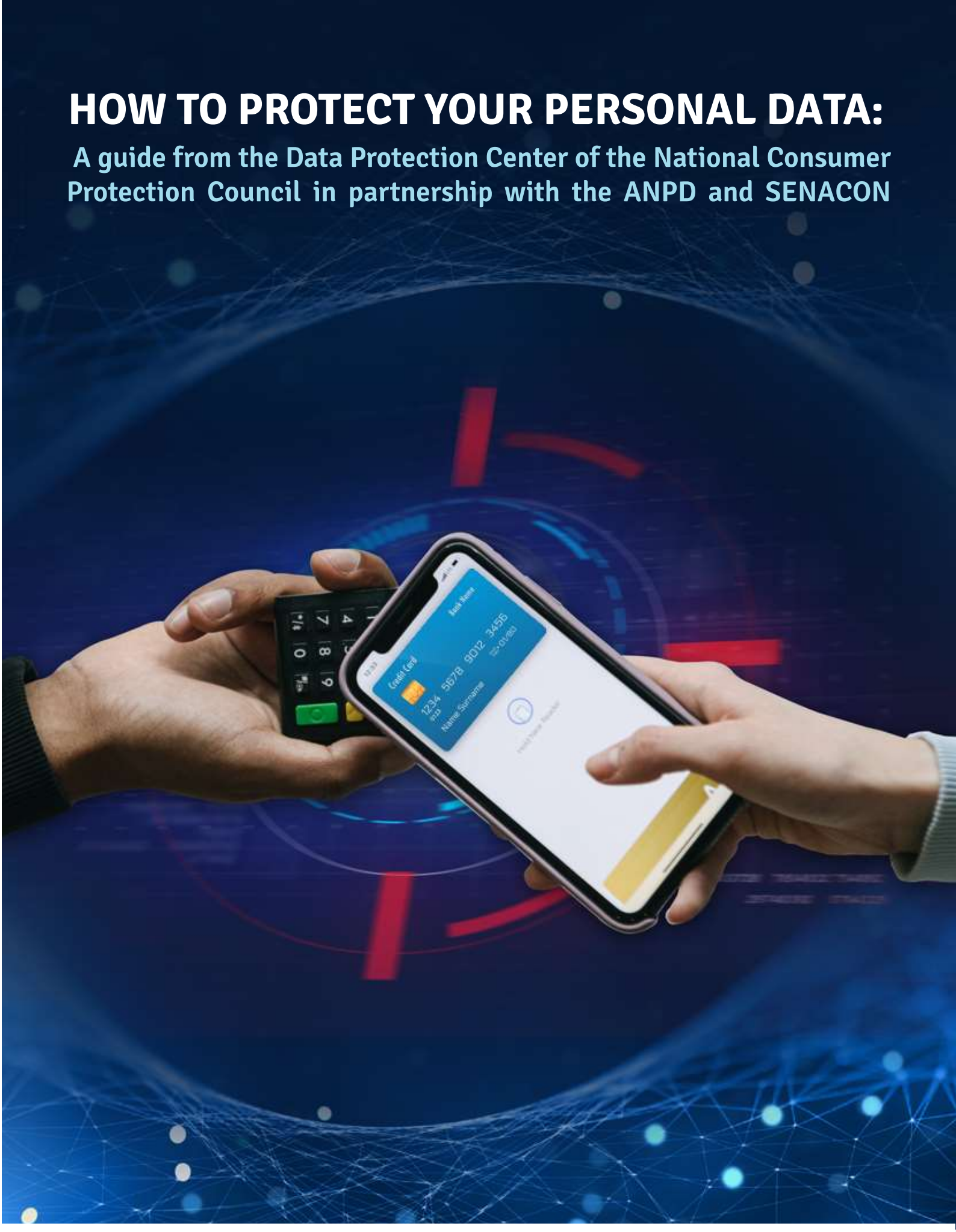
HOW TO PROTECT YOUR PERSONAL DATA:

A guide from the Data Protection Center of the National Consumer Protection Council in partnership with the ANPD and SENACON



SECRETARIA NACIONAL DO CONSUMIDOR
MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA
ANPD

Jair Messias Bolsonaro
Brazilian President

Anderson Torres
Minister of Justice and Public Security

Juliana Oliveira Domingues
Consumer Secretary

Waldemar Gonçalves Ortunho Junior
Chief Executive Officer of the National Data Protection Authority

