FIESP | DEPARTMENT OF DEFENCE AND SECURITY

LGPD

GENERAL DATA PROTECTION LAW

Apoio

GREAT BRITAIN & NORTHERN IRELAND

Realização

FIESP CIESP

With the approval of the Brazilian General Data Protection Law in 2018, the urgency of the matter and the need for the attention of the society as a whole for handling personal data collected on a daily basis becomes more and more evident.

With the intention of supporting companies in the period of adequacy to the new law, the Federation of Industries of the State of São Paulo, FIESP, and the Centre of Industries of the State of São Paulo, CIESP, have prepared this **Personal Data Protection Booklet.**

Since 2015, with the creation of dedicated working groups and through Congresses and Seminars, FIESP and CIESP have been focusing on the topic of Cyber Security and Defence and educating society.

In an objective and simplified way, this Booklet introduces the main information on the new General Data Protection Law so that companies can assess its future operational risks and plan changes and adequacy.

FIESP CIESP

PERSONAL DATA PROTECTION BOOKLET - FIESP

INTRODUCTION

After more than eight years of discussions, based on the General Data Protection Regulation (GDPR) of the European Union, the Brazilian General Data Protection Law (LGPD) was sanctioned on 14 August 2018 (Law 13709/18). **The deadline for compliance is 16 August 2020.**

The LGPD applies to anyone, whether individuals or legal entities governed by public or private law responsible for the online and/or offline processing of personal data. Thus, we can infer that the Law has a broad and comprehensive application, which covers a large part of businesses' projects and activities.

The Law also has extraterritorial application, that is, to companies that (i) carry out the processing of personal data in Brazil; but also (ii) offer services to the Brazilian consumer market; or (iii) collect and process data from persons located in the Country.

With the LGPD Brazil becomes part of a select and important group of countries with a high level of legislation in terms of personal data protection, surpassing the current stage of sectoral processing.

This Law is important for Brazil because of concept harmonisation and updating, which generates greater legal certainty; attraction of investments

from abroad, in view of the level of legal protection we now count on; as well as the cultural promotion of personal data protection.

The LGPD provides for the processing of personal data, including on digital media, by individuals or legal entities governed by public or private law, with the purpose of protecting the fundamental rights of freedom and privacy and the free development of the personality of the individual, establishing rules and limits for companies regarding the collection, storage, processing and sharing of data, which favours economic development.

In general lines, data subjects will have greater control over all processing of their personal data, resulting in a number of obligations for controllers (who are responsible for data processing decisions) and operators (those who process data according to the stipulated by the controllers).

One of the most relevant principles is that of purpose, whereby the data is to be used only for the **specific purposes for which they were collected** and duly informed to the subjects along with the principles of data minimisation, i.e. only the minimum data necessary to achieve the purpose must be collected, and of minimum data retention, which determines **the immediate exclusion of the data after reaching the purpose for which they were collected.**

Thus, the LGPD will bring greater legal certainty to companies and greater protection of the rights of data subjects, and it is crucial to understand the relevant concepts of this new standard to comprehend their impacts in practice.

A) 10 REASONS TO BE CONCERNED WITH THE TOPIC AND THE LAW

1. **Companies of all sectors and all sizes process personal data. The Law applies to all of them;**

2. All business departments usually process personal data: HR; Logistics; Marketing; Data analysis; Software Development and IT; Legal; Compliance, just to name a few;

3. The use of personal data by companies of all sizes is crucial for economic and technological development; innovation; free enterprise; and free competition;

4. The processing of personal data may only be performed if it complies with one of the legal bases provided for in the Law;

5. The Law features relevant principles to guide the processing of personal data, such as purpose (legitimate purposes), adequacy (compatibility), necessity (minimum collection) and transparency;

6. Personal data subjects will now have the following rights: i) confirmation of the existence of the processing of data; (ii) access to data; (iii) rectification of incomplete, inaccurate or out-dated data; (iv) anonymisation; (v) portability; (vi) exclusion; (vii) information regarding data sharing; (viii) possibility of receiving information about not providing consent and its consequences; (ix) revocation of previously given consent;

7. Companies must adopt security, governance and good practice measures;

8. Companies must appoint a Data Protection Officer, who shall be responsible for orienting the institution's employees and contractors regarding practices to be adopted in relation to personal data protection, as well as for guiding and ensuring law compliance;

9. A National Authority for the Protection of Personal Data will be created to monitor compliance with the Law to and apply sanctions in case of violation;

10. Fines in case of violations of the Law can go up to R$50 million.

B) RELEVANT CONCEPTS TO UNDERSTAND THE LGPD

WHAT IS PERSONAL DATA?

