GUIDE
LGPD

PHARMACEUTICAL INDUSTRY

SINDUSFARMA

INTERFARMA
Associação da Indústria Farmacêutica de Pesquisa

GUIDE LGPD

(Brazilian General Data Protection Act)

PHARMACEUTICAL INDUSTRY

GUIDE LGPD

(Brazilian General Data Protection Act)

PHARMACEUTICAL INDUSTRY

SINDUSFARMA

September
2020

INTERFARMA
Associação da Indústria Farmacêutica de Pesquisa

TABLE OF CONTENTS

INTRODUCTION

This LGPD Guide is intended for companies in the pharmaceutical sector associated with SINDUSFARMA – Pharmaceutical Products Industry Union and INTERFARMA – Association of the Pharmaceutical Research Industry. The document has been prepared from the original consultancy work carried out by law firm Chenut Oliveira Santiago Sociedade de Advogados under coordination from Dr. Fernando Santiago, subsequently modified and adapted by employees from a group of associates.

Law 13.709/18 and subsequent amendments has inaugurated a new scenario in the Brazilian legal system with regard to the protection of all Brazilians' personal information. In spite of the existence of laws and regulations that, to greater or lesser extents, already offered legal protection to personal information, it is undeniable that the new law established a new regulatory legal model for the country.

As expected, the text now presented is not binding. It is a construction aimed at guiding those who shall have to subject themselves to the new reality, on the one hand, and bring certain aspects of the sector to the attention of society in this area, on the other. Its objective is simply to guide the Associates as to the existing rules in the LGPD with emphasis on corporate areas inherent to the economic sector, including pharmacovigilance, clinical research, relationships with patients and health professionals.

In view of this purpose, the Guide brings to the Associates an instrumental view of the LGPD, with specific recommendations for the adequacy of the Pharmaceutical Industry in relation to that reference.

Thus, SINDUSFARMA and INTERFARMA hope that the Guide shall contribute to the adequateness of its associates and to the debate on understanding the application of the LGPD to the pharmaceutical sector in Brazil.

DEFINITIONS

i. **Personal data:** information related to an identified or identifiable natural person.

ii. **Sensitive personal data:** personal data about racial or ethnic origins, religious beliefs, political opinions, membership in a union or organization of religious, philosophical or political natures, data relating to health or sexual life, genetic or biometric data, when linked to a natural person.

iii. **Anonymized data:** data related to the Holder that cannot be identified, considering the use of reasonable and available technical means at the time of their handling.

iv. **Database:** structured set of personal data, established in one or several locations, in electronic or physical framing.

v. **Holder:** natural person to whom the personal data that are being handled refer to.

vi. **Controller:** natural or legal persons, under public or private laws, that are responsible for decisions regarding the handling of personal data.

vii. **Operator:** natural or legal persons, under public or private laws, that handle personal data on behalf of the Controller.

viii. **Person in Charge**: person appointed by the Controller and Operator to act as a communication agent among the Controller, data Holders and the National Data Protection Authority (ANPD).

ix. **Handling agents**: the Controller and the Operator.

x. **Handling**: any operation performed with personal data such as those referring to the collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, elimination, evaluation or control of information, modification, communication, transfer, disclosure or extraction.

xi. **Anonymization**: use of reasonable and available technical means at the time of handling, whereby data lose the possibility of association, directly or indirectly, with an individual.

xii. **Consent**: free, informed and unambiguous statement by which Holders agree with the handling of their personal data for a specific purpose.

xiii. **Blocking**: temporary suspension of any handling operation by keeping personal data or the database.

xiv. **Elimination**: deletion of data or data set stored in a database, regardless of the procedure employed.

xv. **International data transfer**: transfer of personal data to a foreign country or international body of which the country is a member.

xvi. **Shared use of data**: communication, broadcast, international transfer, interconnection of personal data or shared handling of personal databases by public bodies and entities in the fulfillment of their legal powers or between these and private entities, reciprocally, with specific authorization, for one or more handling modalities allowed by these public entities or among private entities;

xvii. Report on the impact of the personal data protection: the Controller's documentation that contains the description of the processes for handling personal data that may generate risks to civil liberties and fundamental rights as well as measures, safeguards and risk mitigation mechanisms;

xviii. National authority: Brazilian public administration body responsible for overseeing, implementing and supervising compliance with this Law throughout the Brazilian territory.

xix. Legitimate Interest Tests: tests to be carried out in certain circumstances when the legal basis of the handling is "legitimate interest of the Controller or third parties" with the objective of assessing the impacts on the Holders' rights and freedom as well as their reasonable expectations regarding the handling of their personal data.

