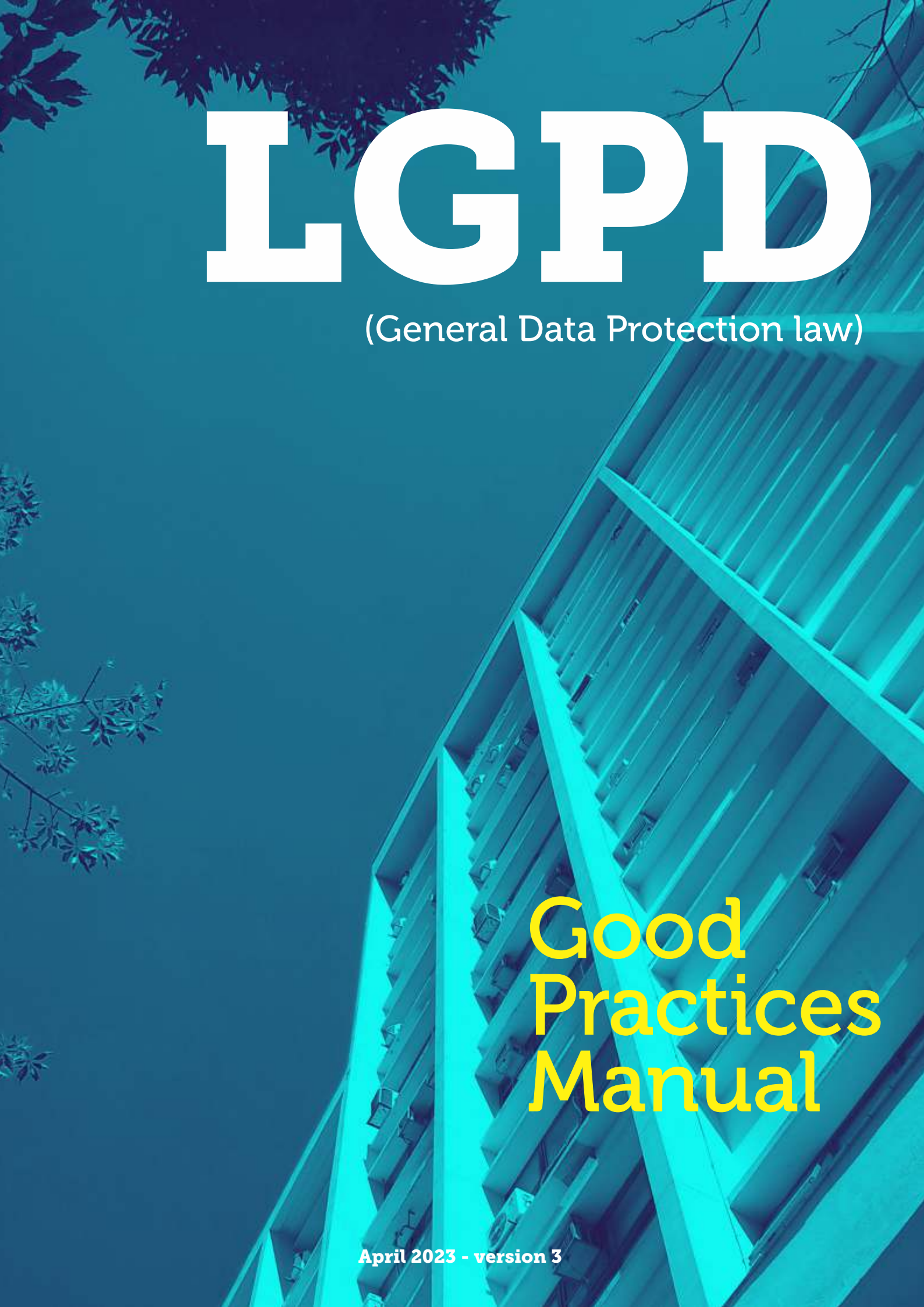


LGPD

(General Data Protection law)

Good Practices Manual

April 2023 - version 3

PROTECTION AND PRIVACY

On February 10, 2022, the National Congress recognized that the protection of personal data, regulated by Law No. 13,709/2018 (General Data Protection Law - LGPD), is a fundamental right of the human being. At PUC-Rio, we are all responsible for the use and disclosure of personal data within our community. We also have rights regarding the use of our own data. Therefore, it is essential to observe the provisions of the LGPD to avoid sanctions and legal proceedings.

