UNDERSTANDING THE LGPD

BASIC ELEMENTS

Understanding the LGPD: Basic Elements

What is the definition of data and personally identifiable information?

The LGPD is applicable to any activity that involves the processing of "personal data", which is defined *as any information related to an identified or identifiable natural person*. Given the nearly identical language, the concept of personal data is as broad as the one adopted by the European General Data Protection Regulation ("GDPR") – personal data is data that directly identifies an individual or that makes that individual identifiable. Therefore, it applies to names, addresses, phone numbers, identification numbers, location data, IP addresses, and nearly all information that can be linked back, directly or indirectly, to the data subject.

Under the LGPD, "sensitive personal data" is any information about a natural person's race or ethnic origin, religion, political opinion, trade union or religious, philosophical or political organization membership, health, sex life, genetics or biometrics.

The LGPD sets more stringent requirements for processing sensitive data. For example, there is a reduced number of legal bases available for processing sensitive personal data.

The LGPD also defines: (i) *anonymized data* as data that was personal and went through a process that removes any reasonable possibility to identify the data subject, and (ii) *pseudonymized data* as data that can no longer be associated, directly or indirectly, to the data subject, except for the use of additional information that is kept separate by the data controller in a secure and controlled environment.

When data is truly anonymized, the LGPD does not apply. When data is pseudonymized, it is still considered personal data and the LGPD applies normally.

Are there any restrictions on transfer of data and storage of data outside the country?

Yes. Similar to the GDPR, under the LGPD personal data can only be transferred to third countries that ensure an adequate level of protection (a list of such countries will be released in the future by the ANPD) or whenever it is based on appropriate safeguards (*e.g.*, standard contractual clauses, specific contractual clauses, binding corporate rules, codes of conduct and certification mechanisms).

The LGPD is silent in relation to the safeguards' mechanics and requirements. For example, it does not provide any details on the content of binding corporate rules or codes of conduct nor the criteria to be followed by the ANPD when approving safeguards. But it does provide that the ANPD will be in charge of drafting or approving these safeguards.

Until the ANPD becomes operational, it is not possible to rely on a country's adequacy or on safeguards to make cross-border transfers of personal data. Alternatively, cross-border

transfers may be based on derogations for specific situations, such as upon the data subject's specific consent, whenever necessary for the performance of a contract to which the data subject is party, whenever necessary to make or defend a legal claim (present or future), whenever necessary for complying with a legal obligation, among others.

Considering the LGPD is largely inspired by the GDPR, is likely that the countries from the European Union will be considered adequate by the ANPD. Similarly, binding corporate rules already approved by European authorities are likely to be considered valid by the ANPD. However, until the ANPD becomes operational, it is not possible to rely on these mechanisms.

Regardless of international data transfers, the LGPD applies to individuals and private and public legal entities, regardless of the country where they are headquartered or where data is hosted, as long as one of the following conditions is met: (i) data processing takes place in Brazil; (ii) data processing is intended to offer goods or services or process data of individuals located in Brazil; or (iii) data subjects are located in Brazil at the time their personal data is collected.

What are the rights of the data subject?

The LGPD provides the main following rights for data subjects:

(i) to obtain confirmation as to the existence of personal data processing;
(ii) to access their personal data;
(iii) to rectify incomplete, inaccurate or outdated data;
(iv) to have unnecessary, excessive or noncompliant personal data anonymized, blocked or erased;
(v) data portability;
(vi) to have personal data processed under the data subject's consent erased;
(vii) to be informed about third parties with which their data has been shared;
(viii) to be informed about the possibility to refuse providing personal data and the corresponding consequences;
(ix) to withdraw their consent; and
(x) to request a review of automated decisions that affect their interest and were solely based on automated processing of their personal data (the review does not need to be necessarily made by a natural person).

Only data controllers are legally responsible for ensuring that individuals can exercise their personal data rights. However, under the LGPD, data processors can also receive a request from data subjects to guarantee the exercise of their rights.

Are there any restrictions on how a company may use, transfer or share data with its group/affiliate companies or with third parties?

Under the LGPD, the obligations may vary depending on whether a company is a data controller or a data processor. "Controller" is the natural person or legal entity (private or public) that

makes the decisions in relation to the personal data collected; and "processor" is the natural person or legal entity (private or public) that processes data on behalf of, and only on the instructions of, the relevant controller. In some cases, a company can be a controller and a processor.

