criminal penalties.	**with a legal or regulatory obligation** by the controller. In addition, the right of deletion does not apply to the processing of personal data that is done exclusively for journalistic and artistic purposes, or academic purposes. Furthermore, the right to deletion does not apply to the processing of personal data that is done for purposes of **public safety, national defence, state security or investigation and prosecution of criminal offences**.

Differences

Data subjects' requests under this right must be replied to without 'undue delay and in any event within **1 month** from the receipt of the request.' The deadline can be extended to **2 additional months** taking into account the complexity and number of requests. In any case, the data subject must be informed of such extension within one month from the receipt of the request.	Data controllers must respond **immediately** to a data subject request. If this is not possible, the controller must: (i) send a reply to the data subject in which they communicate that they are not the data processing agent and indicate, whenever possible, who the agent is; or (ii) indicate the reasons of fact or of law that prevent the immediate adoption of the measure.
The GDPR specifies that data controllers must have in place **mechanisms** to ensure that the request is made by the data subject whose personal data is to be deleted.	There is no requirement to put in place mechanisms to identify the data subject whose personal data is to be deleted.
Methods to submit a request include **writing, orally and by other means, which include electronic means** when appropriate.	The right to deletion shall be exercised by means of an **express request** by the data subject.
Exceptions: In addition to the exceptions enumerated under 'Similarities,' a data controller is also exempted to comply with erasure requests for reasons of **public interest in the area of public health; establishment, or for the exercise or defence of legal claims**.	**Exceptions**: In addition to the exceptions enumerated under 'Similarities', the right to deletion does not apply where the processing of personal data is done by a natural person exclusively for **private and non-economic purposes**, or where personal data was authorised to be stored for the following purposes: **transfer to third parties**, provided that the requirements for data processing are obeyed; and **exclusive use of the controller** with access by third parties being prohibited and provided the data has been anonymised.

5.2. Right to be informed

Fairly consistent

The GDPR and the LGPD present a high degree of similarity with regard to the transparency principle. Notably, both laws require controllers to provide individuals with a detailed privacy notice providing information on the processing of their personal data.

However, the LGPD does not explicitly address the transparency obligations for indirect collection of personal data.

GDPR	LGPD
Articles 5, 12-14 Recitals 58-63	Articles 6, 9-10, 14, 18-19

Similarities

The GDPR includes '**transparency**' as one of the **key principles** of data processing, by affirming 'personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.'

The LGPD includes **transparency** as one of the **key principles** of data processing, by affirming that transparency is the guarantee to the data subjects of clear, precise and easily accessible information about the carrying out of the processing and the respective processing agents, subject to commercial and industrial secrecy.

The GDPR specifies that data subjects have the right to be provided with information about the processing of their personal data. In particular, they must have access to: (i) the **purposes** of the processing; (ii) the **data retention period**; (iii) the **data controller identity**; (iv) the **recipients** (or their categories) of personal data; and (v) the **data subjects' rights**.

The LGPD specifies that data subjects have the right of access to information concerning the data processing of their personal data. In particular, they must have access to: (i) the **specific purpose** of the processing; (ii) the **duration of the processing**, observing commercial and industrial secrecy; (iii) **the identity of the controller**; (iv) information regarding the **shared use of data** by the controller and the purpose; and (v) the **data subjects' rights**, with explicit mention of the rights provided in Article 18.

The GDPR specifies that the information provided to the data subject must be given in a concise, transparent, intelligible, and easily accessible form.

The LGPD specifies that information provided to the data subject must be given in **a clear, adequate and ostensive manner**.

For **consent** to be valid it must be **informed**.

When the processing activity is based on **consent**, it shall be considered void if the information provided to the data subject contains misleading or abusive content or was not previously presented in a transparent, clear and unambiguous way. Additionally, in cases when consent is required, if there are changes in the purpose of the processing of personal data that are not compatible with the original consent, the controller shall previously inform the data subject of the changes of