Being one of the most relevant assets for the exercise of any business, personal or social activity, as well as for the implementation of public policies, there is no doubt about the importance of the processing of personal data for global economic development.

Personal data (art. 5, I): according to the Law, is any information relating to an identified or identifiable natural person.

Thus, the LGPD presents a broad and open concept, because any data that, either by its own (direct personal data) or aggregated to another (indirect

personal data), can allow the identification of a natural person can be considered as personal data.

Examples: **registration data, date of birth, profession, GPS data, electronic identifiers, nationality, tastes, interests and consumption habits, among others.**

Sensitive personal data (art. 5, II): Sensitive personal data is personal data that relates to (i) racial or ethnic origin; (ii) religious conviction; (iii) political opinion; (iv) affiliation to labour unions or to religious, philosophical or political organisations; (v) data related with health or sexual life; (vi) genetic or biometric data, whenever pertaining to an individual. It is data relating to an identified or identifiable natural person, by means of which a person may be discriminated against and, for this reason, should be considered and treated as sensitive data.

WHAT IS NOT PERSONAL DATA?

Anonymised data or data undergoing an anonymisation process are not personal data (art. 5, III and XI): **anonymised data relating to the data subject that cannot be identified,** considering the use of reasonable and available technical measures existing by the time of the processing. Anonymisation, in its turn, is the use of reasonable and available technical measures existing by the time of the processing, by which data could no longer be directly or indirectly associated with an individual. The use of anonymised data is paramount in order to enable the development and improvement of new technologies, such as the Internet of Things and Artificial Intelligence, but there is an enormous difficulty to prove that reasonable technical means available at the time of processing cannot lead to the identification of the subject.

The Law also does not directly address confidential documents, business secrets, formulas, algorithms, copyrights or industrial property, which are protected by other standards, but only occasional personal data that is contained within such content.

WHAT DOES THE LAW CONSIDER AS DATA PROCESSING?

Just like the broad concept of personal data, the LGPD presents an open concept and an exemplary list of actions that are considered as personal data processing.

Data processing (art. 5, X): any operation carried out with personal data, such as those relating to the collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storing, exclusion, evaluation or control of information, modification, communication, transfer, broadcasting or extraction.

In order to process personal data, which includes the collection and all other practices cited by the legal device, such as reception, classification, filing and transfer, a legal basis is always necessary. At this point, it is important to note that consent becomes one of the 10 (ten) legal hypotheses for data processing, as we will see below.

OTHER RELEVANT CONCEPTS

Subject (art. 5, V): natural person to whom the personal data being processed refer.

Controller (art. 5, VI): natural person or legal entity, governed by public or private law, in charge of making decisions about the processing of personal data.

Processor (art. 5, VII): natural person or legal entity, governed by public or private law, that processes personal data on behalf of the controller.
Processing agents (art. 5, IX): the controller and the processor.

Elimination (art. 5, XIV): exclusion of data or of a group of data stored in a database, regardless of the procedure used.

Data protection impact assessment (art. 5, XVII): documentation of the controller that must contain a description of the personal data processing processes that could generate risks to the civil liberties and to the fundamental rights, as well as measures, safeguards and mechanisms to prevent and mitigate risks.

C) GENERAL PRINCIPLES OF PERSONAL DATA PROTECTION

The LGPD lists 10 principles that must be taken into account in personal data processing:

I - PURPOSE: data processing for legitimate, specific, explicit and informed purposes to the data subject, **without the possibility of subsequent processing inconsistently with those purposes;**

II - ADEQUACY: compatibility of the processing with the purposes informed to the data subject, in accordance with the context of the processing;

III - NECESSITY: limitation of the processing to the minimum processing required for the achievement of its purposes, encompassing pertinent, proportional and non-excessive data in relation to the purposes of the data processing;

IV – FREE ACCESS: guarantee, to data subjects, of facilitated and free consultation on the form and duration of the processing, as well as on all their personal data;

V - DATA QUALITY: guarantee, to data subjects, of accuracy, clarity, relevance and updating of the data;

VI - TRANSPARENCY: guarantee of clear, accurate and easily accessible information to data subjects with regard to the processing activities and the respective processing agents;

VII – SECURITY: use of technical and administrative measures to protect personal data from unauthorised access, incidents or unlawful acts that result in data destruction, loss, alteration, communication or disclosure;

VIII – PREVENTION: adoption of preventive measures against occasional damages resulted from data processing;

IX – NON-DISCRIMINATION: prohibition of data processing for purposes of discrimination, performance of unlawful or abusive acts;

X – LIABILITY AND ACCOUNTABILITY: The agent must adopt effective measures that provide evidence of compliance with data protection, as well as demonstrating the effectiveness of such measures.

