



GENERAL TERMS OF USE AND PRIVACY AND DATA PROTECTION STATEMENT OF SERPRO CORPORATE AND ELECTRONIC COMMERCE WEBSITES

Linked to the **Serpro Privacy and Data Protection Policy - PPPD**, pursuant to the provisions of item 7.0 of the [PPPD Statement](#).

1.0 PURPOSE

The Federal Data Processing Service - SERPRO, a public company linked to the Ministry of Economy, considering:

I. the grounds of Law No. 13,709, of August 14, 2018, which provides for the protection of personal data, namely:

- a) respect for privacy;
- b) informative self-determination;
- c) freedom of expression, information, communication and opinion;
- d) the inviolability of intimacy, honor and image;
- e) economic and technological development and innovation;
- f) free enterprise, free competition and consumer protection; and
- g) human rights, the free development of personality, dignity and the exercise of citizenship by natural persons.

II. the entire content of Law No. 13,303, of June 30, 2016, known as the Law of State-Owned Companies;

III. the entire content of Law No. 12,527, of November 18, 2011, called the Law on Access to Information (LAI);

IV. the entire content of Law No. 12,965, of April 23, 2014, called Marco Civil da Internet [Brazilian Civil Rights Framework for the Internet];

V. the entire content of the Serpro Security Program (PSS) and the Corporate Information Security Policy (PCSI);

VI. the entire content of its Serpro Privacy and Data Protection Policy (PPPD);

VII. the entire content of the NBR ISO/IEC 27.701 standard.

It undertakes to make this declaration public and accessible to its customers, users, other interested parties and the general public, which shall come into force in the following terms.

2.0 DEFINITIONS

For the purposes of this Statement, the following definitions apply:

- a) categorization of information: form of organization of information processing within Serpro, corresponding to the so-called “information classification”, in other companies, in order to guarantee unity and coherence in the treatment of data and information;
- b) client: individual or legal entity who maintains a commercial relationship with Serpro, through a service provision contract;
- c) confidentiality: guarantee that the information is accessible only by authorized persons;
- d) business continuity: set of business processes configured so that the organization continues to deliver products or services at an acceptable level previously defined after interruption incidents;
- e) personal data: information related to the natural person, identified or identifiable;
- f) integrity: guarantee of the accuracy and completeness of the information and the methods of its processing;
- g) partner: legal entity with which Serpro maintains a relationship of cooperation and reciprocal support, through agreements, terms of cooperation or similar;
- h) information security: set of practices and methods aimed at preserving the confidentiality, integrity and availability of information handled within the organization;
- i) Holder: the natural person to whom the personal data that are being processed refer to;
- j) treatment: any operation performed with personal data, such as those referring to the collection, production, reception, classification, use, access, crossing, reproduction, transmission, distribution, processing, filing, storage, disposal, evaluation or control of information, modification, communication, transfer, diffusion or extraction; and
- k) user: individual or legal entity who accesses Serpro's services regardless of having data registered in its systems and services, but who, for this access, provides personal data of any nature, with explicit use consent.

3.0 PRIVACY

Serpro acts in line with its institutional mission, respecting the right to privacy and aiming at the best use of information technology for the satisfaction of its customers and society, and the sustainability and business autonomy, guaranteeing the stability and continuity of its services.

Privacy is considered, for the purposes of this Statement, the attribute of certainty on the part of the client, the user and other interested parties in relation to:

- a) the way in which Serpro's services, systems, processes and people act and behave in relation to these agents; and
- b) the reasonable expectation of discretion and the preservation of their interests and information of any nature.

3.1 Exceptions

Excluded from the restriction that privacy imposes, and within the limits of exceptionality that justifies it, is information:

- a) that corresponds to the hypotheses of Article 4 of Law 13,709/2018;
- b) public by legal determination;
- c) object of a final and unappealable judicial decision, by the disclosure or display of the information or data;
- d) ostentatious with a duty of active transparency;
- e) ostensible with a duty of passive transparency;
- f) already made publicly known by act of the holder;
- i) created and managed within the scope of the working relationship between the company and its employees, which is fundamental to the exercise of directive power, within the strict scope of this purpose; and
- j) data necessary for the legitimate performance of Serpro in fulfillment of its institutional mission and within the limit of the purpose adequate to the applicable legal basis.

3.2 Categorization of information

Serpro maintains a systematic model for categorizing information, in accordance with the Law on Access to Information (LAI) and the General Data Protection Law (GDPL), and ensures, under the terms of article 8 of Law No. 5,615, of October 13, 1970, for the confidentiality of the information and data it deals with, whether personal or not, in addition to maintaining alignment with good security practices and technological treatment, and with the most advanced governance practices, using NBR ISO, COBIT/ISACA, ITIL and similar models in their activities.

3.3 - Sensitive Data

Serpro understands that the processing of sensitive data is subject to greater legal rigor and more severe supervision, by the National Data Protection Authority and, in this sense, it handles sensitive data exclusively under the canopy of one of the legal hypotheses of Article 11 of GDPL, preferably with informed and categorical consent.