1 WHAT IS THE BRAZILIAN GENERAL DATA PROTECTION ACT?

The Brazilian General Data Protection Act (LGPD), Federal Law No. 13.709 of August 14, 2018, has the purpose of disciplining the handling of personal data, including in digital media, by a natural person or a legal person under public or private laws, with the objective of protecting the fundamental rights of freedom and privacy and the free development of natural person's personality.

The explanatory memorandum to the Bill (PL) that originated the LGPD – PL No. 4.012/2012- expresses the concern with the way in which personal data has been handled in Brazil, especially in view of recent years' technological advances.

It was based on these premises that the Congress and the President of the Republic approved the LGPD, which seeks, first of all, to ensure persons' dignity by means of their intimacy and privacy protection.

2
LGPD'S PRINCIPLES

The basic principles of Personal Data Holders are those that should be observed by everyone:

i. **Good faith:** it is commonly interpreted as the attitude expected from average individuals based on the social values and ethical conduct expected from a society.

ii. **Purpose:** to carry out the handling for legitimate, specific, explicit and informed purposes to the Holder without the possibility of further handling in a manner incompatible with these purposes.

iii. **Adequateness:** compatibility of the handling with the purposes informed to the Holder, according to the handling context.

iv. **Necessity:** limitation of the handling to the minimum necessary for its purposes accomplishment, with coverage of the relevant data, proportional and not excessive in relation to the data handling purposes.

v. **Free access:** guaranteeing to Holders free and easy consultation on the form and duration of handling as well as on their personal data integrality.

vi. **Data quality:** guaranteeing the data Holders the accuracy, clarity, relevance and updating of the data according to the needs and for the fulfillment of their handling purposes.

vii. **Transparency:** guaranteeing Holders clear, accurate and easily accessible information about the handling and the respective handling agents, observing commercial and industrial secrets.

viii. **Security:** use of technical and administrative measures to protect personal data from unauthorized access and accidental or unlawful situations of destruction, loss, alteration, communication or broadcast.

ix. **Prevention:** adoption of measures to prevent the occurrence of damages due to the personal data handling.

x. **Nondiscrimination:** impossibility of carrying out the handling for illicit or abusive discriminatory purposes.

xi. **Responsibleness and accountability:** demonstration, by the agent, of the adoption of effective measures capable of proving observance and compliance with the rules of protection of personal data and even of the effectiveness of these measures.

3
STRUCTURING ACTIONS TO ASSIST THE LGPD

3.1. Appointment of a Person in Charge for handling personal data (Data Protection Officer – DPO)

The LGPD imposes on the Controller the obligation to appoint a Person in Charge of handling personal data (ETD), better known by the term "Data Protection Officer (DPO)" (article 41).

Initially, the LGPD text associated the Person in Charge only with the Controller. However, the LGPD current wording allows the appointment of this important professional by the "Operator" (article 5, VIII).

The appointment of a Person in Charge has the objective of attributing to a certain individual or legal entity the responsibility for the initiative, centralization and coordination of all the actions necessary for the implementation of a complex project to adapt to the LGPD.

The criteria for appointment and dismissal of the Person in Charge shall be subject to regulation by the future National Data Protection Authority (ANPD), considering the nature and size of the entity or the volume of data handling operations.

Under the LGPD terms, the Person in Charge has the following duties:

- **3.1.1.** Accepting complaints and communications from Holders, providing clarifications and taking action;
- **3.1.2.** Receiving communications from the National Authority and taking action;
- **3.1.3.** Guiding the entity's employees and contractors about the practices to be taken in relation to the protection of personal data and
- **3.1.4.** Performing the other attributions determined by the Controller or established in complementary norms

3.2. Development of a Personal Data Handling Record

Development and maintenance of a handling record are structural elements of the greatest importance and their conservation is mandatory for the purposes of internal control, audit and inspection (article 37).

Record of handling provides companies with knowledge about how they handle personal data in their multiple activities, generating knowledge and a global view of the company's activities and departments.

By offering a global view of the company, the record represents an extremely useful tool, being the starting point for any action or investigation related to personal data, especially in cases of incidents.

Thus, each activity or action involving personal data within the company must be represented by a handling record. Considering the procedure novelty, it is suggested that its initial preparation be entrusted to those responsible for carrying out these activities with the assistance of the Person in Charge or specialized professionals. After structuring the first version and increasing the knowledge and understanding of those involved about the document, its constant updating can be regularly done by the performers of the activity portrayed in the record, with no mandatory model for its realization.