In this context, this electronic magazine aims to inform the PUC-Rio community about the main rules of the LGPD and, without claiming to exhaust the subject, seeks to recommend some ways of handling data that you will use in your day-to-day activities.

PRESENTATION

We have created this manual to help the PUC-Rio community understand the basic concepts of the General Data Protection Law – LGPD. The manual is a useful tool that provides an easy and direct reference. In it, you will find answers to key questions regarding the handling of individuals' data, including considerations for operations such as collection, production, and storage of printed copies and emails, among others.

The first part of the manual presents the definition of concepts, basic rules, and the role of each data processing agent within the scope of the law.

The second part focuses on daily work routines, guiding on how to follow and implement good practices in data handling at the University. Presented in a didactic format, in a question-and-answer style, the manual outlines what can and cannot be done with personal data.

So, let's then understand the responsibility and care we must have when dealing with personal data.

PART #01

The General Data Protection Law (LGPD) - Law No. 13,709, of August 14, 2018 - was created to protect the fundamental rights of freedom, privacy, and also the free formation of the personality of each individual.

It concerns the processing of personal data, whether in physical or digital form, carried out by natural or legal persons, whether public or private.

The processing of personal data, according to LGPD, can be carried out by two agents, namely:

Meet the key roles within LGPD:

1. Controller - responsible for decisions regarding the processing of personal data, such as purposes and means of processing (Article 5, VI);
2. Operator - performs the processing of personal data on behalf of the controller.

In addition to these two agents, there is also the Data Protection Officer (DPO), defined as the person appointed by the controller to act as a communication channel between the controller, data subjects, and the National Data Protection Authority (ANPD).

Two key principles to highlight:

1. Storage of only essential data for the execution of activities;

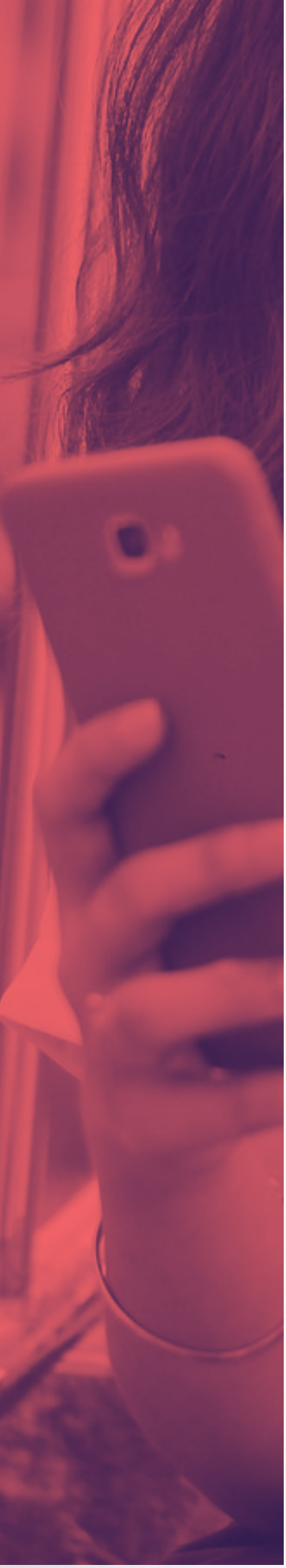
2. Relevance of discarding data that is not necessary.

Before delving into the principles of LGPD, three ideas are worth emphasizing:

1. The importance of minimizing the use of data to the maximum extent possible;

2. Storage of only essential data for the execution of activities;

3. The relevance of discarding data that is not necessary."



NOW LET'S EXPLORE 6 CONCEPTS AND SOME GENERAL RULES OF LGPD:

1. What is data processing?
Data processing encompasses collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, disposal, evaluation, among other activities that involve the use of personal data in the execution of their operation.

2. What are personal data?
Personal data refers to information related to an identified or identifiable natural person, such as name, CPF (Brazilian individual taxpayer registration), phone number, address, etc.

