PERSONAL DATA PROTECTION AND PRIVACY POLICY

Edition
2.0
12/20/2023

Personal Data Protection and Privacy Policy

Area responsible for issuing

Executive Vice Presidency Governance, Risks, *Compliance* and Sustainability / Executive Management Information Security / Information Protection Management

Target audience

Eletrobras employees who carry out activities that involve, directly or indirectly, the processing of personal data.

Approval

Resolution 670/2023, of 12/18/2023, of the Executive Board of Eletrobras.
Deliberation 208/2023, of 12/20/2023, of the Board of Directors of Eletrobras.

Repository

The policies of Eletrobras can be found on the website:
https://eletrobras.com/pt/Paginas/Estatuto-Politicas-e-Manuais.aspx

Copyright and confidentiality

The contents of this document may not be reproduced without permission. All rights belong to Eletrobras.

Maximum review period: 5 years.

Issue history:

Editing	Approval	Main changes
1.0	DEL-247/2019, of 12/17/2019	it does not apply.
2.0	RES-670/2023, of 18/12/2023 and DEL-208/2023, of 12/20/2023	Update of the standard wording and exclusion of mandatory legal references to the federal public administration, due to the change in the legal nature of Eletrobras.

Summary

1 Purpose

Establish guidelines and guidance for the processing of personal data, with the aim of protecting the privacy of consumers, employees, partners or suppliers with a view to managing personal data and managing information security incidents in Eletrobras' conventional or technology environment.

2 References

2.1 Law No. 12,813, of May 16, 2013 – Provides for conflicts of interest in the exercise of a position or employment of the federal Executive Branch and subsequent impediments to the exercise of the position or employment (Conflicts of Interest Law).

2.2 Law No. 12,965, of April 23, 2014 – Establishes principles, guarantees, rights and duties for the use of the *internet* in Brazil (Marco Civil da *Internet*).

2.3 Law No. 13,709, of August 14, 2018 – General Personal Data Protection Law (LGPD).

2.4 Law No. 13,853, of July 8, 2019 – Amends Law No. 13,709/2018, to provide for the protection of personal data and to create the National Data Protection Authority (ANPD).

2.5 Decree No. 8,771, of May 11, 2016 – Regulates Law No. 12,965, of April 23, 2014, to deal with the accepted hypotheses of discrimination of data packages on the internet and traffic degradation, indicate procedures for storage and protection of data by connection and application providers, point out transparency measures in the request of registration data by the public administration and establish parameters for inspection and investigation of infractions.

2.6 Decree No. 9,637 of December 26, 2018 - Institutes the National Information Security Policy, provides for information security governance.

2.7 Eletrobras Corporate Document and Information Management Policy.

2.8 Eletrobras Document Classification Plan.

2.9 Eletrobras Privacy Governance Program.

3 Values

3.1 **Purpose:** carrying out data processing for legitimate, specific, explicit and informed purposes to the holder, without the possibility of subsequent processing in a manner incompatible with these purposes.

3.2 **Adequacy:** compatibility of data processing with the purposes informed to the holder, according to the context of the processing.

3.3 **Necessity**: limitation of processing to the minimum necessary to achieve its purposes, with coverage of data relevant to, proportional to and not excessive in relation to the purposes of data processing stated.

3.4 **Data quality**: guarantee to holders of accuracy, clarity, relevance and updating of data, according to the need and to fulfill the purpose of its processing.

3.5 **Transparency**: guarantee to data subjects of clear, precise and easily accessible information about the processing carried out and their respective processing agents, observing commercial and industrial secrets.

3.6 **Security**: use of technical and administrative measures capable of protecting personal data from unauthorized access and accidental or illicit situations of destruction, loss, alteration, communication or dissemination.

3.7 **Prevention**: adoption of measures to prevent the occurrence of damage due to the processing of personal data.

3.8 **Free access**: guarantee, to holders, easy and free consultation on the form and duration of processing, as well as the completeness of their personal data.

3.9 **Non-discrimination**: impossibility of processing data for unlawful or abusive discriminatory purposes.

4 Guidelines

4.1 Legal basis for data processing

4.1.1 The processing of personal data, that is, the collection, access, deletion, editing, or any other operation, must only be carried out on one of the legal bases set out in the General Personal Data Protection Law (LGPD).