For the record, reference is made to the minimum information:

- 3.2.1. Record object activity;
- 3.2.2. Objectives pursued – describing the handling purpose;
- 3.2.3. Categories of people involved – Holders of personal data;
- 3.2.4. Categories of data collected – the types of data involved in the activity;
- 3.2.5. Retention periods for each data category;
- 3.2.6. Data recipient categories;
- 3.2.7. Data transfers abroad;
- 3.2.8. Security measures;
- 3.2.9. Legitimate Interest Tests (TLI/LIA (Legitimate Interests Assessment));
- 3.2.10. Data Privacy Impact Report (RIPD/DPIA (Guidelines on Data Protection Impact Assessment)).

3.3. Development of Policies Related to the Handling of Personal Data

An important element for the company's internal structuring in compliance with the rules provided for in the LGPD is the creation of policies and procedures that must be observed by everyone in the company and by those who relate to it and that interact with personal data.

Among the policies and procedures we highlight **(i)** Privacy Policy, **(ii)** Personal Data Protection Policy, **(iii)** Personal Data Retention Policy, **(iv)** Personal Data Access and Circulation Policy and **(v)** Personal Data Sharing Policy. Such Policies may provide for the following topics.

3.3.1. Privacy Policy

i. Introduction;

ii. Specific purposes of the handling;

iii. Form and duration of the handling;

iv. Controller's identification;

v. Controller's contact information;

vi. Information about the shared use of data by the Controller and the purpose;

vii. Responsibilities of the agents who shall carry out the handling;

viii. Holder's rights.

3.3.2. Personal Data Protection Policy

i. The basic principles to be observed for the handling of personal data by the company;

ii. The way of handling sensitive data;

iii. The processing of personal data by Operators (possibly with a link to the clauses to be inserted in Contracts with third parties);

iv. How transfers of personal data to third countries are handled;

v. The personal data Holders' rights;

vi. The procedures for handling data Holders' complaints;

vii. Observation of privacy rules from the design stage of the company's products and processes (privacy by design);

viii. The occasions when an impact analysis on the protection of personal and other data must be carried out.

3.3.3. Personal Data Retention Period Policy

The storage time may be legal or conventional, depending on the nature of the data. The legal term must follow the retention time provided for by laws and regulations, when applicable, and the conventional term must be stipulated by each company depending on the nature of the handling.

As an example, a document unrelated to FGTS (Federal Severance Pay Fund) or INSS (National Institute of Social Security) dealing with an employee's employment Contract (e.g., medical certificate, authorization for discounts not provided for by law, etc.) can be filed for up to five (5) years during the employment situation and up to two (2) years after the termination of the employment Contract. Such term is determined by law (Brazilian Federal Constitution, Article 7, XXIX and CLT (Brazilian Consolidation of Labor Laws), article 11).

On the other hand, there is a variety of handling situations of personal data, the filing deadline of which is not determined by law such as, for example, the retention time of personal data of a commercial prospectus. For such data – and in the absence of an indication by the regulatory authority – the company must stipulate a retention period that is consistent with market practices and the nature of the handling, justifying the reason for the adopted period.

3.3.4. Internal Access Control Policy

An access control policy must be carried out by each company, regarding the size, sector of activity and structure, limiting access to the company's database. It is therefore a question of determining which areas – or even which jobs within each area – really need full or partial access to the company's personal database and to structure the implementation of this access compartmentalization with the responsible sector by information technology.

In this sense, the company's Internal Access Control Policy determines the access profile of each area to the company's database

– possibly with different access profiles within each area, if applicable, the procedure to be adopted in case of need to access blocked personal data and the person responsible for examining that request.

For example – except if the circumstances of the specific case justify it – the personnel department of a company would not, in principle, need access to the database used for commercial prospecting.

3.4. Adequacy of Contracts

It is believed that every company, at some point, shares personal data. Thus, it is necessary that the Contracts by which the Controller relates to a third person establish the qualification of the parties (Controller and Operator) in terms of the LGPD, specific confidentiality about personal data and the allocation of responsibilities.

It is worth remembering that the LGPD holds all handling agents (Controllers and Operators) responsible for the security and guarantee of the integrity of the personal data they handle (article 46) and the Operator can be considered jointly and severally liable with the Controller if they fail to comply with the LGPD or fail to follow the lawful instructions instituted by the latter (article 47). The relationship between the handling agents, therefore, must be defined in an appropriate contractual instrument.

3.5. Structuring of the International Flow of Personal Data

In the event that the company transfers personal data abroad, it must follow the requirements provided for in article 33 of the LGPD.

It is worth remembering that international data transfer is a more common practice than imagined. In effect, companies often contract the storage of their database or e-mails on servers (cloud computing) located abroad.