Arthur Pereira Sabbat
Joacil Basilio Rael
Miriam Wimmer
Nairane Farias Rabelo Leitão
Officer of the National Data Protection Authority

Lilian Claessen de Miranda Brandão
Officer of the Department of Consumer Protection and Defense

Preparation team of the National Consumer Secretariat

Daniele Correa Cardoso
General Coordinator of Sindec

Maria Cristina Rayol dos Santos Sobreira Lopes
General Coordinator of Articulation and Institutional Relations

Andiara Maria Braga Maranhão
Coordination of the National Consumer Protection School

Production team of the National Data Protection Authority

Alexandra Krastins
Jeferson Barbosa
Managers

Isabela Maiolino
General Coordinator of Standardization

Lucas dos Anjos
Servant of the General Coordination for Technology and Research

Rodrigo Santana dos Santos
Coordinator of Standardization

Team of the Data Protection Center of the National Consumer Protection Council

Laura Schertel Mendes
Rapporteur of the Data Protection Center

Danilo Doneda
Member of the Data Protection Center

Marcela Mattiuzzo
Member of the Data Protection Center

Flávia Lira
Representative of the Consumer Protection and Defense Agency of the State of Rio de Janeiro

Production team of University of Brasilia

Prof. Dr. Ugo Silva Dias
Coordination

Janaina Angelina Teixeira
Pedagogical coordination

Angélica Magalhães Neves
Revision

Israel Silvino Batista Neto
Graphic design and formatting

1. YOUR PERSONAL DATA MATTER!

Your personal data is your representation in society and, therefore, it is part of your personality. It must be used fairly and safely, according to legitimate expectations. Brazilian General Data Protection Law (LGPD) guarantees that data is processed in a legal, appropriate, and safe manner.

When your personal data may be processed:

- ✓ Upon contracting a bank loan, data on your payment capacity is processed;
- ✓ When interacting on a social network, personal data on your behavior is processed;
- ✓ When participating in a company's loyalty program, data on your consumption may be collected;
- ✓ For health treatment in a hospital, personal data is processed including registration and health data.

We live in a society powered by data. Many activities in our everyday lives involve the collection, use, and sharing of data with companies or government agencies. We also share data on the Internet, be it when we shop or we use social networks.

2. WHAT IS THE GENERAL DATA PROTECTION LAW?

The General Data Protection Law (Law No. 13709/2018), also known as LGPD, created rules for protecting the personal data of all Brazilians aiming at guaranteeing the rights to freedom, privacy, and free of personality development. LGPD materializes rights provided in the Brazilian Federal Constitution of 1998 and it complements the protection granted by the **Consumer Protection Code** and the **Civil Rights Framework for the Internet**.

Data protection is important for the citizen, the economy, and the society as a whole. It empowers citizens to control their data and strengthens rights of freedom of expression, access to information, and rights to privacy, honor, and image. The law is also a tool for the Brazilian economic development, as it encourages the creation of new technologies in strategic sectors by small companies such as microbusinesses and startups, which have a differentiated regime under the law.

2.1 Who is the Authority?

LGPD created obligations and standards for whoever processes personal data and it instituted the Nacional Data Protection Authority (ANPD) to regulate data collection, use, processing, and sharing in the Country. The citizen may send complaints and reports on undue data processing directly to the ANPD. To have more information on the responsibilities and activity of the ANPD, the citizen may visit the following website: (www.gov.br/anpd).

2.2 Role of LGPD for legal security

LGPD also generates more legal certainty for both consumers and companies by more clearly defining situations in which personal data may be collected, processed, stored, and transferred legally, all common activities in an increasingly digital economy.

What are the risks for the consumer when there is illegal data processing?

- ✓ Behavior Monitoring and restriction to fundamental freedoms;
- ✓ Discrimination;
- ✓ Economic damages;
- ✓ Access restriction to goods and services;
- ✓ Privacy violation;
- ✓ Frauds that affect your identity;;

3. IMPORTANT CONCEPTS

What is a personal datum?

LGPD defines as personal data any **"information related to an identified or identifiable natural person"**. In practice, this means information that may be associated with a person, be it to identify them directly or to associate this data with a context thus allowing their identification.

There are personal data that circulate intensely and that allows the identification or definition of a person's profile based on less direct information, such as email address, mobile phone number, location, or Internet post. All this data may be considered personal data.