4.1.2 When the processing of personal data is based on the legitimate interest of the controller/operator, it must be accompanied by a Personal Data Protection Impact Report (RIPD).

4.2 Minimal data collection

4.2.1 Processes involving collection of personal data must be adjusted by Eletrobras based on the concept of minimum collection, with specific purposes and obtaining respective consent, when applicable.

4.3 Consent

4.3.1 At the time of collection, the holder of personal data must consent and be informed, clearly and explicitly, about the purpose, the mandatory or optional nature of the provision and the consequences of refusing to provide them. Consent may also be renewed periodically and may be revoked at any time, at the request of the holder.

4.4 Management of contractual instruments

4.4.1 Contracts, agreements and other contractual instruments related to activities involving the processing of personal data must explicitly provide for the responsibility for the correct processing of data by third parties, as well as guarantee the carrying out of due diligence, with provision for the "right to return" from Eletrobras in case of non-compliance by the other party.

4.5 Incident management

4.5.1 Procedures and plans for responding to incidents related to the privacy of data subjects must be developed and kept updated by Eletrobras, based on criteria for controlling and recording leaks, and communicating with those involved and the National Data Protection Authority (ANPD).

4.6 Information Security

4.6.1 Measures against data leakage, as well as investments in security tools and processes, must prioritize the protection of sensitive personal data and data whose processing uses, as a legal basis, the legitimate interest of the controller.

4.7 Data inventory

4.7.1 The personal data inventory at Eletrobras must be kept permanently updated, identifying the document types and the information that contains them, aiming to ensure their

processing (including possible eventual obtaining of consent from the holder) in accordance with the respective legal basis, with the adoption of the concept of minimum collection.

4.7.2 The inventory must be carried out considering the context of production or accumulation of documents and information, structured based on the Eletrobras Document Classification Plan.

4.8 Privacy and personal data governance

4.8.1 The Eletrobras Privacy Governance Program must aim to establish a relationship of trust with holders of personal data, through transparent action, with continuous monitoring and periodic assessments integrated into its general governance structure. It must organize internal processes and policies that ensure comprehensive compliance with standards and good practices regarding the protection of personal data.

4.9 Training and awareness

4.9.1 Educational, training, awareness-raising and awareness-raising actions regarding best practices regarding the processing of personal data at Eletrobras must be promoted on an ongoing basis, as well as broad disclosure of the risks and threats of not using these practices.

4.10 *Web browsing* and *cookies*

4.10.1 Eletrobras may, through mechanisms for obtaining and revoking user consent, use *cookies* and similar technologies that aim to better understand user behavior and contribute to the effectiveness of content distribution, informing which pages and contents of *websites* were visited.

4.11 Information technology systems

4.11.1 Information technology systems supporting processes and activities involving the processing of personal data that are developed or acquired by Eletrobras must follow the concept of *Privacy by Design*. Therefore, its adherence to the LGPD and this policy must be observed since its conception/acquisition.

4.12 Project methodology

4.12.1 Eletrobras' project management methodology must consider the concept of *Privacy by Design*, aiming to avoid the emergence of new processes, activities, systems, practices, projects, products or any other solution that is not adherent to the LGPD.

4.13 Meeting the Demand of the Personal Data Holder (*Data Subject Request – DSR*)

4.13.1 Eletrobras must develop mechanisms to comply with the rights of data holders provided for in the LGPD, with emphasis on confirmation and access to data, rectification, restriction of processing, revocation of consent and deletion of data, always observing the impacts and rights of the controller.

4.13.2 Receiving requests from holders of personal data may also be done through the Ombudsman Channel, thus supporting the Person in Charge of Personal Data Processing (DPO).

5 Responsibilities

5.1 Eletrobras Board of Directors

5.1.1 Approve this policy and deliberate on the strategic guidelines for personal data protection governance.

5.1.2 Delegate to the Eletrobras Executive Board the approval of updates to the Eletrobras Document Classification Plan.

5.2 Eletrobras Executive Board

5.2.1 Approve this policy and the detailed normative documents that allow its implementation.

5.3 Area responsible for information security

5.3.1 Support the Person in Charge for Processing Personal Data (DPO) in their duties.

5.3.2 Coordinate and methodologically support the creation of the personal data inventory, based on information provided by Eletrobras areas.