D) WHAT ARE THE LEGAL BASES FOR THE PROCESSING OF PERSONAL DATA?

Companies must prove at least one of the following legal bases for processing personal data (art. 7):

I - consent by the data subject: free, informed and unambiguous manifestation by which the data subject agrees to the processing of their personal data for a specific purpose;

II - compliance with legal or regulatory obligation by the controller;

III - by the Public Administration, for the processing of data that is necessary to the implementation of political policies;

IV - for carrying out studies by research agencies;

V - for the performance of a contract or preliminary procedures related to the contract in which the data subject is a party;

VI - as a means of regular exercise of rights in judicial, administrative or arbitral proceedings;

VII - for protection of the life or physical integrity of the data subject or a third party;

VIII - for the protection of health, when the proceeding is carried out by healthcare professionals or sanitary entities;

IX - whenever it is necessary to meet the legitimate interests of the controller or of third parties, considered from concrete situations, unless in case the data subject's fundamental rights that require personal data protection prevail; and

X - for credit protection.

Where data is sensitive, processing may only occur in the following cases (art. 11):

I - consent by the data subject, on a specific and highlighted manner, for specific purposes;

II - without giving the consent of the data subject, in cases where it is indispensable for:

a) - compliance with legal or regulatory obligation by the controller;

b) - shared processing of data required for the enforcement, by the Public Administration, of public policies set forth in the laws or regulations;

c) - for carrying out studies by research agencies;

d) – for the regular exercise of rights, including in contract and in judicial, administrative and arbitral proceedings;

e) - for protection of the life or physical integrity of the data subject or a third party;

f) - for the protection of health, when the proceeding is carried out by healthcare professionals or sanitary entities;

g) - guarantee of fraud prevention and of security of the data subject in processes of registration identification and authentication in electronic systems, unless in the event the data subject's fundamental rights and liberties that require the protection of personal data prevail.

E) PERSONAL DATA SECURITY, GOVERNANCE AND GOOD PRACTICES

The LGPD highlights the security, prevention and adoption of measures for the establishment of good practices and governance in the processing of personal data as pillars, and it is important to note that the National Data Protection Authority may legislate in relation to the minimum technical standards to make security standards and governance applicable, in particular for the processing of sensitive personal data.

Security (art. 46): Processing companies shall adopt technical and administrative security measures to protect personal data from unauthorised access and from accidental or unlawful situations involving destruction, loss, alteration, communication or any other occurrence arising from improper or unlawful data processing.

Good practices and Governance (art. 50): Companies will be able formulate good practice and governance rules that establish organisation conditions, the operational regime, procedures, including claims and petitions from data subjects, safety standards, technical standards, specific obligations for the various parties involved in the processing of data, educational activities, internal mechanisms for the supervision and mitigation of risks and other aspects related to the processing of personal data.

Data Protection Officer: natural person appointed by the controller, who shall be responsible within the company for ensuring compliance with the rules established by the Law and for orienting the institution's employees and contractors regarding practices to be carried out in relation to personal data protection. Thus, among the roles of the Data Protection Officer, we highlight: (i) receiving and meeting the demands data subject demands; (ii) interacting with the National Data Protection Authority and (iii) advising employees and contractors on data protection practices. The Data Protection Officer reports directly to the highest management level, must perform their duties with autonomy and stability, budgetary independence and is mandatory for companies that process personal data as controllers.

F) PRIVACY BY DESIGN AND PRIVACY BY DEFAULT

Privacy by design represents the use of privacy mechanisms/solutions throughout the data lifecycle. By this concept, **privacy is incorporated into the architecture of the systems and processes** developed, in order to ensure, through the infrastructure of the service provided, conditions for users to be able to preserve and manage their privacy and the collection and processing of their personal data.

In its turn, *Privacy by default* represents the obligation for all these tools to be active by default. That is, setting as **default configuration the greatest possible privacy to the data subject.**

The processing agents must, therefore, from the product or service design up to their implementation, adopt technical, security and administrative measures capable of protecting personal data from unauthorised access and from accidental or unlawful situations of destruction, loss, modification, communication or any form of inappropriate or unlawful processing of data (art. 46, §2).

G) WHO IS TO ENFORCE COMPLIANCE WITH THE LAW?