3.4 - Children's Data

Likewise, with regard to data on children and adolescents, Serpro, in line with the terms of item 5.4 of its PPPD, will handle any processing according to the following commandments:

3.4.1 - With regard to data processing based on consent - Serpro will only process data from children (up to 12 years old) with the consent of the parent or guardian, under the terms of the Law;

3.4.2 - Regarding the processing of data on minors under 16 years of age and in the case of treatments based on other legal bases, Serpro will operate in accordance with the provisions of the Statute of Children and Adolescents and other rules applicable to the species.

4.0 PRINCIPLES OF PERSONAL DATA PROTECTION

The protection of personal data observes the following principles, with regard to their application, management and form of interpretation.

4.1 Principle of the protection of personal data

The processing of personal data within the scope of Serpro is done with attention to the rights of the holders of personal data and to the contractual and legal requirements.

4.2 Principle of actuality

This Statement is dynamic and consistent with the state of the art in technology and should be read and interpreted in its latest version, published on the webpage www.serpro.gov.br.

4.3 Principle of integrity

The services provided by Serpro are focused on the public purpose and the fulfillment of its institutional mission, under the terms of the law, and under no circumstances should they converge with private interests, especially those that offer or may offer losses to the Federal Public Administration or to the company's services.

4.4 Principle of universality

Serpro acts on behalf of its customers and does not offer, in relation to them, any degree of priority or disregard for each other, acting with neutral treatment, in relation to guaranteed service levels, except in the cases in which, for contractual option, there is this differentiation in an explicit and pre-defined way.

4.5 Legal protection of institutional customer data

The data and manipulated elements related to services provided to Serpro's clients, whether personal or corporate, are treated with due confidentiality, under the terms of article 8 of Law No. 5,615, of October 13, 1970.

4.6 Principle of purpose

The practices of processing personal data within the scope of the company are consistent with its nature, its scope and its institutional mission, but, above all, they are carried out in alignment with the legal, contractual and purpose informed to the Holder, in the cases of application of the legal basis "consent".

4.7 Principle of adequacy

The treatment given by Serpro to personal data and the purposes observed are strictly linked to the purpose informed to the Holder or provided for in a contract, agreement, law, regulation or public policy and consistent with the legal basis that authorizes it.

4.8 Principle of necessity

The services, applications and business rules, since their conception, observe minimalist rigor, guided by the collection of only data strictly necessary for the realization of the purposes and the processing itself.

4.9 Principle of Free Access

In accordance with the rules and rights prescribed in Articles 9 and 18 of the GDPL, the Holder is guaranteed free access to its own personal data, through adequate personal identification, so that there is no prejudice to the principle of security.

4.10 Principle of Quality

Data accuracy, correction, updating and integrity is a concern subject to continuous review and improvement and checking practices within the scope of Serpro, without prejudice to the franchised access to the Holder so that it can intervene whenever there are quality failures in the processing.

4.11 Principle of Transparency

Not only advance publications, but also access rights are granted to the Holder and the control bodies, in order to ensure clarity regarding the practices and policies applied to our services. This Statement is also linked to the Serpro Privacy and Data Protection Policy (PPPD).

4.12 Principle of Security

Serpro not only maintains one of the largest and most prepared teams of information security and physical security in constant activity and updating, but also acts in the constant updating and integration of rules and policies, review of procedures and harmonization of the information security management level and the level of Privacy Management with the level of Corporate Governance.

4.13 Principle of Prevention

Serpro's performance is guided by the understanding that its structure, processes and people must be prepared to anticipate problems, with adequate risk management, innovation, respect for the user experience and respect for the quality of its deliveries.

4.14 Principle of Non-discrimination

Under no circumstances can the decisions, configurations, planning and management of Serpro's activities in the processing of personal data imply any type of targeting or discrimination or prejudice to individual rights and freedoms, guaranteeing the effective dignity in the treatment of the individual, the equal opportunities, neutrality in the configuration of managed assets and corporate and commercial decisions.

4.15 Principle of Accountability

In the treatment of personal data and the individual's privacy, Serpro understands that proactive responsibility must guide the conduct of its employees and the decisions of their level of governance, through appropriate processes and the fulfillment of proper planning in line with their PPPD.

5.0 COMPLIANCE AND GOVERNANCE

5.1 Legal compliance

Serpro declares itself

I - In accordance with Law No. 13,709, of August 14, 2018, and committed to maintaining this conformity through the execution of continuous improvement actions;

II - Adhering to the aforementioned principles and committed to maintaining this adherence through the execution of continuous improvement actions.

5.2 Risk governance, compliance and information security

Serpro, in accordance with its Governing Law, the Law on Access to Information (LAI) and the complementary rules issued by the Information and Communications Security Department (DSIC/PR), maintains an adequate Security Program and Information Security Corporate Policy, in addition to the Corporate Policy for Business Continuity, the Corporate Policy for Risk Management, Internal Control and Compliance, and an entire internal normative substrate related to information security and good corporate governance practices, in addition to the PPPD.

Serpro has governance and Information Security management bodies, acting in accordance with contemporary best practice frameworks, such as the NBR ISO, COBIT/ISACA, ITIL and similar models.