The subject still needs regulation by the National Data Protection Authority, to be created by the Brazilian Federal Government. However, as an example, international data transfer may occur:

i. with the consent for such act granted by the Holder of the transferred personal data (highlighted and with prior information of the international nature of the operation).

ii. by drafting a specific contractual clause with the recipient of the data abroad including the guarantees of compliance with the principles, the Holder's rights and the data protection regime provided for in the LGPD (such clause must be adequate to the positions to be issued later by the ANPD);

iii. in compliance with legal or regulatory obligations by the Controller.

3.6. Mechanisms to Ensure the Exercise of Rights by Holders of Personal Data

The LGPD has brought a series of new rights and guarantees (mainly articles 17 and 18) to the personal data Holders. As an example, personal data Holders may request confirmation of the existence of handling, correction of inaccurate data or their deletion as well as

information about public or private entities with which the Controller may have shared personal data from those.

3.7. Employees' Awareness Training

The principle of necessity is one of the LGPD's basic principles. It essentially concerns the quality of personal data handled by the Controller. The latter, by means of their employees, must stick to collection and handling of data strictly necessary for the purpose for which it was collected.

Observance of this principle implies a drastic reduction in the quantity and type of data (quality) collected and all those that are not essential for the achievement of the intended purpose should be eliminated.

In this sense, the organization of training for employees is an essential element for achieving the objectives advocated by the LGPD. The frequency of this training shall depend on the size, profile, volume of personal data handled and periodicity of renewal of the employees of each company. Respect for the standard is more easily achieved when it is understood by those responsible for its application.

4
IMPLICATIONS OF THE LGPD ON THE MAIN AREAS OF THE PHARMACEUTICAL INDUSTRIAL SECTOR

4.1. Human Resources Sector

Due to the amount and diversity of personal data that the Human Resources (HR) sector handles, it stands out as one of the most affected by the LGPD.

The company's HR sector handles not only the company's employees' personal data but also those of their dependents and those of job seekers. Such data are often sensitive in nature (medical certificates) or refer to minors (dependents), which reinforces the need for their inclusion and protection.

Thus, below are the main points that are submitted to the HR but which may vary due to the follow-up, size, origin and other factors inherent to the company.

4.1.1. Extensive Information to Holders of Personal Data

Employees and Contractors managed by the HR sector must receive an information note on the handling of their personal data. A simple and effective means of achieving this objective consists, for example, of fixing this document in strategic places in the workplace or even disseminating it through internal company networks. Gradually this news item of information must be incorporated into new employment or outsourcing Contracts by means of the inclusion of a specific clause on the topic.

Regarding apprentices, information about the handling must be provided in a simple, clear and accessible way, considering their physical, perceptual, sensory, intellectual and mental characteristics, using audiovisual resources when appropriate.

In the same sense, the means of collecting personal data from job seekers must include information on the handling of personal data, identifying the purpose, consent for possible sharing, if applicable, as well as the retention period and the rights conferred to the Holder by the LGPD.

If there are surveillance cameras and geolocation of a certain category of employees, it is important that such handling be included in the information news that is intended for them. Possibly this topic shall be subject to regulation by the ANPD.

4.1.2. Physical File Security

Physical HR files deserve special attention. They must be kept under surveillance and with restricted access (including, if applicable, within the team) until their proper disposal. If these files storage location is outsourced, it is suggested that the outsourcing Contracts provide for specific security and access control mechanisms.

4.1.3. Sensitive Personal Data

The sensitive personal data of employees or their dependents collected and handled by the Controller must also be handled with care. Most of the time such data are obtained at the time of hiring and are under the custody of the HR sector.

4.1.4. Minors' Data

Collection of personal data from employees' dependents is common for the purpose of assigning various benefits (health plans, family allowance and others). The LGPD requires that handling be performed in the best interests of children and adolescents. Restricted conditions for the handling of children's data, thus considering those under 12 years of age incomplete under the terms of the current legislation. In such cases, a good practice consists of obtaining specific and highlighted consent by at least one of the parents or legal guardian for this handling, emphasizing that such consent can be obtained through a highlighted clause that is part of the employment Contract of the child's legal guardian.

It is important to note that there may be situations that justify the handling of children's data, regardless of obtaining parental consent (for example, to comply with legal or regulatory obligations).

In relation to the handling of "apprentices'" personal data, who may eventually be legally qualified as adolescents by law, it may be based on the execution of the apprenticeship Contract, always observing details of specific cases.