5.3.3 Develop procedures for handling and responding to incidents relating to the privacy of data subjects.

5.3.4 Promote training and development actions regarding the protection of personal data and privacy, including technical, regulatory and behavioral aspects.

5.4 Data Protection Officer - DPO

5.4.1 Carry out dialogue with data subjects and the National Data Protection Authority (ANPD), including reporting incidents and guiding employees and third parties regarding practices related to the protection of personal data and privacy.

5.5 Area Managers

5.5.1 Ensure the information produced and received by their team due to the area's activities, carrying out and monitoring the data inventory under their responsibility, its appropriate classification and access authorization, as well as the mapping, implementation and operationalization of their controls, enforcing compliance with the guidelines of this policy.

5.6 Staff

5.6.1 Comply with this policy and other instruments that regulate it, using corporate information that contains personal data in a responsible, professional, ethical and legal manner, respecting the rights and privacy of data holders.

6 Concepts

6.1 Anonymization – Use of reasonable technical means available at the time of processing, through which data loses the possibility of association, directly or indirectly, with an individual.

6.2 National Data Protection Authority (ANPD) – Public administration body responsible for ensuring, implementing and monitoring compliance with the General Personal Data Protection Law (LGPD) throughout the national territory.

6.3 Minimum collection – Concept derived from the principle of purpose, which defines that data collection can only be carried out for a specific purpose and this must be informed to the holders in advance; this principle results in minimizing collection, that is, collection is restricted to the data necessary to achieve the specific purpose.

6.4 Controller – Natural or legal person, governed by public or private law, who is responsible for decisions regarding the processing of personal data.

6.5 Cookies – These are data files generated by a website during browsing the *internet*, transferred to the user's computer or other electronic device, registered and recorded by the browser used. These files contain data that serves to identify the user, to personalize the page according to the preferences shown by the user during their visit to the *site*, and even to facilitate navigation between pages within the same website.

6.6 Anonymized data – Data relating to a holder who cannot be identified, considering the use of reasonable technical means available at the time of its processing.

6.7 Personal data – Information related to an identified or identifiable natural person, which identifies or can identify them, such as name, numbers, identification codes, telephone numbers, addresses.

6.8 Sensitive personal data – Data linked to a natural person whose processing may lead to discrimination against its holder, with respect to: racial or ethnic origin; religious conviction; political opinion; membership of a union or organization of a religious, philosophical or political nature; health; sex life; genetics; or biometrics.

6.9 Eletrobras – Holding company, its wholly-owned subsidiaries and companies in which it has direct and indirect corporate control.

6.10 Data Protection Officer (DPO) – Professional appointed to deal with incidents related to breaches of privacy or which cause damage to personal data subjects and to act as a communication channel between the controller, data subjects and the national data protection authority (ANPD).

6.11 Operator – Natural or legal person, governed by public or private law, who processes personal data on behalf of the controller.

6.12 Privacy by Design (*Privacy by Design*) – Methodology in which the protection of personal data is designed from the conception of systems, commercial practices, projects, products or any other solution that involves the handling of personal data.

6.13 Data Processing Registration (RTD) – Form that the controller and operator must maintain with a record of the personal data processing operations they carry out, especially in the case of processing based on legitimate interest.

6.14 Data Protection Impact Assessment **(RPID)** – Documentation from the controller that contains details of all processing processes that personal data undergoes during its life cycle in the operation, as well as the necessary legal bases and security measures adopted in the processing of this data, as well as the measures, safeguards and risk mitigation mechanisms.

6.15 Personal data holder – Natural person to whom the personal data that is subject to processing refers.

6.16 International data transfer – Transfer of personal data to a foreign country or international organization of which the country is a member.

6.17 Processing of personal data – Any operation carried out with personal data, such as those relating to the collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, elimination, evaluation or control of information, modification, communication, transfer, diffusion or extraction.

7 General Provisions

7.1 The legislation related to the topic and the specific legal provisions and agreements in force at the company must be observed.

7.2 In order to meet the specificities of each process, this policy can be broken down into specific normative documents, always aligned with the principles and guidelines established here.

7.3 This policy replaces the Personal Data Protection and Privacy Policy of Eletrobras Companies (POL-33) – edition 1.0, approved by DEL-247/2019, of 12/17/2019.

7.4 The normative documents and provisions contrary to this policy are hereby revoked.