

LGPD

GLOSSARY

1 Accountability

It is the demonstration, by the processing agent, of the adoption of effective measures capable of proving the observance and compliance with the rules for the protection of personal data, and even the effectiveness of these measures.

2 Adequacy

It is one of the general principles of the LGPD (art. 6), according to which there must be compatibility between the processing of personal data and the specific purpose informed to the data subject to carry out the processing.

3 Anonymized data

It is personal data that goes through the anonymization process, considering the use of reasonable technical means available at the time of processing, in order to make the data subject non-identifiable.

4 ANPD

It is the acronym for National Data Protection Authority, a public administration body responsible for ensuring, implementing, and supervising compliance with the LGPD throughout the national territory.

5 Anonymization

It is the use of reasonable technical means available at the time of processing in order to eliminate the association that exists between the personal data and the data subject, definitively erasing the characteristics that make it possible to identify the data subjects based on such data.

6 Audit

It is a verification of compliance of the activities carried out by a given Processing Agent with the LGPD. In general terms, during this verification, a review of all internal policies and procedures related to the processing of personal data and the information security practices of the Processing Agent is made, with the aim of verifying any failures and inconsistencies that may result in security incidents.

7 CD/ANPD No. 02

It is the resolution published by the ANPD, on January 27, 2022, which establishes specific rules for small and medium-sized enterprises and startups as processing agents.

8 Compliance

Compliance can be defined as compliance with laws and regulations. When adopted by companies, compliance aims to create practices and procedures to ensure that all legal obligations are met, avoiding losses and forming a good reputational image for the company.



9 Compliance with a legal or regulatory obligation

It is one of the legal bases of the LGPD used for the processing of data, whose purpose is compliance with a legal or regulatory obligation by the controller, such as labor, tax, anti-corruption obligations, among others.

10 Consent

It is defined as the free, informed defined as the free, informed, and unequivocal manifestation by which the data subject agrees with the processing of their personal data for a specific purpose.. It is one of the legal bases provided for in the LGPD.

11 Controller

A natural person or legal entity, governed by public or private law, who is responsible for decisions regarding the processing of personal data.

12 Cookies

These are files created by websites and browsers that are saved on the user's computer. From these files, used information are collected, for example, to identify the user and their preferences within the places visited on the internet, making the user experience personalized.

13 Credit protection

It is one of the legal bases of the LGPD that justifies the processing of data in cases of personal data processing necessary to protect credit. For example, this legal basis authorizes the processing of data inherent to the analysis of credit of a consumer interested in obtaining a loan.

14 Cross-border processing

It is the transfer of personal data that is in the Brazilian territory to a foreign country or international organization.

15 Cybercriminal

The individual who commits crimes in the online and virtual environment.

16 Cybercrime

It refers to illicit practices carried out in the online and virtual environment.

17 Database

It can be understood as a structured set of personal data, established in one or several places, in electronic or physical support.



18 Free access

It is one of the principles of the LGPD and establishes that data subjects can consult, in an easy and free way, the information that is managed in databases controlled by the processing agents, such as the form, duration of processing, and the completeness of their personal data.

19 Data incident

Any unauthorized access, whether accidental or unlawful, that leads to destruction, loss, alteration, leakage, and other inappropriate forms of data processing.

20 Data mapping

It is used to analyze and record the entire data lifecycle from the moment of collection to its disposal, identifying the entire flow of data and its purposes.

21 Data quality

It is one of the principles of the LGPD that guarantees the personal data subjects the right to the quality of their information, i.e., the accuracy, clarity, relevance, and update of the data, according to the need and for the fulfillment of the purpose of their processing.

22 Data sharing

It is the communication, diffusion, international transfer, interconnection of personal data or shared processing of personal databases by public bodies and entities in compliance with their legal competences, or between these and private entities, reciprocally, with specific authorization, for one or more processing modalities allowed by these public entities, or between private entities.

23 DPO

The Data Protection Officer (DPO), existing in the GDPR (General Data Protection Regulation), generally corresponds to Encarregado in the LGPD. The DPO is a specialist in data protection laws and practices, whose role is to monitor and ensure the organization's compliance with the LGPD rules, in addition to acting as a communication channel between the controller/processor, the data subjects, and the supervisory authority.

24 GDPR

It is the acronym for the General Data Protection Regulation, which is the regulation 2016/679 that provides for privacy, protection of personal data, and free movement of such data.