5 ADMINISTRATIVE-FINANCIAL SECTOR

As a rule, the Administrative-Financial sector is responsible for activities related to Controllership, treasury and management of accounts payable and receivable. Although the attributions of this sector considerably vary among companies, in most cases the personal data handled by it refer to employees, representatives of their customers or suppliers.

Often the Administrative-Financial department shares personal data with other companies, notably financial institutions and/or credit and collection analysis companies.

The diversity of the purposes for which personal data are handled by the Administrative-Financial sector shall give rise, depending on the case, to different hypotheses of legal basis. As an illustration, there are a Contract execution (remuneration) and compliance with legal obligations (Brazilian Social Security), among other possibilities.

6
PHARMACOVIGILANCE SECTOR AND SAC (CUSTOMER SERVICE DEPARTMENT)

The Pharmacovigilance, Quality and SAC sectors often combine two similar activities in terms of form but different in terms of content and above all in relation to the desired purpose. These are the activities of pharmacovigilance or cosmetic products vigilance (depending on the company's activity) and the Customer Service Department (SAC).

The pharmacovigilance sector collects sensitive personal data and, very often, performs international data transfer. The Customer Service Department (SAC) is essentially aimed at answering questions and complaints from customers but also serves as a platform for reporting adverse effects, a typical pharmacovigilance activity.

Thus, it appears that the correct identification of the object of contact with the company, in the shortest possible time, is of paramount importance for the Quality sector. The early identification of the nature of the call allows to correctly structure the form and, above all, the legal basis for the handling of personal data carried out.

6.1. Consent

Regarding the principles imposed by the law, the handling of personal data – including sensitive ones – resulting from the activities of pharmacovigilance and cosmetic products vigilance does not require consent from the data Holder since they are based on the fulfillment of legal or regulatory obligations.

Handling of consumers' personal data related to the SAC, excluding reports of adverse effects containing data related to health, may be justified by legitimate interests. Since the right to the personal data protection is extremely specific, eventual need for consent cannot be excluded, depending on specific cases and the type of patient (children and others).

6.2. Period for Retention of Personal Data

Personal data handled by the pharmacovigilance system must be stored for the period established in the legislation applicable to the subject, especially the regulations issued by the National Health Surveillance Agency (Anvisa).

In relation to personal data collected through the SAC and unrelated to the activity of pharmacovigilance, companies must determine their storage period according to the characteristics of specific cases.

6.3. Subcontractors Management

In the case of hiring a company to carry out Pharmacovigilance, Cosmetic Products Vigilance and SAC and Quality activities, as applicable, the Contract must provide, in addition to a specific clause on the personal data confidentiality, other clauses specifically applicable to personal data protection such as the parties' (Controller or Operator)

qualification, the allocation of responsibilities, the management of the Holders' rights and others.

6.4. International Flow of Personal Data

In the case of multinational companies, it is possible that reports of adverse events and complaints about the quality of the product are sent for knowledge and handling of headquarters abroad. If the personal data sent is anonymized, there is no additional legal requirement related to this transfer.

However, if identification of the Holder is possible, it is necessary to observe the rules provided for in article 33 of the LGPD as well as the regulations and guidelines of the ANPD on the subject.

International data transfer may also be characterized by hiring a third person who stores all or part of the Controller's database on a server located outside Brazil, a situation already highlighted in subitem 3.5.

7
COMMERCIAL AND MARKETING SECTOR

The Commercial and Marketing Sector, through the Sales Force, often has access to several categories of personal data, especially those from health professionals and doctors. Such data are used both for the purpose of visiting these professionals and for sending invitations or collaborations when holding events, exhibitions, classes, congresses and others.

It is worth mentioning that, in certain companies, activities and actions related to the medical profession are subordinate to a medical directorate and not the commercial one.

7.1. Physicians' and Customers' Data

For the purposes of the analysis carried out in this Guide, we classify health-related professionals into three categories: **i)** professionals or clients who already have regular contact with the company, **ii)** those who are under Contract with the company and **iii)** prospective ones.

i. *Health-related professionals or customers in regular contact with the company.*
If there are voluntary acts that show interest in the products or information provided by the company, it is possible to sustain the legitimate interest as a legal basis for the handling of nonsensitive personal data, both from these professionals and from the customers (support and promotion of the Controller's activities).

ii. *Health-related professionals or customers under Contract with the company*
Handling of nonsensitive personal data from health-related professionals and customers can, among other possibilities, be based on the execution of the Contract (sponsorship Contract, supply Contract, etc.). However, if the handling involves sensitive personal data, the specific case must be analyzed in order to identify the appropriate legal basis.

iii. *Health-related professionals and prospective clients*
Handling of personal data for the purpose of commercial disclosure must be analyzed in the light of specific situations and it is possible to base the handling of personal data on the company's legitimate interests if there is no handling of sensitive personal data and this basis proves to be adequate after completion of the Legitimate Interest Tests. In this way, specific actions can be individually analyzed, taking into account the type of data handled and their primary source, notably if acquired from specialized companies. On the topic, it is worth mentioning that anonymized information or statistics on products prescribed in a given geographic area are not personal data for the LGPD purposes.