GDPR	LGPD
Similarities (cont'd)	
	purpose, and the data subject may revoke their consent if they disagree with the changes.
When the processing is based on **legitimate interest**, the legitimate interest of the data controller and the third party must be specified in the privacy notice.	When the processing activity is based on **legitimate interest**, the controller must adopt measures to ensure transparency of data processing.
Differences	
Further information that needs to be included, as stated in the GDPR, in the privacy notice is: (i) the **categories** of personal data; (ii) **contact details of the DPO**; (iii) the **transfer of data** to third countries; (iv) the **right to withdraw consent** at any time; (v) the right to **lodge a complaint** with a supervisory authority; (vi) when data processing is based on a **contract** the consequences of not providing the personal data; and (vii) **the existence of automated decision making**, including profiling, the **logic** involved and the **consequences**. In case personal data is not collected directly from the data subject, the **source** of the data must be included.	Further information that needs to be included, as stated in the LGPD, in the privacy notice is: (i) the **type** of processing; (ii) the **contact details of the controller**; and (iii) **responsibilities of the agents** that will carry out the processing.
The GDPR explicitly addresses the transparency obligations for **indirect collection** of personal data.	The LGPD does **not** explicitly address the transparency obligations for **indirect collection** of personal data.
When the processing of personal data involves **children's personal data**, 'any information and communication [...] should be in such a clear and plain language that the child can easily understand.'	When the processing of personal data involves **children's and adolescents' personal data**, controllers shall make public the information about the types of data collected, the way it is used and the procedures for exercising the rights referred to under Article 18 of the LGPD.

5.3. Right to object

Fairly consistent

Both the GDPR and LGPD provide data subjects with the right to object and restrict the processing of their personal data, and to withdraw consent of processing.

In addition, the GDPR explicitly provides the right to opt-out in the context of direct marketing.

GDPR Articles 7, 18, 21	LGPD Articles 15, 18

Similarities

Controllers shall no longer process personal data when requested by the data subject and in the circumstances listed in the law, including when withdrawing consent.

Controllers and processors are required to terminate the processing of personal data upon communication by the data subject, including when exercising their rights to revoke consent.

Information about these rights and on how to exercise them must be included in the privacy notice.

Information about this right must be made available to the data subject in a clear, adequate and ostensive manner.

This right must be exercised **free of charge**.

This right must be exercised **free of charge**.

Data subjects' requests under this right must be replied to without 'undue delay and in any event within **1 month** from the receipt of the request.' The deadline can be extended to **2 additional months** taking into account the complexity and number of requests. In any case, the data subject must be informed of such extension within one month from the receipt of the request.

Data controllers must respond **immediately** to a data subject request. If this is not possible, the controller must send a reply to the data subject in which it communicates that it is not the data processing agent and indicate, whenever possible, who the agent is; or indicate the reasons of fact or of law that prevent the immediate adoption of the measure.

Data subjects have the **right to the restriction of processing** in order to (i) contest the accuracy of the data; (ii) when the processing is unlawful; (iii) the controller no longer needs the personal data but the data subject needs it for exercising of legal claims or defence; or (iv) the data subject has previously objected to the processing and the processing needs to be restricted in order to analyse the objection request.

Data subjects have a **right to block the processing** of data which means 'a temporary suspension of the processing' in order to verify if the data is unnecessary, excessive or the processing violates the LGPD. The ANPD can also block any processing activity violating the LGPD until the person responsible rectifies it.

Differences

Data subjects have the **right to object to the processing when personal data** is processed on the basis of legitimate interest, or

Data subjects have **the right to oppose the processing** carried out based on one of the bases other than

GDPR	LGPD
Differences (cont'd)	
public interest. Data subjects can also object to the processing of data by automated means, or when it is processed for historical and statistical purposes. Upon the exercise of such right, the controller is required to stop the processing unless it demonstrates grounds that override the data subject's request.	consent, if there is non-compliance with the LGPD.
The GDPR provides data subjects with the right to object to processing of their data for direct marketing purposes. In particular, in the context of direct marketing, opting-out must be as easy as opting-in.	The LGPD does **not** address objection to direct marketing specifically.

5.4. Right of access


Fairly inconsistent

The right of access is recognised in both the GDPR and the LGPD, in that organisations must provide individuals with access to their personal data when requested.

There are a number of differences between the two pieces of legislation including the time period in which an access request must be responded to, the information which must be included in the response and limitations to the right.

GDPR	LGPD
Articles 12, 15 Recitals 59-64	Articles 6, 18, 19

Similarities

The GDPR **recognises** that data subjects have the **right to access** their personal data being processed by the data controller.

The LGPD **recognises** that data subjects have the **right to access** their data being processed by the data controller.

The GDPR states that, when responding to an access request, a data controller must indicate the **purposes** of the processing; **the recipients** or categories of recipient to whom the personal data have been or will be disclosed; and **any available information as to their source** when the data are not collected from the data subject.