25 Governance

Governance is a set of actions aimed at planning, monitoring, and executing procedures related to privacy and personal data management. For reference, it is the privacy governance program that will define the data management strategy to be followed in a given organization, demonstrating commitment, establishing trust and transparency.



26 Hacker

The individual who has an advanced level of computer knowledge, being able to handle systems, programs or networks, and invade them. A hacker is not necessarily a cybercriminal, as this specific knowledge can not only be used to break into programs, steal or leak information, but also to identify flaws in systems and improve them. This practice by some hackers (white hat) is carried out with the consent of the owner of the system and aims to identify vulnerabilities in order to bring improvements to the system.

27 Independent controllership

It occurs when the processing of personal data is carried out jointly by two controllers, but with different purposes. Independent controllers are controllers that act independently, where each one has autonomy to decide their own purposes for the processing of personal data, without interference from the other party.

28 Interoperability

It is the term used to designate systems and/or organizations that can operate together, ensuring that people, organizations, and computer systems exchange information quickly and efficiently.

29 Joint controllership

It occurs when two or more persons responsible for the data processing (also called joint controllers or co-controllers) jointly or convergently determine the purposes and means for carrying out a certain personal data processing activity/operation.

30 Legal bases

The legal hypotheses, provided for in the LGPD, that authorize a certain personal data processing activity/operation.

31 Legitimate interest

It is one of the most subjective and generic legal bases of the LGPD, which allows the processing of personal data when necessary to meet the legitimate interests of the controller or third parties, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

32 LGPD

It is the acronym for the General Data Protection Law (law No. 13,709/2018), which regulates the processing of personal data in Brazil.

33 Life protection

It is one of the legal bases of the LGPD that justifies the processing of data in case of risk to the life of the data subject.

34 Malware

It is a term that defines any malicious software designed to invade a device or a computer system without the user's knowledge. They are adware, rootkits, spyware, among others.



35 **Material reach**

It concerns the application of the LGPD in different means. This term stems from the first article of the LGPD which establishes that the LGPD will provide for the processing of personal data in physical and digital means.

36 **Necessity**

It is one of the principles of the LGPD that establishes that the processing of personal data must be limited to the minimum necessary for the specific purpose of the processing, avoiding excessive and unnecessary collection.

37 **Non-discrimination**

It is one of the principles of the LGPD that establishes the impossibility of processing personal data for unlawful or abusive discriminatory purposes.

38 **Open banking**

It is an open financial system, which allows customers of financial products and services to share their information between different institutions authorized by the Central Bank and to operate their bank accounts from different platforms.

39 **Personal data**

All information related to an identified or identifiable natural person.

40 **Personal data of children and adolescents**

Personal data of minors under eighteen (18) years of age.

41 **Personal data subject**

The natural person to whom the personal data belong.

42 **Performance of the contract**

It is one of the legal bases of the LGPD and establishes that personal data may be processed for preparatory acts or the performance of a contract to which the data subject is a party.

43 **Performance of studies by a research entity**

It is one of the legal bases of the LGPD that justifies the collection and processing of data by a research entity.



44 Phishing

It is a malicious practice, used to deceive internet users in order to collect confidential information and personal data through electronic fraud.

45 Prevention

It is the adoption of information security measures, by the Processing Agent, to prevent the occurrence of damages due to the processing of personal data.

46 Privacy by default

It is the concept that all services and products, when launched by companies in the market, have privacy settings by default, i.e., only strictly necessary data will be processed by default.

47 Privacy by design

It is an approach developed by Ann Cavoukian for the management of personal data, bringing a set of principles to be adopted throughout the information lifecycle.

48 Privacy policy

The privacy policy, or privacy notice, is the terms that explain how personal data will be used and what processing operations will be carried out, including, but not limited to, the purpose for which they will be processed and the security measures that will be used to protect the personal data and privacy of the data subjects. The purpose of the privacy policy is to provide transparency to the processing of personal data carried out by a certain Processing Agent.

49 Processing

It can be considered as synonymous with Treatment.

50 Processing agent

The one who processes personal data, whether a natural person or legal entity, governed by public or private law. Pursuant to article 5, item IX of the LGPD, the processing agents are the controller and the processor.

51 Processing or treatment

It consists of any and all operation of collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, deletion, evaluation or control of information, modification, communication, transfer, diffusion or extraction, which uses personal data.