The following may be considered personal DATA, AMONG OTHERS:

- ✓ **Name and surname;**
- ✓ **Residential address;**
- ✓ **Email address (if it has elements that help identify the owner, such as name and surname;**
- ✓ **Gender;**
- ✓ **Date of birth;**
- ✓ **ID numbers such as General Registration (RG), Individual Taxpayer Identification Number (CPF), and Social Security Card;**
- ✓ **Geolocation data from a mobile phone;**
- ✓ **Personal phone number;**

Who owns the data?

According to LGPD, the owner of personal data is every natural person to which the processed data refer. Therefore, any person is the owner of personal data in some context.

Who are the processing agents?

In turn, the natural or legal persons, public or private, who process personal data for any purposes provided in LGPD are considered processing agents. In this case, LGPD lists as processing agents the data controller and operator.

The **processing agents** are those who carry out the collection, use, sharing, or other activities with the personal data. The law provides for two processing agents with distinct functions and responsibilities: the **controller** and the **operator**.

The **controller** is the processing agent responsible for making the main decisions regarding the processing of personal data, as well as defining its purpose and the essential elements of this processing.

He/she is responsible for complying with the rights created by LGPD for data owners. If the controller does not grant these rights, the owner may make a complaint before ANPD. For example, upon request, the controller is required by law to inform what data it has on the data owner. The refusal to present this information is not in compliance with LGPD, and the controller may be inspected and punished.

In turn, the **operator** is the processing agent that acts on behalf of the controller and they must process the data only according to their instructions and in compliance with the law.

Who is the Data Protection Officer?

LGPD establishes that the processing agents - such as companies and public agencies - indicate a **Data Protection Officer (DPO)**. It is a figure created to facilitate the communication of the processing agents with data owners and ANPD. Hence, the owner may request control over their personal data before the DPO, except in the event that ANPD rescinds this obligation, which may occur in given sectors or specific situations.

3.1 Personal Data Processing

3.1.1 Definitions

The LGPD defines data processing as any operation carried out with personal data, such as the following: production, receipt, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, elimination, assessment or control of the information, modification, communication, transfer, diffusion, or extraction.

See also:
BRAZIL. ANPD. *Guidance on treatment agents.* Available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acessed on Set. 2021

3.1.2 Processing Prospect

LGPD limits the situations in which the processing of personal data is possible. For such, the law lists legal basis that may be used in each case. There are ten possibilities for the processing of personal data:

- ✓ **when there is the consent of the personal data owner;**
- ✓ **when the controller needs to process these data to meet a statutory or regulatory obligation;**
- ✓ **when public administration executes public policies or in the conduct of its institutional functions;**
- ✓ **for the conduction of studies by research agencies;**
- ✓ **for the execution of a contract in which the owner is a party, upon the request of the data owner;**
- ✓ **for the exercise of rights in a judicial, administrative, or arbitral process;**
- ✓ **for the protection of the life and physical safety of the owner;**
- ✓ **for the protection of the health in a procedure performed by health professionals, health services, or a health authority;**
- ✓ **when necessary to meet the legitimate interests of the controller or a third party, except in the case of fundamental rights and freedoms of the owner that require the protection of personal data prevail; and**
- ✓ **for the protection of credit.**

In the case of the processing of personal data defined as sensitive, there are other legal basis that must be observed.

4. WHAT ARE THE PRINCIPLES THAT GUIDE DATA PROCESSING IN BRAZIL

It is important to identify what legal basis supports data processing in concrete cases. Hence, it is possible to verify if the activities are in agreement with LGPD. The processing of personal data must respect the principles of LGPD. They are the following:

- **purpose:** the processing of personal data must have a specific, clear goal which must be informed to the owner. The processing cannot occur with generic purposes;
- **need:** only personal data strictly necessary to achieve the initially defined goal must be processed;
- **adequacy:** the processing of personal data must be coherent with the purpose that motivated it;
- **transparency:** the owner must be informed clearly and appropriately about the relevant aspects and characteristics of the processing of their data;
- **free access:** the owner must have guaranteed access to their personal data at any time, in a facilitated manner, and at no cost;
- **data quality:** he processed personal data must be correct, precise, and updated;
- **security:** the personal data must be treated with physical and logical measures necessary to their protection, to prevent unauthorized access;
- **prevention:** whoever processes personal data must adopt measures that prevent processing in non-compliance with LGPD;
- **non-discrimination:** no processing may be performed for discriminatory, illegal, or abusive purposes;
- **accountability and rendering of accounts:** the processing agent must guarantee and demonstrate, in a documented manner, that they took all necessary, effective, and sufficient measures to adapt the processing to the legislation.