The response to an access request must include a clear statement indicating the **origin of the data**, the existence of any records the **purpose of the processing,** and **information about which agents** the data was shared. When a response is given immediately, the format may be a simplified one.

The GDPR provides that the right of access should not adversely affect the rights or freedoms of others, **including trade secrets**.

In providing information to the data subject, **trade and industrial secrets** must be taken into consideration.

Data subjects must have a variety of means through which they can make their request, including through **electronic means**.

The response may be provided, at the discretion of the data subject, in **printed form**, or by **electronic means**, safe and suitable for this purpose.

The GDPR states that data subjects can exercise this right **free of charge**. There **may be some instances where a fee may be requested**, notably when the requests are unfounded, excessive or have a repetitive character.

Data subjects must be guaranteed easy and **free of charge** access to information on the form and duration of the processing, as well as on the completeness of their personal data.

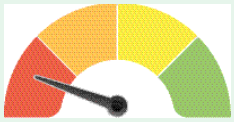
Differences

Data subjects' requests must be complied with without '**undue delay** and in any event within **1 month** from the

Access to personal data must be provided, upon request of the data subject, within a period of **up to 15 days**

GDPR	LGPD
Differences (cont'd)	
receipt of the request.' The deadline can be extended to **an additional 2 months** taking into account the complexity and number of requests. In any case, the data subject must be informed of such extension within one month from the receipt of the request.	of the data subject's request, if the data requested is more than the simplified request version.
The GDPR specifies that data controllers must have in place **mechanisms** to ensure that the request is **made by the data subject** whose personal data is requested access to.	The LGPD does not explicitly request organisations to have in place mechanisms to ensure that the request is made by the data subject. However, the LGPD states that the right of access must be exercised upon **the express request of the data subject or their legal representative**.
Data subjects must have a variety of means through which they can make their request, including **orally**.	The LGPD does **not** explicitly provide for oral requests.
When the access request is made through electronic means, the data controller should submit **the response through the same means**.	There is **no** requirement in the LGPD that electronic requests are responded to in the same means.
The GDPR states that, when responding to an access request, **a data controller must indicate** the **categories of personal data concerned**; the **retention period**; the **right to lodge a complaint with the supervisory authority**; the **existence of automated decision making**; and the **existence of data transfers**.	The LGPD only explicitly requires organisations to provide information on **origin of the data**, the existence of any records and the **purpose of the processing** when a complete declaration is made.
Data controllers can **refuse to act** on a request when it is **manifestly unfounded**, **excessive** or has a **repetitive** character.	The LGPD does **not** include a list of reasons to refuse an access request.
The GDPR states that the right of access should not adversely affect the rights or freedoms of others. As well as trade secrets (under 'Similarities'), this includes **intellectual property** and in particular the **copyright protecting software**.	The LGPD does **not** include a list of rights and freedoms that needs to be balanced against the right to access. In relation to trade secrets, please refer to 'Similarities'.
The GDPR does **not** include any provision on the format the information must be stored in relation to facilitate the data subject's access to their personal data.	The LGPD states that personal data must be **stored in a format** that favours the exercise of the right to access.

5.5. Right not to be subject to discrimination for the exercise of rights


Inconsistent

The LGPD explicitly recognises the principle of non-discrimination as a fundamental data protection principle. Although the GDPR does not recognise this principle explicitly, it can be inferred as part of the principle on the fair processing of personal data, and within the basis of several other provisions within the GDPR.

GDPR	LGPD
Articles 5, 22 Recitals 39, 71-73	Articles 1-2, 6(IX), 20

Similarities

The GDPR protects individuals from automated processing that may result in a decision with legal or significant effects, and that may have discriminatory consequences on the individuals by, among others, limiting the legal basis upon which this processing activity may be carried out and by giving individuals the opportunity to challenge the decision and to ask for human intervention.

The LGPD states that when decisions are taken solely on the basis of automated processing of personal data that affect their interests, the data subject has the right to request a review of the decision and the supervisory authority may carry out an audit to verify discriminatory aspects in automated processing of personal data.

Differences

The GDPR does **not** explicitly recognise non-discrimination as a fundamental principle, although it is the basis for several provisions such as fair processing (Article 5), freely given consent (Article 7) and transparency (Article 13).

The LGPD **explicitly** recognises the principle of non-discrimination as the impossibility of carrying out the processing for unlawful or abusive discriminatory purposes. The right to request a review of decisions taken solely based on automated processing does not explicitly include the right to ask for a human review.

5.6. Right to data portability

Both the GDPR and the LGPD recognise a right to data portability for data subjects. However, the grounds and the scope of the right differ.