52 Processor

A natural person or legal entity, governed by public or private law, who carries out the processing of personal data on behalf of the controller (art. 5, VII, LGPD).

53 Pseudonymization

It is a technique used to process personal data so that data subjects can only be identified through the use of additional information, not available to everyone, and which is typically separated in a controlled and secure environment.

54 Purpose

It is one of the general principles of the LGPD (art. 6) and establishes that personal data may be processed if it has a legitimate, specific, explicit, and informed purpose without the possibility of further processing in a way that is incompatible with the initially informed purpose.

55 Ransomware

It is a type of malware (malicious software) that hijacks data, usually encrypting information and asking for a ransom to decrypt or release the information again.

56 Regular exercise of rights in judicial, administrative, or arbitration proceedings

It is one of the legal bases of the LGPD that allows the processing of data, for example, for the maintenance of evidence and documents to be used by the defense in judicial, administrative, and arbitration proceedings, among other situations.

57 Research entity

An entity of direct or indirect public administration or a non-profit legal entity governed by private law legally organized under Brazilian law, with headquarters and jurisdiction in the country, which includes basic or applied research of a historical, scientific, technological, or statistical nature in its institutional mission or in its corporate or statutory purpose.

58 Retention

It is the continuous filing or storage of data.

59 RIPD

This is the acronym for Data Privacy Impact Assessment. The RIPD typically has a description of the personal data processing processes that may pose risks to data subjects regarding civil liberties and fundamental rights, as well as measures, safeguards, and risk mitigation mechanisms related to the respective processing operation.



60 Security

It is one of the principles of the LGPD establishing that, as a processing agent, it is necessary to adopt technical and administrative measures capable of protecting personal data against security incidents.

61 Sensitive personal data

It consists of a subgroup of personal data that have discriminatory potential and, normally, are part of the data subject's private life. In this regard, the LGPD determines that the following information are sensitive personal data: information about racial or ethnic origin, religious belief, political opinion, affiliation to a union or organization of a religious, philosophical or political nature, data referring to health or sexual life, genetic or biometric data, when linked to a natural person.

62 Small and medium-sized enterprises and startups

CD/ANPD resolution No. 02 defines the small agents as very small and medium-sized business, startups, legal entities governed by private law, including non-profit entities, under the terms of the legislation in force, as well as natural persons and unincorporated private entities that process personal data, assuming typical obligations of Controller or Processor.

63 Social engineering

It is the application of strategies to persuade and manipulate a user to provide personal data or confidential information.

64 Sub-processor

Although not expressly provided for in the LGPD, the figure of the sub-processor can be conceptualized as the one who is hired by the processor to assist in the processing of personal data. The sub-processor is subordinate to another processor, i.e., it has a direct relationship with the processor and not with the controller.

65 Territorial reach

It concerns the geographic territories in which the LGPD applies with regard to activities/operations of personal data processing. For reference, the LGPD applies to personal data processing activities/operations carried out in Brazil; on individuals located in Brazil; conducted by international organizations that offer services and products in Brazil; and/or whose object is personal data collected in Brazil.

65 Transparency

It is the principle of the LGPD that guarantees data subjects access to information on the processing of their personal data and the respective Processing Agents, in a clear, accurate, and easily accessible manner, observing commercial and industrial secrets.



Our recognitions



Análise Advocacia (2021)



Chambers & Partners Brazil (2021 & 2022)



Leaders League (2021 & 2022)



Transactional Track Record (2021 & 2022)



The Legal 500 (2022)

Meet our Partners



Alan Campos Thomaz

Partner

Technology & Digital Business, Privacy and Data Protection, Fintechs and Intellectual Property

at@camposthomaz.com

+55 11 9 8375.2627 +1 (650) 6436652



Sérgio Meirelles

Partner

Corporate, M&A, Venture Capital and Wealth

sergio@camposthomaz.com

+55 11 9 7551.9865



Filipe Starzynski

Partner

Litigation & Law Enforcement, Civil, Real State, Labor and Family

filipe@camposthomaz.com

+55 11 9 7151.9639



Juliana Sene Ikeda

Partner

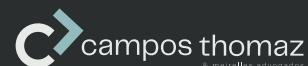
Intellectual Property, Technology, Contracts and Life Sciences

juliana@camposthomaz.com

+55 11 9 8644.1613



Follow us



Subscribe to our newsletter