The LGPD also pertains to sensitive personal data, which includes information about racial or ethnic origin, religious beliefs, political opinions, union membership, or data related to health, sexual life, genetic or biometric data, as well as information of a philosophical, religious, or political nature.

3. In which cases does LGPD NOT apply?
The Law on the processing of personal data does not apply in the following situations:

a) When carried out for exclusively private and non-economic purposes;

b) When applied for exclusively journalistic, artistic, and academic purposes;

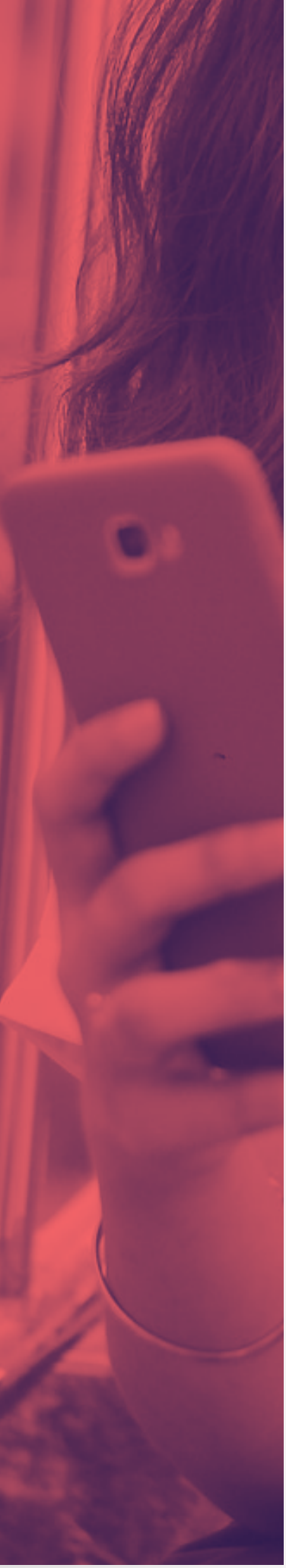
c) When used for exclusive purposes of public security, national defense, state security, or activities of investigation and repression of criminal offenses;

d) When originating from outside the national territory and not subject to communication, shared use of data with Brazilian data processing agents, or the subject of international transfer of data to another country, provided that it provides a degree of protection of personal data appropriate to that provided for in LGPD.

4. What are the legal bases for data processing?
Get to know the 10 hypotheses, called legal bases, in which the LGPD authorizes the processing of data:

I. Consent by the data subject. This is the rule of autonomy of will. It is the free and unequivocal expression by which the data subject agrees to the processing of their personal data for a specific purpose.

II. For compliance with a legal or regulatory obligation by the controller. It exempts the need for the data subject's consent. This is the rule of broad legality and the preservation of public interest over private interest. Such authorization allows the law not to conflict with other existing legislations or regulations.



III. By the public administration, for the processing and shared use of data necessary for the execution of public policies provided for in laws and regulations or supported by contracts, agreements, or similar instruments.

IV. For the conduct of studies by a research entity, ensuring, whenever possible, the anonymization of personal data. It exempts the need for the data subject's consent. Strict use for the purpose of conducting studies by a public or private research entity.

V. When necessary for the execution of a contract. In this case, it exempts the need for new consent from the data subject, provided that the processing of the data in question is essential for the proper fulfillment of the contract.

VI. For the regular exercise of rights in judicial, administrative, or arbitration proceedings, in accordance with Law No. 9,307, of September 23, 1996 (Arbitration Law).

VII. For the protection of the life or physical safety of the data subject or a third party. In this case, it exempts the need for consent from the data subject in cases of the necessity to protect the greater good of the natural person, life, both encompassed within the concept of human dignity as a foundation of the Republic.

VIII. For the protection of health exclusively, in procedures carried out by healthcare professionals, healthcare services, or health authorities.

IX. When necessary to meet the legitimate interests of the controller or a third party, except in cases where the fundamental rights and freedoms of the data subject that require the protection of personal data prevail.

I - Support and promotion of the activities of the controller;

II - Protection, concerning the data subject, of the regular exercise of their rights or the provision of services that benefit them, respecting expectations, rights, and fundamental freedoms, in accordance with the LGPD.