To determine whether a company is a controller or a processor, it is necessary to consider the company's role and responsibilities in relation to the data processing activities. Whenever a company operating in Brazil exercises control over the processing of personal data due to its local operations, deciding on the means and the purposes of the processing – for example, by directly collecting and using data such as customer information or obtaining such data via third parties, along with other personal data – it is considered a data controller. On the other hand, if a company does not have any purpose of its own for processing data and it only acts on behalf of and on the instructions of a third party, it is a processor, even if it makes some technical decisions (for example, a cloud computing provider).

The LGPD requires a valid legal basis in order to process personal data. Like in the GDPR, "processing" is broadly defined as any operation which is performed on personal data, which includes sharing data within a company's economic group or with third parties.

There are ten available legal bases for processing:

(i) consent of the data subject;
(ii) compliance with a legal or regulatory obligation imposed on the controller;
(iii) enforcement of public policies under laws, regulations or pursuant to contracts, conventions or similar instruments (this legal basis is only available to the public administration);
(iv) studies by a research entity;
(v) performance of a contract or preliminary procedures relating to a contract to which the data subject is party, at the data subject's request;
(vi) regular exercise of rights in the course of judicial, administrative or arbitral proceedings;
(vii) protection of someone's life or physical integrity;
(viii) protection of health via procedures carried out by healthcare professionals or public health entities;
(ix) legitimate interests of the controller or third parties, except when data subject's fundamental freedoms and rights require personal data protection to prevail, and
(x) credit protection.

Controllers are in charge of determining the most appropriate legal basis in accordance to the LGPD. Such assessment depends on what data will be collected from data subjects and for what purposes. Processors, on the other hand, can rely on the legal basis identified by the relevant controller, provided that such legal basis specifically covers the purposes of the processing of which the processor will be in charge.

There are specific requirements for each one of the legal bases mentioned above. For instance, the controller may rely on consent whenever it has obtained a freely given, informed and

unambiguous consent from the data subject (*i.e.*, a positive opt-in). Pre-ticked boxes or other methods of default consent are not allowed. Consent must be expressly confirmed in writing or in any other verifiable means. When in writing, consent requests must be prominent and unbundled from other terms and conditions. Controllers must keep evidence of consent: who consented, when and how.

Meanwhile, whenever relying on legitimate interests as a legal basis for processing, the controller must carry out a legitimate interests assessment ("LIA") before it starts the processing. The LIA's results must be recorded. The controller must also carry out a Data Processing Impact Assessment ("DPIA") regardless of the ANPD's request. The controller must be ready to promptly provide the DPIA upon request to the ANPD.

Moreover, regardless of the legal basis used to justify the processing, the LGPD sets out ten different principles for processing personal data:

(i) Purpose ("*finalidade*"): personal data must be processed for legitimate, specific and explicit purposes informed to the data subject, without any subsequent incompatible processing;

(ii) Adequacy ("*adequação*"): personal data must be processed in a manner consistent with the purposes informed to the data subject, also taking into consideration the context of such processing;

(iii) Necessity ("*necessidade*"): personal data must be processed to the minimum extent necessary for achieving the relevant purposes, using appropriate, proportionate and non-excessive data only;

(iv) Free access ("*livre acesso*"): data subjects must be assured of the right to make easy and free-of-charge inquiries about the means and duration of processing, and the integrality of their personal data;

(v) Data quality ("*qualidade dos dados*"): data subjects must be assured of the right to accurate, clear, relevant and up-to-date data, to the extent necessary and for achieving the relevant purposes;

(vi) Transparency ("*transparência*"): data subjects must be assured of the right to clear, accurate and easily accessible information on processing activities and the respective processing agents, with due regard to trade and industrial secrets;

(vii) Security ("*segurança*"): technical and organizational measures must be adopted to protect personal data from unauthorized access and from accidental or unlawful events of destruction, loss, change, communication or dissemination of such data;

(viii) Prevention ("*prevenção*"): preventive measures must be adopted to avoid damages arising from personal data processing;

(ix) Non-discrimination ("*não discriminação*"): personal data cannot be processed for discriminatory purposes, in an unlawful or abusive manner; and

(x) Accountability ("*responsabilização e prestação de contas*"): processing agents must demonstrate they adopt effective measures to comply with personal data protection requirements.

If controllers or processors, when processing personal data, cause economic or non-economic damages to others, individually or collectively, in violation of the LGPD, they will be liable for redressing such damages.