EXAMPLE OF APPLICATION IN A PURCHASE:

Question 1

What is the goal of this data processing? What is it for?

For a store to deliver a product purchased by a person at the indicated address, it must have this information.

Question 2

What data is necessary to achieve this goal?

In the case of delivery, the person's name, delivery address, and contact phone number (in case it is not possible to locate the person at the address) are necessary.

Question 3

Does the data effectively serve to achieve this goal?

If it is possible to make the delivery based on the information collected from the person, the answer is affirmative. However, if the data does not serve that goal, the processing needs to be based on another purpose. For example, the person's CPF may be necessary to issue the invoice but not to make the delivery.

Question 4

Is the person able to know that this processing is being performed and by whom it is performed?

If the person contacts the store, they need to be informed that the processing is taking place for the goal of delivering the product and also know which data is being used for this purpose. It is also important that the person know that that specific store is processing the data, including, if it is the case, that the store has a contract with other companies to make the delivery of the product (such as a carrier).

Question 5

Is the data updated and precise?

If this is untrue, it will not even be possible to make the delivery. The store must concern itself with having correct information, including to achieve the goal of that processing. It is clear that the information may change over time; for this reason, it is important to have mechanisms that allow the person to update their information (for example, if they are to make a new purchase, they need to confirm if the address remains the same).

Question 6

Is the data secure, and what problem preventive measures have been adopted?

It is important for the data to be stored in secure systems and that only authorized people have access to them. The store must also not allow all its employees to have access to the address of whoever made a purchase, but rather, only the people who needs this information to do their work - whoever makes contact with the carrier, for example.

Question 7

Is the data being used in a discriminatory manner, i.e., so to treat situations differently when they should be treated similarly?

It is fundamental that data processing does not generate discriminatory effects for the owner, given that the law prohibits abusive and illegal discrimination.

Question 8

Does the data processing occur transparently so other actors may control and monitor it?

The principle of accountability and rendering of accounts demands the demonstration by the agent of the adoption of measures that prove compliance with the data protection legislation.

5. WHAT ARE THE RIGHTS OF DATA OWNERS?

LGPD guarantees data owners the right to monitor and exercise control over their personal data in a facilitated manner free of charge. The specific rights established by LGPD are presented below.

> “In accordance with the principle of **transparency**, the law establishes the right of the data owner to **information**, i i.e., the right to be informed about how the data processing will occur.”

Hence, appropriate information on the processing, such as the purpose, form, and duration of the processing, identification of the controller, and any sharing with third parties, must be provided.

The owner also has the right to **confirm** the processing of their data by a controller, and, when the processing is confirmed, they will have **free access** to their own personal data. Both the confirmation and the access to personal data by the owner must be arranged immediately by the controller, and requests involving the origin of the data, the inexistence of a record, the criteria used, and the purpose must be met in up to 15 days.

The owner has the right to the **correction** of their incorrect personal data. This correction right comprises the possibility of updating the data and, when necessary, even the insertion of new data to the processing.

Whenever personal data is processed in non-compliance with the law or their processing is not necessary, it is up to the owner to request their **anonymization**, **blocking**, or even **exclusion**. It is also up to the owner to request the portability to another controller to which they wish to migrate the processing operation.

For personal data processing that has consent as a legal basis, it is up to the owner to request its **elimination**, without the need to explain the motivation.

Besides, the owner will be able to **revoke consert** they provided to the processing of their data at any time, without the need for grounds, and the controller must facilitate this procedure.

The owner has the right to **request information** on the entities with which there was shared use of their personal data; and, on the consequences of not providing their consent for the personal data processing, when they ask for it. The owner may also request information on the purpose of the processing, its form and duration, identification and contact information of the controller, information on the shared use of data by the controller and the purpose, responsibilities of the agents that will carry out the processing, besides any other information relevant to the specific processing.

When personal data is used to make automated decisions that are capable of concretely influencing their interests, it is up to the owner to request the **revision** of such decisions to be aware of the criteria and parameters used and contest them when it is the case.

The right to **request an explanation** on criteria and procedures adopted so they may make a decision is guaranteed.

The owner **cannot be charged** for the costs of the exercise of his/her rights. The deadlines for meeting their requests will be established by ANPD in regulation.

Lastly, the owner may postulate in favor of his/her rights before ANPD and before consumer protection agencies **whenever the data processing occurs in the context of a consumer relationship**.