7.2. Privacy by Design

The Commercial, Medical, Access and Marketing departments are often at the forefront of reflections on new projects and communication strategies. In this sense, it is important to emphasize the importance of incorporating the principle of privacy by design when envisaging such projects. It is about taking into account the privacy rules recommended by the LGPD since the conception of new actions, projects and products envisaged by the company. Observation of this principle at the origin avoids subsequent modification of the processes in order to adapt them to the law.

8
MEDICAL AND CLINICAL TRIAL SECTOR

Activities of the Medical and Clinical Trial sectors taken into account for the purposes of this Guide consist of: **i)** contracting clinical studies, **ii)** managing the relationship with the medical profession and **iii)** managing patient support programs.

Clinical research is a well-regulated subject in Brazil. Personal data from both the doctors involved in the studies and those of patients are provided for by the Research Ethics Committees (CEPS), the National Health Council (CNS), the National Council of Research Ethics (CONEP) and Anvisa.

Often, a substantial part of clinical research is outsourced to a Representative Clinical Research Organization (ORPC) (or Contract Research Organization (CRO)). In these cases, the Sponsor does not have access to the identification of the patients involved in the research since the data are pseudonymous. Patients are mentioned in the study electronic clinical record by means of a code susceptible of identification solely by confrontation with the Free and Informed Consent Term, the safekeeping of which is the Research Institution's responsibility. Thus, this scenario does not seem to us to pose greater

challenges for members in relation to the management of personal data involved in this activity.

On the other hand, both ORPCs and companies that fully internalize clinical studies must adopt adequate methods to guarantee the security of their databases as well as the anonymization of the handled personal data, whenever possible.

Regarding the Patient Support Programs (PSP), it appears that this generic name includes some very different practices. For certain companies, PSP consist of donating medicines for health professionals hired by other institutions (associations, outsourced companies and others) for use by patients selected by them. In this model, the company does not have access to the personal data of the patients attended by the entity responsible for the Program, receiving only a report with the personal data of the doctors responsible for the application, the quantity of medicines supplied and the patients served.

Among other cases, the PSP consists of collecting personal data from patients in order to register them in a database, offering discounts on the purchase of medicines and health information. This type of program requires more attention since the company can collect and handle personal data related to the health of a significant number of people.

One of the first points of attention in relation to the programs currently underway concerns the information of the Holders of personal data on the handling carried out. In most cases, the information currently available to patients is restricted to the purposes of the handling, which is why such information must be complemented in order to adapt it to the LGPD requirements (form and duration of handling, information about the shared use of data, the Holders' rights and others).

9
TECHNOLOGY AND INFORMATION SECURITY SECTOR

The activities of the sectors related to Information and Communication Technology (ICT) taken into account for the purposes of this manual consist of **I)** Collection and use of personal data for management of access to the Data Network, Applications and Systems, **II)** Mapping of information and data assets, **III)** Information Security, **IV)** Response plan to Personal Data Security incidents.

The Information Technology sector processes personal data for the purpose of registering the initial access to the Company's data network and allowing the user, using an ID (Identifier) and a password, to access various services such as Corporate E-mail, Internet, Intranet, Telephony, Network services in general and other Systems/Applications made available according to the needs and function performed by the employee/service provider.

It is also the Information Technology sector's responsibility to maintain and monitor the organization's various assets. It is an area that ends up relating to the entire organization and that often knows the process of the areas in detail.

9.1. Collection, use and storage of data for access to network and information systems

Handling of personal data, including sensitive data in the case of biometrics resulting from Information Technology activities, may rely on some legal bases such as I – Consent II – Legitimate interest from the Controller and III – Execution of Contracts. It is important to note that the possibility of these legal bases is considered due to the need to grant access to employees (in this case, one can use the legal basis of the Controller's legitimate interest or Contract Execution, unless one does not collect biometric data that in this case may additionally require the data Holder's consent – visiting service providers (Consent legal basis) who may need access to the visitor's Wi-Fi network (Consent legal basis).

Points that should be highlighted in this type of data handling:

I. Collecting only the minimum amount of personal data necessary for achieving the purpose.

II. Considering the location where the data shall be stored (if there is international data transfer) and this should be informed to the data Holders.