GDPR	LGPD
Articles 12, 20 Recital 68	Articles 11, 17-18, 40

Similarities

The GDPR provides individuals with the **right to data portability**.

The LGPD provides individuals with the **right to data portability**.

Anonymous data is not subject to the GDPR, and therefore to the right to data portability.

The portability of personal data does not include data that have already been **anonymised** by the controller.

Differences

The GDPR defines the right to data portability as the **right to receive data processed on the basis of contract or consent and processed by automated means, in a 'structured, commonly used, and machine-readable format'** and to transmit that data to another controller without hindrance.

The LGPD defines the right to data **portability as portability of the data to another service or product provider, by means of an express request** and subject to commercial and industrial secrecy, pursuant to the regulation of the controlling agency.

The GDPR does **not** explicitly limit the scope of the right to data portability to special categories of personal data.

Communication or shared use between controllers of **sensitive personal** data referring to health for the purpose of obtaining an economic advantage is prohibited, except in cases of: (i) a data subject request regarding the portability of their data; (ii) provision of health services, pharmaceutical assistance and health care, e.g. diagnosis and therapy, for the benefit of the data subject; and (iii) to enable the financial and administrative transactions resulting from the services mentioned in item (ii).

⚠ 6. Enforcement

6.1. Monetary penalties

Fairly inconsistent

Both the GDPR and the LGPD provide for the possibility of monetary penalties to be issued in cases of non-compliance.

However, the nature of the penalties, the amount and who is subject to them differs.

GDPR	LGPD
Article 83 Recitals 148-149	Articles 52-54

Similarities

The GDPR provides for the possibility of administrative, monetary penalties to be issued by the supervisory authorities in cases of non-compliance.

The LGPD provides for the possibility of administrative, monetary penalties to be issued by the ANPD in cases of non-compliance.

When **applying an administrative sanction, the supervisory authority must consider**: (i) the nature, gravity and duration of the infringement; (ii) the intentional or negligent character of the infringement; (iii) any action taken to mitigate the damage; (iv) the degree of responsibility of the controller or processor; (v) any relevant previous infringements; (vi) the degree of cooperation with the supervisory authority; (vii) the categories of personal data affected by the infringement; (viii) the manner in which the infringement became known to the supervisory authority; (ix) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures; (x) adherence to approved codes of conduct or approved certification mechanisms; and (xi) any other aggravating or mitigating factor applicable to the circumstances of the case.

When **applying an administrative sanction, the ANPD must consider**: (i) the severity and the nature of the infractions and of the personal rights affected; (ii) the good faith of the offender; (iii) the advantage taken or intended by the offender; (iv) the economic condition of the offender; (v) recidivism; (vi) the level of damage; (vii) the cooperation of the offender; (viii) repeated and demonstrated adoption of internal mechanisms and procedures capable of minimising the damage, for secure and proper data processing, in accordance with the provisions of Article 48(2)(II); (ix) adoption of a good practice and governance policy; (x) the prompt adoption of corrective measures; and (xi) the proportionality between the severity of the breach and the intensity of the sanction.

Supervisory authorities may develop guidelines that establish further criteria to calculate the amount of the monetary penalty.

The ANPD will develop its own regulation on the criteria to apply and calculate any fines, which must be the object of public consultation.

Differences

The GDPR has only one category of administrative fine, which also applies to government bodies.

The LGPD establishes two types of monetary fines: simple and daily fines, both with the same limit of

GDPR	LGPD
Differences (cont'd)	
	BRL 50,000,000 (approx. €9.5 million). A daily fine is normally used to enforce a previous decision.
Depending on the violation occurred the penalty may be up to either: **2% of global annual turnover or €10 million**, whichever is higher; or **4% of global annual turnover or €20 million**, whichever is higher.	The money from any fines applied by the ANPD will be directed to a federal public fund that applies its resources on projects which aim to protect consumer rights, the environment, and assets of artistic, aesthetic, historical, and touristic value. The LGPD's fines do not replace the application of administrative, civil, or criminal sanctions defined in other laws, such as those under the Brazilian Consumer Code.
Under the GDPR, it is left to Member States to create rules on the application of administrative fines to public authorities and bodies.	Depending on the violation, a simple **fine of up to 2%** of a private legal person's, group, or conglomerate revenues in Brazil, for the prior financial year, excluding taxes, up to a total maximum of **BRL 50,000,000** per infraction may be issued. Under the LGPD, government agencies cannot be sanctioned with administrative fines.