How must public and private organizations act on the processing of personal data?

- ✓ **Guaranteeing** that all personal data processing has a legal basis;
- ✓ **Maintaining** a record of data processing operations;
- ✓ **Elaborating** an impact report to the protection of personal data when processing may generate risks to civil freedoms and fundamental rights of the owners;
- ✓ **Conceiving** secure systems that protect the data from their conception;
- ✓ **Informing** data owner and ANPD about personal data security breaches that may cause relevant risk or damage, with due containment or mitigation measures;
- ✓ **Informing** data owner if there is any alteration to the data collection purpose;
- ✓ **Repairing** damages caused due to the processing of personal data that violates the legislation;
- ✓ **Confirming** the existence or arranging access to personal data upon the request of the owner;
- ✓ **Disclosing** the types of data collected;
- ✓ **Describing** the methodology used for collecting and sharing data;
- ✓ **Discribing** the methodology used to guarantee the security of the information;
- ✓ **Assessing** the safeguards and risk mitigation mechanisms adopted in a permanent way;
- ✓ **Indicating** the DPO and disclosing their contact information publicly;
- ✓ **Accepting** complaints, communications, and providing clarifications to data owners;

How may the data owner protect their personal data?

- ✓ **Creating** backups of the stored data, especially in the “cloud”;
- ✓ **Activating** cryptography in disks and external media such as pen drives;
- ✓ **Creating** strong passwords that contain the combination of special characters, upper-case and lower-case letters, and numbers, avoiding using personal data or common words;
- ✓ **Enabling** the two-step password verification whenever available, especially in cloud storage systems and message applications;
- ✓ **Installing** only applications from official sources and stores;
- ✓ **Updating** operating systems and applications always;
- ✓ **Deleting** stored data before discarding equipment and media;
- ✓ **Distrusting** links received through message applications;
- ✓ **Limiting** the disclosure or provision of personal data on the Internet, including on social networks or to companies, to the strictly necessary cases.

For more about the theme, see:
https://cartilha.cert.br/fasciculos/protecao-de-dados/fasciculo-protecao-de-dados.pdf
https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo-vazamento-de-dados.pdf

What to do in case of a violation of my rights? Who shall I seek?

In case your rights have been violated, gather all pieces of evidence you have, such as emails, message app prints, newspaper articles, communication from the organization about the incident, among other proof. When it is a consumer relationship, it is possible to register a complaint at Consumidor.gov.br or with consumer protection and defense authorities such as Consumer Protection Offices (Procons), Public Defenders' Offices, Public Prosecutors' Offices, etc.

Seek the company to solve your problem

With the maximum information at hand, seek the responsible company immediately, inform what happened, write down the service data (protocol number, guidance received, etc.), and store the messages and emails forwarded. And, in case you do not obtain a solution for your complaint, seek the competent authority to report the violation of your rights. With this direct contact with the company, it is possible that the requests of the data owners are met swiftly.

Contact ANPD

In case your request is not met by the responsible processing agent, you may file a complaint with ANPD, following the instructions available in the service channels https://www.gov.br/anpd. The establishment of an administrative process against the organization is possible, and it may culminate with the application of the sanctions provided in LGPD.

What if the disrespect of my rights occurs in a consumer relationship?

Access Consumidor.gov.br

Consumidor.gov.br

You may establish communication directly with the company through the platform Consumidor.gov.br in a faster and bureaucracy-free manner, from the comfort of your own home. The platform is a public service that is entirely free of charge, it is maintained by the National Consumer Secretariat (Senacon) of the Ministry of Justice and Public Security (MJSP).

Currently, the platform has over 1000 participating companies and an average solution index of 78% in a period of about 8 days.

How does Consumidor.gov.br work?

a. First, the consumer must verify if the company they wish to complain about is registered in the system.

b. The consumer then registers their complaint on the website, and, from there on, the deadline countdown begins, the company has 10 days to reply. During this period, the company has the opportunity to interact with the consumer before posting their final answer.