III. Whether personal data shall be shared with third parties (for cases where access management is carried out outside the organization or where the access management system uses the SaaS (Software as a service) model). It is necessary to establish specific data handling clauses.

IV. Data retention period – establishing a temporality table based on legal and regulatory requirements for this type of personal data.

V. Maintaining transparency in the use of data for these purposes by means of training, notices, newsletters and other.

9.2. Mapping of information and data assets

The Information Technology area is an important player in the privacy and data protection scenario as it is able to assist in the understanding of relevant information about components of information systems by means of its CMDB (Configuration Management Database).

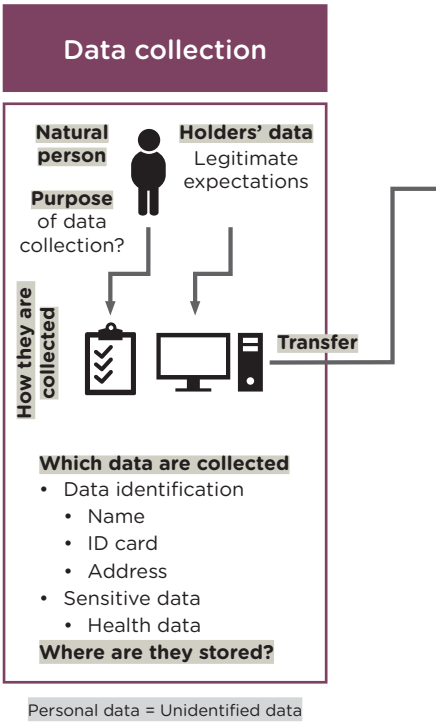
The CMDB offers an organized view of the data and the interconnection among the various types of assets (such as, for example, Systems, Hardware, Database, Location, Classification, Documentation, among other valuable items).

The combination of this information with the personal data handling record shall provide a final view of the data handled by the organization, enabling the necessary adjustments to be made to comply with the legal and regulatory requirements of the privacy and data protection rules and laws.

As an example, below is a mapping model for illustrative purposes:

DATA LIFE CYCLE

Collection, storage, use and disposal



Data storage

Computerized system? Spreadsheet? E-mail?

Data in transit

System name:

Where is it?

In which format?

Transferred within the group?

Sent to another system?

Database

Enriched with other data?

Who uses them?

How are they used?

Transferred to other countries?

Which activities?:

- Prospecting customers?
- Report creation
- Forecast
- Customer service?
- Payments?
- Services provision?

Shared data?

Technical and organizational measures for data protection?

DPA (Data Processing Agreement) or BCR (Binding Corporate Rules for Processors)?

Use of data disposal

Usage activities

Legitimate expectations?

Holder's rights?

Security:

Restricted access control?

Storage time?

Use of removable devices?

Data with the possibility of anonymization?

Are there other means of protection available?

Possibility to correct the data (keeping updated).

Is it expected by those involved that such an activity shall occur?

Legal basis for LGPD:

Conflict with other regulations?

Sensitive data = data on health, race, ethnicity, religion, politics, sexual life, genetic or biometric data.

9.3. Information security

It is important to conceptualize initially that information security is based on some pillars as well as disciplines that deal with specific topics.

The pillars of information security are:

I. **Confidentiality** – Ensuring that only authorized persons have access to information.

II. **Integrity** – Ensuring that the data maintain their original characteristics or that they are not altered without due permission and control.

III. **Availability** – Ensuring that the information is available for use at any time.

Some of the information security disciplines are:

I. **Access management** – A discipline that aims to ensure that access is controlled and monitored. Some of the topics that stand out are: Authentication, Authorization and Audit. It is also worth mentioning that the technology area has in its characteristic the privileged access of some of its members, which requires additional control (known as Privileged Access Management) to ensure that only duly authorized persons can access with this level of permission.

II. **Vulnerability management in information systems** – The objective of this discipline is to act proactively mitigating possible failures in systems or systems architectures that could compromise information. The process consists of identifying, classifying and addressing the vulnerabilities found. It is important to note that this "prioritization" is based on risk management, which consists of assessing the "probability" and "damage" that a vulnerability can cause in the asset

and, based on the risk grade, make a decision to minimize, avoid, mitigate or accept the identified risk.

III. **Cryptography** – A technique that encrypts data ensuring strong protection during data storage and/or transit. It is a technology that requires in-depth analysis before use as there are prerequisites for adopting such solutions that must be considered: 1) Encryption Type (Symmetric Key: the same key is used to encrypt and decrypt the data; Asymmetric Key: the key used to encrypt the data is different from the one used to decrypt the data). Another important item is the management of such keys against unauthorized access, loss or theft and that the process must comply with ICP Brazil, which is the Brazilian digital certification system.