5.3 IT Governance, Person in Charge and Contacts

Serpro, under the terms of Law 13,303/2016 (Law of State-owned companies), maintains an instance of Information Technology Governance, responsible for the elaboration and conduction of the IT Strategic Plan (PETI) and the IT Master Plan (PDTI).

Likewise, in terms of IT Governance and Privacy Governance, Serpro declares itself in compliance with contemporary best practice frameworks, such as the NBR ISO, COBIT/ISACA, ITIL and similar models.

The governance of privacy and data protection is the internal instance of support for corporate governance, under the theme “Privacy and Data Protection”, under the coordination of the Person in Charge of privacy and protection of personal data.

6.0 TERM OF USE OF THE SERVICES

Serpro may publish specific rules for each service, subject to the general principles of this Statement and the PPPD, without prejudice to the provisions contained in the contracts entered into.

In the absence of specific rules for a given service or in case of conflict between those specific rules, the contracts, this Statement and the PPPD, the terms of the latter will prevail.



6.1 Responsibility

Serpro is not responsible for malicious practices or for the personal misuse of content on other sites, nor for the malicious exploitation of data security flaws or illegal acts committed by third parties.

Thus, Serpro is committed to offering the best in terms of security to the services that each citizen accesses, acquiring modern and effective assets, applying methodologies notoriously identified as best practices and adopting measures available in the state of the art in favor of information security.

6.2 Collection of information

For various services, Serpro collects data essential to the operation of applications, such as name and CPF (or Corporate Name and CNPJ, in the case of Legal Entities), address, email, telephone numbers, among others. The holder may choose not to provide any of this information. In this situation, the application will warn about the consequences of non-authorization, both in terms of service limitations and denial of access to the application, expressly stating the reasons.

Serpro can also collect and store information about the holder's browsing, such as IP address, pages accessed, length of stay and characteristics of mobile devices. Information from other sources, partner records or other Union bodies can also be added to our database.

6.3 Cookies

Cookies are small files that can be saved on the user's device (computer, tablet or phone) when visiting a website. Serpro can use cookies when it sends small data packets to the user's browser, which are stored on their device. This technology helps us to better understand the behavior of users, including for security and privacy purposes, and inform us of the most visited sections on our sites, contributing to an increasingly better experience in the use of our services.

We use session cookies, temporary, which are deleted when the user leaves our site or persistent cookies, which are not deleted, until the user deletes them or their browser does, depending on the expiration date of the cookie. Persistent cookies have an expiration date written in your code, but their duration may vary.

Most browsers are preset to accept cookies automatically. In the settings, it is possible to change this rule, however, with cookies disabled some features of the site may not work in the most appropriate way.

By clicking "I am aware", in the notice on the use of cookies, the user agrees to our use of cookies. To understand more about the cookies we use, we recommend reading the table below.

<i>Levels of collection</i>	<i>How they are used</i>	<i>Benefits</i>
Strictly necessary cookies	These cookies are necessary for the functioning of the website and cannot be turned off. They are defined when the user requests a service. They do not store any personally identifiable information.	Allow setting cookies and authenticating users.
Performance cookies	These cookies allow us to count visits and traffic sources, so that we can measure and improve the performance of our website. All information that these cookies collect is aggregated and therefore anonymous. If these cookies are not allowed, we will not know that the user has visited our site.	They help to provide a good browsing experience, as they allow us to know the most and least popular pages and how visitors move on the site.
Functional cookies	These cookies allow the website to provide enhanced functionality and customization. They can be defined by us or by third parties, whose services we add to our pages. If these cookies are not allowed, some or all of these services may not work correctly.	They help provide a good browsing experience.
Advertising cookies	These cookies can be set on our website by our advertising partners. They do not store personal information directly, but are based on the unique identification of the user's browser and internet device. If these cookies are not allowed, advertising will be less relevant on third party websites.	Build a profile of users' interests and show relevant ads on other sites.

The option of not using cookies, with the exception of session cookies, for the time being is not presumed in favor of the user. Only after exercising the opt out option, the user will have the option to block cookies. From the month of May 2021, when we have completed the pro-privacy adjustment, the user will be able to previously configure its acceptance for the different types of cookies (opt in mode).



6.5 Use of information

The information collected during browsing allows the customized offer of our services, the study of preferences and, consequently, a browsing experience closer to the interests of each user.

Serpro may also use this information for purposes of communicating with users and customers. In this way, notices and service information developed by Serpro may be sent, which can be inhibited by the user.

The information may also be used in audits, statistical analysis, data science, development and improvement of services provided by the company.

In the event of enabling third-party cookies, the user must inquire with these third parties about the purpose of collection and treatment.

6.6 Sharing information with third parties

Serpro will not pass on the collected information to third parties, partners or in any commercial negotiation. Any and all information regarding Serpro's customers and users will only be passed upon their express approval or by court order.

7.0 PERSON IN CHARGE

To exercise the rights of the holder of personal data, make a request for information on the PDC (Citizen's Digital Privacy) platform. This channel can be accessed at <https://www.serpro.gov.br>, option Privacy and Data Protection.

Other information must be forwarded to the electronic address encarregado@serpro.gov.br.