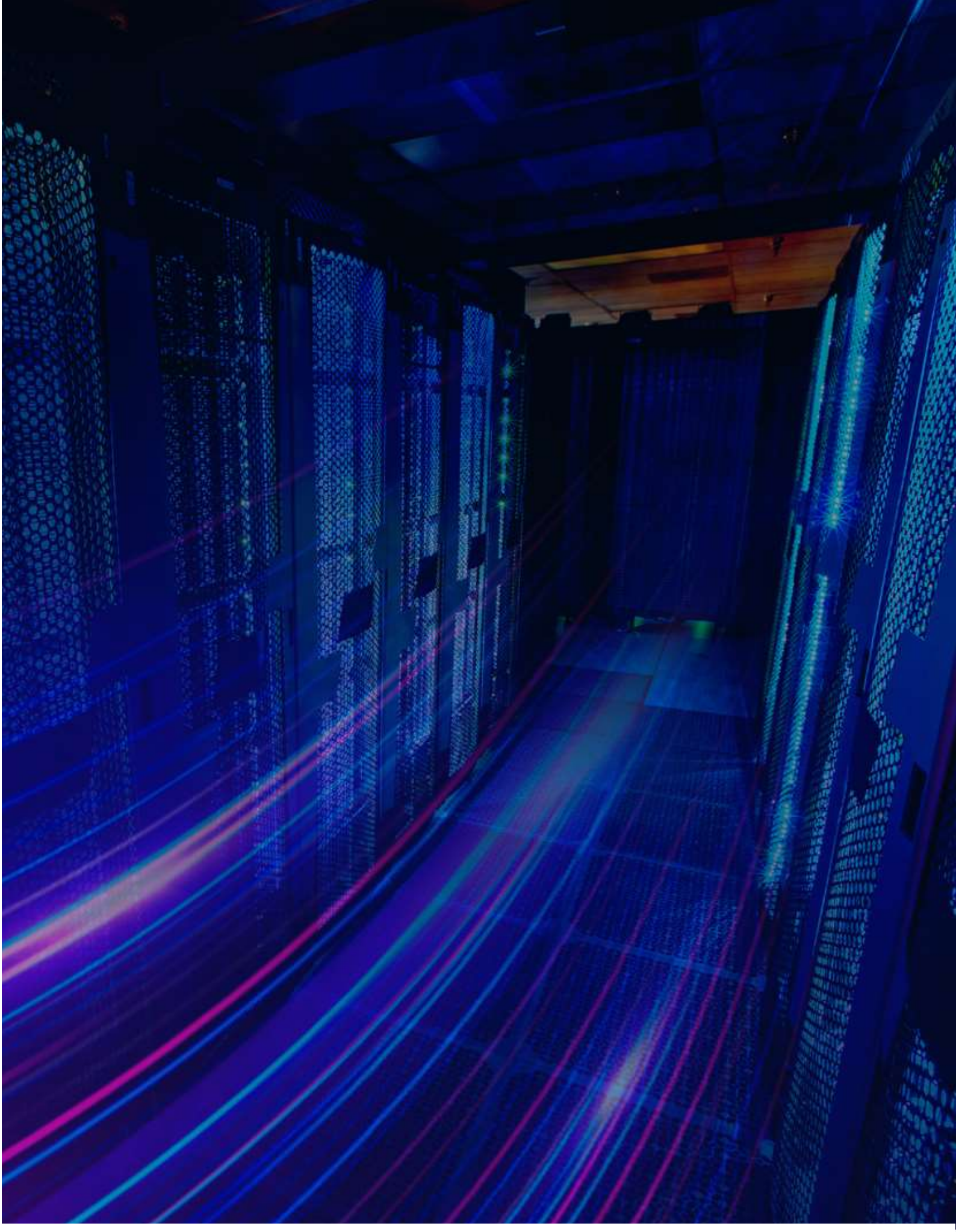
c. After the company´s reply, the chance to comment on the response received is guaranteed to the consumer, in addition to classifying the demand as Resolved or Unresolved, and even indicating their satisfaction level with the service received.

Consumer Protection Offices (Procons)

You also have the Consumer Protection Offices (Procons), which have in-person and electronic services. When the complaint is presented at Procon, the company is called to clarify the demand, and an opportunity for a conciliation hearing with the consumer is given. There is no need to be accompanied by an attorney. If an agreement is not reached, an administrative process may be opened by Procon, and the company may be subject to the penalties indicated in the Consumer Protection Code. If necessary, you may start a suit before the Judiciary Branch.

Caution!

If there is an indication of fraud or suspicion of identity theft, the owner must formalize the complaint through a Police Report before the competent police authority. This may prevent damages such as the cloning of credit and debit cards, invasion of email or social network accounts, or even the use of your identity to obtain unauthorized loans or other types of fraud.



SECRETARIA NACIONAL DO CONSUMIDOR

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

ANPD