National Authority (art. 5, XIX and art. 55-A): a public administration agency responsible for overseeing, implementing and ensuring compliance with the Law. An essential part of the normative framework in question, with the responsibility of promoting studies and data protection culture, cooperation with other national and international authorities, editing regulations, supervision, sanctioning, among others. The international experience reinforces the need to create such a regulatory agency, with **characteristics of independence, technical expertise** and effective enforcement powers.

H) WHICH ARE THE SANCTIONS PROVIDED FOR IN THE LAW?

The LGPD implements the application of severe sanctions for companies that fail to comply with the legal provisions and, for that reason, companies compliance to the provisions of the Law is relevant. In addition, it should be noted that the National Data Protection Authority, among other elements, must observe, in the event of applying a sanction, not only the level of the data provided, but also the internal measures, mechanisms and procedures previously adopted by the company, which demonstrates the clear need for adequacy and implementation of good governance, security and prevention practices.

Administrative sanctions (art. 52): data processing agents, due to violations of the norms provided for by the Law, shall be subject to the following applicable administrative sanctions by the National Authority:

(I) a warning, indicating the deadline for the adoption of corrective measures;

(II) a flat fine, up to two percent (2%) of the sales revenue from legal entities governed by private law, groups or conglomerates in Brazil in their latest fiscal year, excluding taxes, capped at fifty million Brazilian reais (R$50,000,000.00) per infraction;

(III) a daily fine, subject to the cap referred to in item II;

(IV) disclosure of the infraction after the occurrence has been being duly verified and confirmed;

(V) blockage of the personal data to which the violation relates until it has been regularised;

(VI) exclusion of personal data to which the violation relates.

Liability and compensation for damages (section III):

1. The controller or operator that, while performing the processing of personal data, causes property, moral, individual or collective damage to another in violation of the legislation on the protection of personal data, is obliged to compensate it.

2. The operator is jointly and severally liable for damage caused by the processing of data when it fails to comply with the obligations of the data protection legislation or when it has not followed the lawful instructions of the controller;

3. Controllers that are directly involved in the processing from which the data subject has suffered damages are jointly liable.

4. The party that compensates the damage to the data subject has recovery rights against the other responsible parties, to the extent of their participation in the damage.

5. Processing agents will not be liable only when they prove: that they have not processed the referred personal data; that there was no violation of the data protection legislation; or that the damage is the sole fault of the data subject or of a third party.

6. The processing of personal data will be irregular when it fails to comply with the legislation or when it fails to provide the security that the data subject should expect, considering the relevant circumstances, including: the way in which it is performed; the result and the risks that are reasonably expected from it; the techniques of personal data processing available at the time it was performed.

I) HOW TO COMPLY WITH THE LAW?

The LGPD shall enter into force on 16/08/2020. The estimate for full company compliance may vary from 4 (four) to 14 (fourteen) months, according to, among others, the following criteria: the level of maturity of the company on the topic; the existing rules and procedures; the number of areas and projects that process personal data; the level of sensitivity of the data subject to the processing; the budget estimated for adequacy.

Thus, aiming at complying with the legislation in question, we suggest some basic actions, such as:

(I) Seeking to get executives involved from the very beginning of the adequacy plan so that the protection of personal data is incorporated into the values of the company so the topic can get the necessary engagement and strength;

(II) Establishing actions and a leader for the plan, identifying the main projects and areas of the company affected by the LGPD and occasional sectoral legislations;

(III) Establishing a data protection governance programme with the development of measures and controls to monitor the implementation of standards that are in compliance with the LGPD and applicable sectoral legislation;

(IV) Structuring the area with the appointment of the Data Protection Officer (DPO);

(V) Preparing and reviewing legal documents carrying out occasional additions to the existing contracts to comply with data protection standards, mainly for those that involve the processing and sharing of personal data;

(VI) Ensuring the exercise of the rights of the subjects, through the confirmation of the implementation of technical and organisational measures;

(VII) Conducting internal training in order to introduce the new personal data protection policies and disseminate corporate culture on the subject.

TECHNICAL SHEET

CREATED BY

Rony Vainzof
Director of the Department of Defence and Security of FIESP
and Coordinator of the Working Group on Cyber Security and Defence

Luciana Nunes Freire
General Counsel and Head of Legal of FIESP

Caio Oliveira
Contributor to the Working Group on Cyber Security and Defence

COORDINATION

Luciano Villela Coelho
Manager of the Department of Defence and Security of FIESP
and member of the Working Group on Cyber Security and Defence

Av. Paulista, 1313
São Paulo - SP | CEP: 01311-923
deseg@fiesp.com.br
www.fiesp.com.br