IV. **Anonymization** – An item commonly referred to in the LGPD to mischaracterize data as personal. It is a technical resource that is characterized by the irreversibility of the process so that there is no reasonable condition to return to the original state, that is, "personal data". Some techniques used for anonymization are: 1) Suppression of attributes – this aims to remove a section or column in a database in the data set. 2) Record deletion – this is the removal of an entire record from the data set. 3) Character Masking – changing characters in a value of the data, for example, substitution by "*" or "x". 4) Pseudonymousness – The data lose the possibility of direct or indirect association with an individual and only by means of the use of additional information can the data Holder be identified.

V. **Additional topics that require attention** – 1) Information security policies that establish rules and standards for protecting information. 2) Malware protection software. 3) Software to prevent data leakage, known as DLP (Data loss prevention). 4) Cyber Insurance (when applicable to the model and risk to which the company

is exposed). 5) Security audits that can identify possible points for improvement. 6) Analysis of information security for critical systems (Pentest – it is a test that simulates attacks to systems and allows to anticipate possible vulnerabilities of the systems. Bug Bounty Program – it is an award program for researchers and developers who discover vulnerabilities in applications and systems).

9.4. Response plan for personal data security incidents

The response plan for personal data security incidents is an important item in meeting the requirements of the LGPD and consists of the measures that shall be adopted by the organization when an information security incident involving personal data is identified.

A security incident can be defined as an event or chain of events that compromises information on one or more of the three pillars of information security (Confidentiality, Integrity and Availability).

It should be noted that for the LGPD only cases involving personal data shall be considered. The topics below provide suggestions for possible basic steps in adopting a data security incident response plan:

I. **Registration of personal data handling operations** – The idea is to identify the volume of data, as well as the criticality of such data and, with that, prioritize databases containing "most critical information";

II. **Creation or designation of a crisis committee** – Identifying sectors and the respective managers in the organization who should be part of an action committee in view of an information security incident crisis involving personal data. Examples are the HR, IT, Legal, Communication, Investor Relations and Information Security sectors. It is important to define roles and responsibilities for each member of this crisis committee.

III. **Prior identification of suppliers** – Defining the need to use specialized services with third-party companies such as: 1) Computer Forensic Expertise. 2) Specialized Legal services. 3) Specialized technology and information security teams. 4) Specialized communication services with the press, media, customers and investors.

IV. **Defining an internal response structure** – Key people who guide internal and external communication must be identified. Another important point is to establish a response structure previously validated and approved for each specific audience, which include, among others: 1) The data Holder. 2) The National Data Protection Authority. 3) The specialized media. 4) The press. 5) Employees and Suppliers.

V. **Simulation of personal data security incidents** – The purpose of the simulation is to validate whether the points described in the plan actually work and how long it takes to mobilize the people involved, creating a crisis room, establishing the necessary contacts, creating the necessary communications and, at the appropriate time, monitor the repercussions in the media and press. Simulation is an important exercise that helps to measure the response plan efficiency and effectiveness.

VI. **Post-crisis measures** – Validating whether the "exposed" data actually constitutes an organization's database (Controller or Operator) and whether the data object of such an incident has the "Personal Data/Sensitive Data" structure.

VII. **Documentation of what happened** – Preparing detailed technical documentation of how such an incident occurred, what the lessons learned were, identifying possible systems that have the same exposure.

VIII. Investigations and collection of digital evidence – Identifying a possible person responsible for the crime as well as proving diligence in conducting digital analysis and evidence.

IX. Monitoring in web and deep web environments – In case of leakage of personal information it is important to monitor social networks, web and deep web for repercussions of the incident and to identify possible "sales or negotiations" of personal data related to the event. There are specialized services that can be hired for such monitoring.

ANNEX I

Suggested Consent Form Template (Nonbinding)

(Controller of Personal Data and Controller's Contact Information)

By this term I authorize the handling of my personal data for the purposes of (list the purposes).

I also authorize the sharing of my personal data with the group's companies and business partners involved in achieving the above purposes (if possible, list the companies with which the sharing is carried out or their lines of activity according to the purposes listed above, e.g.: travel agencies, hotels, telemarketing companies etc.).

(optional)

I authorize the international transfer of my personal data to the group's companies and business partners involved in achieving the above purposes located notably in the following countries (list the countries).

Name and qualification:

_____, _____ _____, 20_____.

_____

Signature