X. For credit protection, including as provided in relevant legislation, it exempts the need for the data subject's consent.

5. What should I be concerned about in the processing of personal data?

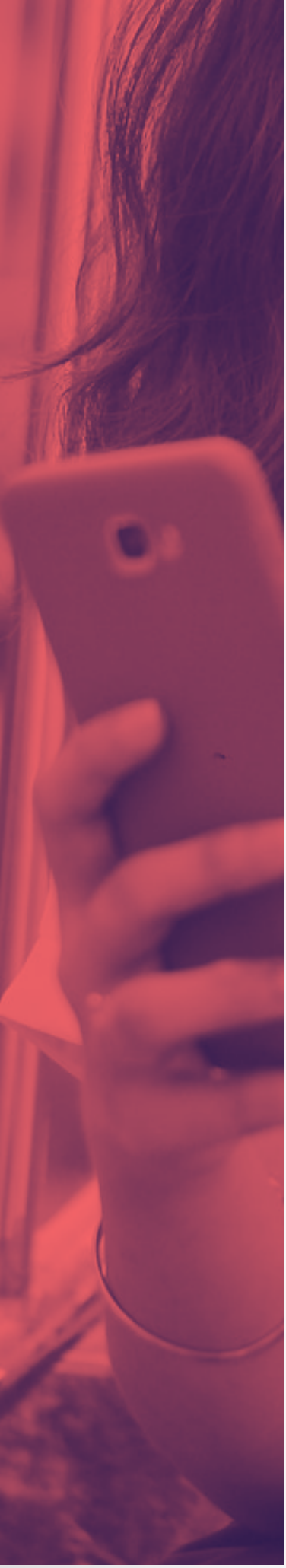
a) Identify the purpose: Determine the purpose for which data processing is necessary. Purposes should be legitimate, specific, and explicit (principle of purpose).

b) Define how the purpose will be communicated: Specify how the purpose of data processing will be communicated to the data subject, and this should be done before the commencement of data processing (principle of purpose).

c) Treatment of data initiated before the law's enactment: In the case of data processing that began before the law's enforcement, outline the steps to inform the data subject about the processing and its intended purpose (principle of purpose).

d) Ensure data processing aligns with the informed purpose: Guarantee that data processing is only for the purpose informed to the data subject (principle of adequacy). Any changes in the purpose of processing should also be communicated to the data subject.

e) Limit data usage to the necessary minimum: When planning the data processing method, strive to limit the use of information to the minimum necessary (principle of necessity).



f) When deciding to process data, define in advance the mechanisms and procedures that data subjects should use to easily and free of charge inquire about the content, form, and duration of the processing of their personal data (principle of free access).

g) Ensure that any changes to the specified purpose for data processing, the form or duration of processing, and the scope of sharing are communicated to the data subject (principle of free access).

h) Define a continuous verification procedure regarding the accuracy, clarity, relevance, and updating of the data subject's data. The goal is to remain faithful to the informed processing purpose (principle of data quality).

i) Observe the need to ensure that the data subject has the option to easily obtain clear and accurate information, upon request, about the processing of their data and the respective data processing agents (principle of transparency).

6. What is a personal data security incident?

Incidents can occur accidentally, such as sending information to the wrong recipient, or as a result of intentional acts, such as invading an information system or stealing a data storage device.

It is a confirmed adverse event that compromises the confidentiality, integrity, or availability of personal data. It can result from voluntary or accidental actions that lead to the disclosure, alteration, undue loss, or unauthorized access to personal data, regardless of the medium in which they are stored.

Source: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-detratamento/comunicado-de-incidente-de-seguranca-cis