6.2. Supervisory Authority

Fairly consistent

Both the GDPR and the LGPD provide for the establishment of a supervisory authority with corrective as well as investigative powers. However, the structures and budgets can vary.

GDPR	LGPD
Articles 51- 59	Articles 55-A - 55-K

Similarities

Under the GDPR, supervisory authorities have **investigatory powers** which include: (i) ordering a controller and processor to provide information required; (ii) conducting data protection audits; (iii) carrying out a review of certifications issued; and (iv) obtaining access to all personal data and to any premises.

Under the LGPD, the ANPD has **investigatory powers** which include requesting information, at any time, from controllers and processors.

Under the GDPR, supervisory authorities have **corrective powers** which include: (i) issuing warnings and reprimands; (ii) imposing a temporary or definitive limitation including a ban on processing; (iii) ordering the rectification or erasure of personal; and (iv) imposing administrative fines.

Under the LGPD, the ANPD has **corrective powers** which include: (i) issuing warnings and fines; (ii) publicising of the infraction; (iii) blocking or deletion of the processing or personal data to which the infraction refers; (iv) imposing a temporary limitation (up to six months, extendable for an equal period) until the processing activity is rectified; and (v) imposing a definitive limitation including a ban on a processing activity.

Under the GDPR, supervisory authorities shall also: (i) handle complaints lodged by data subjects; and (ii) cooperate with data protection authorities from other countries.

Under the LGPD, the ANPD shall also: (i) handle complaints lodged by data subjects; and (ii) cooperate with data protection authorities from other countries.

Under the GDPR, supervisory authorities are tasked with promoting public awareness and understanding of the risks, rules, safeguards and rights in relation to processing as well as promoting the awareness of controllers and processors of their obligations, amongst other tasks.

Under the LGPD, the ANPD is tasked with promoting public awareness on the protection of personal data and on security and undertaking studies on national and international practices for the protection of personal data and privacy, amongst other tasks.

Differences

It is left to each Member State to establish a supervisory authority, and to determine the qualifications required to be a member, and the obligations related to the work, such as duration of term as well as conditions for reappointment.

The ANPD is a federal agency, with technical and decision-making autonomy, its own assets, and national jurisdiction. Since June 2022, the ANPD is no longer subordinated to the Brazilian Presidency.

GDPR	LGPD

Differences (cont'd)

Supervisory authorities may be subject to financial control only if it does not affect its independence. They have separate, public annual budgets, which may be part of the overall national budget.

The ANPD is composed of the Board of Directors, the National Council for Data Protection and Privacy, Internal Affairs Office, its own legal department, and administrative and specialised departments required for applying the LGPD.

The ANPD does not have financial autonomy, and its budget is set forth by the Presidency as the LGPD does not clearly grant a specific budget for its activities. Besides the appropriations established in the federal government budget, the ANPD has other sources of revenue such as sales of publications, technical material, data and information; resources from partnerships or contracts with public or private national or international entities; and revenue from financial investments and real estate renting.

6.3. Civil remedies for individuals

Fairly consistent

In addition to administrative sanctions, any natural person has the right to seek compensation for any material and non-material damage resulting from a violation of the GDPR or the LGPD respectively. Both laws allow for both individual and collective action before the court.

The GDPR specifies how damages are compensated by the controller and the processor. The LGPD does not address this point.

GDPR	LGPD
Articles 82 Recitals 146-147	Articles 22, 42

Similarities

The GDPR provides individuals with a **cause of action** to seek material or non-material damages for violation of privacy laws before the courts.

The LGPD provides individuals with a **cause of action** to seek civil damages (pecuniary or moral) for violation of privacy laws before the courts.

The GDPR allows Member States to provide for the possibility for data subjects to give a mandate for representation to a non-for-profit association, association or organisation that has as its statutory objective the protection of data subject rights.

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, even if the data subject has not agreed to this right of action.

Differences

The GDPR specifies how damages are compensated by the controllers and processors responsible for the damages.

The LGPD does not specify how damages are compensated, allowing for damages based on the Civil Code, that does not set any limit or methodology, relying on case law.

The LGPD explicitly states that the private parties involved in a security incident (e.g. a company and the affected consumers) may settle the case among themselves.

BAPTISTA LUZ ADVOGADOS

BAPTISTA LUZ WAS RANKED A **DATA PROTECTION LEADING FIRM** IN BRAZIL BY ***LEADERS LEAGUE***