In addition to civil liability, the ANPD may impose the following penalties, after due process and considering the seriousness of the respective offense:

(i) warning, with indication of a term to adopt corrective measures,
(ii) fine of up to 2% of the gross income in Brazil in its last fiscal year, net of taxes, limited to BRL 50 million per offense;
(iii) daily fine, limited at the amount provided in item (ii),
(iv) once investigated and confirmed, disclosing the offense to the public,
(v) temporary suspension of the ability to use the personal data to which the breach refers;
(vi) deletion of the personal data;
(vii) total suspension of the database;
(viii) partial suspension of the database; and/or
(ix) suspension of business activities.

What is the duration for which a company is allowed to retain data?

Under the LGPD, personal data can only be retained as long as there is a legal basis that allows its processing. This usually means that personal data can be retained as long as (i) a valid business purpose exists, or (ii) there is a need to comply with a regulatory or legal obligation, or (iii) such data may be needed for a company to exercise its rights in existing or future lawsuits, up to the time period set forth by statutes of limitations.

However, the retention of user data applicable to online services is regulated by Articles 15 of the Internet Act (also known as "Marco Civil da Internet").

If a company operates in Brazil and offers online services, it needs to comply with the data retention obligations set forth in the Internet Act. In practice, this means such company must keep Internet applications access records – defined as *"the set of information pertaining to the date and time of use of a certain Internet application from a specific IP address"*, stored for six (6) months, under secrecy, in a controlled and safe environment.

In this scenario, every time a Brazilian user accesses a website or app provided by this company, the respective IP address and the date and time of access must be retained for six

months. There is no mandatory requirement to collect the actual names or addresses of users and, therefore, there is no penalty in case those cannot be disclosed because they were never collected.

The retention period of these Internet applications access records on specific investigations may be extended by a precautionary requirement from a police or administrative authority or the Public Prosecutor's Office.

Under what circumstances is a company required to disclose data?

In general terms, judges may order a company to disclose data on court cases when deemed relevant to an ongoing civil or criminal matter, particularly as evidence.

The disclosure of user data applicable to online services is regulated by Article 22 of the Internet Act, which provides that the disclosure of user data and/or the content of private communications may be requested by the interested party to a judge for the purpose of constituting evidence in a civil or criminal lawsuit. Such request must contain, under penalty of being inadmissible: (i) substantiated evidence of the occurrence of an unlawful act; (ii) a motivated justification of the usefulness of the data/content requested for purposes of investigation or filing of evidence; and (iii) the period to which the data/content pertain.

Whenever a legal obligation of disclosure is imposed on a controller – such as the obligation to disclose personal data to a public body or government entity – then such disclosure is deemed lawful and authorized by Article 7, II, of the LGPD, which provides that personal data can be processed for compliance with a legal or regulatory obligation imposed on the controller. In these scenarios, there is no need to obtain consent from the data subject, given the need for compliance with the legal obligation.

Should a company refuse to comply with a court order determining the disclosure of user data in a lawsuit, then penalties for noncompliance could apply, such as daily fines until the data is disclosed or even the detainment of executives in-country for contempt of court. That has been the case, in the past, for several tech companies that operate in Brazil, in which refusal to comply with local court orders based on jurisdictional matters led to growing daily fines and even the detainment of local executives for alleged contempt of court.

On top of those penalties, a larger fine may also be imposed, limited to 10% of the economic group's revenues in Brazil in its last fiscal year (excluding taxes) and, in cases of recurrent non-compliance, the law establishes that judges may temporarily suspend and block the activities of the company involving collection, storage, retention and handling of data, personal information or communications of users. Certain online services have been temporarily blocked in Brazil in the past for alleged non-compliance with the Internet Act.

About the Author

Marcel holds a Bachelor's, Masters and Doctoral Degree in Law from University of São Paulo and a postdoctoral degree from Berkeley Law. He was the Director of Public Policy at Google from 2011 to 2018, where he collaborated intensively in the drafting of the Internet Act and the General Data Protection Law. He also worked on public policy issues in the most varied subjects in the technology and Internet sectors. Specialized in the protection of personal data and certified by IAPP in EU Privacy (CIPP/E) and US Privacy (CIPP/US). Author of the books "Responsabilidade Civil dos Provedores de Serviços de Internet", "Tutela e Privacidade na Internet" and "Fundamentos de Direito Digital", Marcel has been a professor at FGVLaw since 2005, founding partner of Leonardi Advogados and founder of Leonardi Legal Learning.

Marcel Leonardi

Founder Leonardi Legal Learning
Partner of Leonardi Advogados
CIPP/E, CIPP/US
E-mail: marcel@leonardi.adv.br