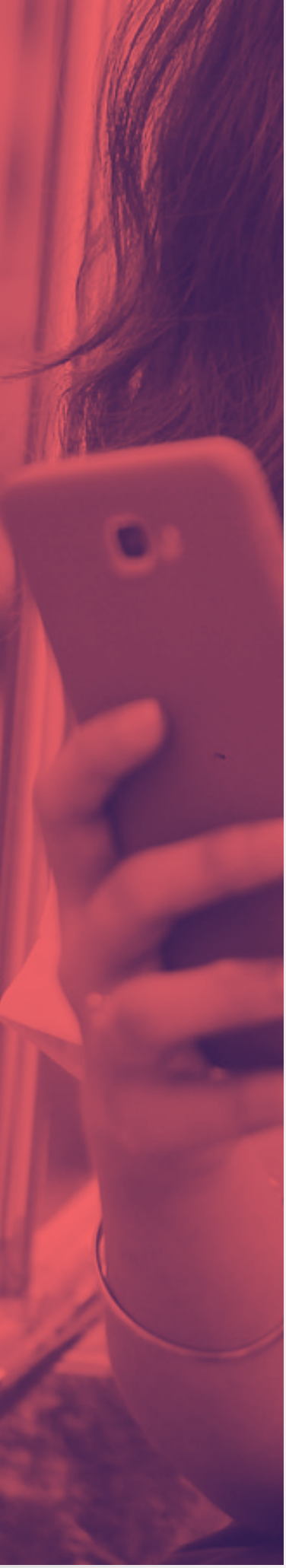
7. When using a corporate cell phone, employees/teachers cannot process personal data, as per LGPD terms, through applications such as WhatsApp, under penalty of being held responsible for any security incidents. For the processing of personal data, only official communication channels should be used, and when using applications like WhatsApp, it should be used on a corporate account.

8. Sanctions for Non-compliance with LGPD:

I - Warning, with an indication of a deadline for the adoption of corrective measures;

II - Simple fine, up to 2% (two percent) of the private legal entity's gross revenue, group, or conglomerate in Brazil in its last fiscal year, excluding taxes, limited in total to R$ 50,000,000.00 (fifty million Brazilian Reais) per infringement;

III - Daily fine, subject to the total limit referred to in item II;



IV - Public disclosure of the infringement after duly investigated and confirmed occurrence.

V - Blocking of the personal data related to the infringement until its regularization.

VI - Deletion of the personal data related to the infringement;

(...)

X - Partial suspension of the operation of the database related to the infringement for a maximum period of 6 (six) months, extendable for an equal period, until the regularization of the processing activity by the controller;
XI - Suspension of the exercise of the processing activity of the personal data related to the infringement for a maximum period of 6 (six) months, extendable for an equal period.

XII - Partial or total prohibition of the exercise of activities related to data processing.

In addition to the administrative sanctions that can be imposed by the national authority, the data subject who believes that their rights have been violated may seek civil liability for damages, in accordance with Article 42 of the LGPD: "Art. 42. The controller or the operator who, in the exercise of the processing of personal data, causes material, moral, individual, or collective damage to others in violation of the personal data protection legislation, is obliged to repair it." V - Blocking of the personal data related to the infringement until its regularization;

PART #02

A tool to assist in your routine

SEE HOW TO APPLY THE BEST DATA PROCESSING PRACTICES IN CARRYING OUT YOUR PROFESSIONAL ACTIVITIES AT THE UNIVERSITY.

1. Where should personal data be stored at PUC-Rio?
All data should be stored in a secure location, preferably in folders located on the RDC server, in the University's corporate systems, or in content management software, such as SharePoint, already available at PUC-Rio.

2. What to do with data that is in physical documents (paper)?
In this case, physical documents should be archived in lockable cabinets. Do not leave papers with personal data exposed on desks/workstations.

3. Should I be cautious with printed copies and spreadsheets?
Yes, you should store them securely, as mentioned above, or dispose of them in a secure manner. Avoid making unnecessary printed copies and Excel spreadsheets.

4. What other precautions do I need to take with physical files or documents?
When leaving your workplace, ensure that there are no files with personal data open on your computer or papers exposed.

NOTE1: Files containing recordings of meetings/classes contain personal data (such as names and faces of participants). Do not share such files with third parties to ensure the privacy of participants.

NOTE2: Exercise caution when sharing email histories/exchanges with more recent recipients. Older messages may contain personal data of third parties that should not be known to these more recent recipients. Forward only the messages that are essential.

5. What are the recommendations for email usage?
To ensure the security of email services and protection against the main causes of security incidents, we recommend that all professors and technical-administrative staff preferably use the email address with the domain "puc-rio.br" for communications related to their functions at the University.

6. Can I create email lists to send communications?
Minimize the use of email lists within Departments/Units, and instead, utilize the official email lists provided by the University.

7.Can teachers and staff use WhatsApp lists or other application programs to communicate with students?
In principle, everyone should avoid WhatsApp or other applications because they are not traceable. Prefer the use of broadcast lists.

The student/teacher should be the one to have the interest in participating in any groups, and they should have the option to leave them at any time without academic prejudice.

If the use of WhatsApp is truly necessary, activate two-factor authentication to protect the information contained there, including the access password to the application account.

8. Can I use email data for marketing purposes?
If it is of genuine interest to the University, you can use the email lists. However, pay attention: the person receiving the email must have the right to immediately opt-out of the message and stop receiving further emails on that topic (for example, by including an unsubscribe tool in the message - "opt-out").

9. What type of messages am I allowed to use for marketing?
I can only promote courses/events from the University itself (and those institutionally supported by PUC-Rio), without including content of diverse interest, such as the promotion of courses conducted by professors outside the University and other external events.

10. When do I need to use the data subject's consent?
When there is no other legal basis justifying the processing of their data, the data subject may consent to its use, depending on the purpose of the processing. They need to know which data will be processed to give free, informed, and unequivocal consent.

Consent can be given through a physical signature, by clicking a button ('electronic consent'), checking an option in a text box (which must be unchecked; the use of pre-checked options invalidates consent), or by recording audio or video confirming acceptance of the terms and conditions.

It is recommended to provide the data subject with the option to review these consent terms as well as to withdraw them at any time. Departments and Units handling sensitive data need to be attentive to the request and storage of consent terms.

11. Where can I find the consent terms?
The Working Group on the General Data Protection Law (LGPD) can provide guidance to Departments and Units regarding the need for using the Consent Form. In case of doubts, please access the LGPD Service Channel through the link below:

https://sgu.rdc.puc-rio.br/SGUWeb/protocolo/WApresentaProtocolo.aspx?idCC=2

When applicable, these Consent Terms should be signed electronically and stored in a secure environment.

12. Do I need to request consent signatures for each interaction or inquiry?
There is no need to obtain the consent form for each processing activity, provided that the purpose and legal basis are the same. This should be stated in the document, along with the right of the data subject to revoke the consent given. Please include this information in the document.

13. How do the security and privacy policies work?
For more information on PUC-Rio's Security and Privacy Policy, please visit the link: https://www.puc-rio.br/sobrepuc/lgpd/.

14. How should information and documents containing personal data circulate at PUC-Rio?
The use of PUC-Rio's Service Center through SGU should be prioritized. This tool should be used for exchanging information and sending documents between departments involving personal data of professors, staff, students, and also non-affiliated individuals.

15. What do I need to do to obtain the signature of the legal representative of PUC-Rio?
To obtain signatures on documents, contracts, agreements, and cooperation terms, it is necessary to seek the signature of the Rector, Vice-Rectors, or those who have the authority to sign on behalf of the University.

The prioritized use of electronic signatures is recommended. For documents submitted in printed form, Departments and Units should scan them after signature and archive the final version in SGU.

Regarding contracts managed on third-party platforms, the procedures of the platform should be followed, and after signature, the document should be uploaded to SGU.

16. What is the correct procedure for signing documents?
To minimize physical document handling, it is strongly recommended to use electronic signatures for administrative agreements, confirmations, authorizations, requests, statements, and other signable acts. This provides security, speed, sustainability, and mobility—whether on a desktop, laptop, or mobile device—for online document signing with legal validity, eliminating the need for digital certification. Electronic signatures can be performed directly through SGU access (Administrative – Electronic Signature) at no cost to the University Department/Unit. Integration with our management system and the CertiSign company portal not only ensures user-friendly functionality but also assembles and indexes a single database of electronically signed documents for future access.

17. What is the correct procedure in case of a personal data security incident?
When an employee notices a personal data security incident, they should immediately contact the PUC-Rio Service Channel and report the incident using the following link:
https://sgu.rdc.pucrio.br/SGUWeb/protocolo/WApresentaProtocolo.aspx?idCC=2

If you still have questions regarding LGPD, please contact encarregado-lgpd@puc-rio.br

This manual may undergo regular updates, considering the current legislation and institutional demands.