banrisul

Privacidade para você, proteção para seus dados.

Personal Data Protection Guidelines



Personal Data Protection Guidelines

1. Definition

The Brazilian General Data Protection Law (Law 13,709/18, or simply "LGPD") establishes rules on how the Processing Agents must safely and transparently process Personal Data in physical or digital environments. The enactment of Constitutional Amendment 115, in February 2022, recognized the importance of protecting Personal Data in Brazil and includes the fundamental rights and guarantees of the Brazilian Federal Constitution.

The LGPD stipulates that institutions may create policies and rules of good practices and governance that establish organizational conditions, operating systems procedures (including complaints and petitions from Data Holders, security standards, technical standards, specific obligations for the various parties involved in Processing, educational initiatives, internal supervision mechanisms, risk mitigation measures, and other aspects related to the Processing of Personal Data.

To reinforce its institutional commitment to fundamental rights to privacy and Personal Data protection and to ensure compliance with regulations, Banrisul has established the Privacy and Personal Data Protection Governance Program, which addresses not only the legal aspects of the Law but also the governance of Personal Data privacy in its entirety.

Considering that Banrisul – directly or through its representatives, employees, or suppliers – performs numerous Personal Data Processing Operations, it is necessary to strengthen the culture of commitment to data protection to ensure that these operations align with legal requirements and best practices in Personal Data protection.

To ensure and demonstrate this compliance with Personal Data protection, Banrisul presents the **Personal Data Protection Guidelines**, which are part of the Privacy and Personal Data Protection Governance Program, reaffirming its commitment to privacy, security, and the rights of Data Holders.

2. Scope

These Guidelines apply to Banrisul's suppliers, service providers, partners and their respective agents and employees, herein referred to as "Third Party" or "Third Parties", who, within the scope of their contracts, carry out the Processing of Personal Data due to joint activities conducted with the Bank, as Processing Agents.

3. Purpose

The purpose of this Policy is to establish principles, rules, roles, and responsibilities for Personal Data protection, ensuring Banrisul's compliance with the LGPD, with the regulations issued by the National Data Protection Authority (also known as "ANPD") and all other rules applicable to Personal Data protection and privacy.

Through this document, Banrisul declares its commitment to maintaining a balance between its economic interests and the protection of Personal Data belonging to Data Holders – whether clients, partners, or employees.

4. Principles

The core principles of the LGPD are fundamental for adopting good data protection practices and must be observed throughout the entire lifecycle of Personal Data.

Good faith in the Processing of Personal Data is a foundational principle adopted by Banrisul across all its activities, ensuring alignment among the purposes, the nature of the processing, and the information provided to Data Holders. These actions undergo systematic privacy impact and risk assessments, considering aspects such as the purpose and objective of the Processing, the necessity of the data to carry out activities, the adequacy of the amount of Personal Data processed for the intended purpose, the requirement of Consent from Data Holders, and risks of discrimination, among others. At Banrisul, the following key principles must guide all practices related to the Processing of Personal Data:

- **Purpose**: Processing must follow legitimate, specific, explicit purposes, which must be informed to the Data Holder, with no possibility of subsequent Processing in a manner incompatible with the originally informed purpose. Processing must be linked to the objective indicated for its collection and use, ensuring so-called "contextual privacy," preventing its use for other or incompatible purposes.
- **Adequacy**: Processing must occur in a manner compatible with the purposes informed to the Data Holder, in accordance with the context of the Processing carried out in each specific case.
- **Necessity**: Processing must be carried out only with the Personal Data strictly necessary to achieve the intended purposes, that is, avoiding using excessive or irrelevant Personal Data. All Processing of Personal Data must be approached with critical scrutiny.
- **Free Access**: Data Holders must have facilitated and free access to inquiries regarding the form and duration of the Processing of their Personal Data, as well as to the completeness of their Personal Data.

- **Data Quality**: Personal Data maintained by Banrisul must be accurate, clear, and up to date, as well as relevant to the business purpose, necessity, and objective of its Processing.
- **Transparency**: Data Holders must have easy access to clear and accurate information about the Processing of their Personal Data in various Banrisul activities, while respecting trade and industrial secrets.
- **Security**: Banrisul must adopt technical and administrative measures, such as procedures, technologies, and solutions, that ensure greater Personal Data protection and prevent the occurrence of Security Incidents, such as unauthorized access and accidental or unlawful situations that may result in the destruction, loss, alteration, or leakage of Personal Data.
- **Prevention**: Proactive measures must be adopted to anticipate and mitigate risks related to the Processing of Personal Data, seeking to prevent the occurrence of Security Incidents.
- **Non-discrimination**: The Processing of Personal Data must not be carried out with the objective of discriminating against or abusing Data Holders; that is, the Bank prohibits the use of Personal Data, particularly Sensitive Personal Data, such as those regarding racial or ethnic origin, affiliation with a political organization, or health information, to harm, stigmatize, or create unfair distinctions among people.
- **Responsibility and Accountability**: Banrisul must comply with the legislation and demonstrate its compliance through evidence that it has adopted effective measures and procedures to protect Personal Data throughout its entire lifecycle, subject to commercial and industrial secrets.

5. Processing of Personal Data at Banrisul

Any Processing of Personal Data carried out by, or on behalf of, Banrisul must have a legitimate and specific purpose and must be supported by, at least, one of the Legal Basis for Processing provided in the LGPD and no Personal Data should be processed differently than what was informed to the Holder of the Personal Data.

Efforts must be made to ensure that Data Holders are properly informed about the Processing of their respective Personal Data. In the event Personal Data is shared with Third Parties (including those belonging to the same economic group), Banrisul ensures access to information about the sharing, including its respective purpose.

Banrisul's Privacy Policy provides necessary and updated information for Data Holders to gain awareness of the Processing activities it carries out, as well as the channels available for the Holders to exercise their rights provided in the LGPD.

Processing of Data Belonging to Children and Adolescents

The Personal Data of children and adolescents must be processed with maximum caution, having their best interests and protection as a guiding principle, whose application will be assessed on a case-by-case basis, pursuant to applicable legislation.

According to the understanding of the National Data Protection Authority ("ANPD") in Brazil, the Processing of Personal Data belonging to children and adolescents can be based on any of the Legal Basis provided in the LGPD, including cases where Parent or Legal Guardian Consent is applicable. When Processing depends on the Consent of at least one parent or legal guardian, such Consent must be express, specific, and distinct, indicating the purpose to be fulfilled by the Processing. Although Consent represents a possible Legal Basis for the Processing of Personal Data, it is not the only option, as the other Legal Bases under the LGPD are valid and more appropriate in certain situations.

The Processing of Personal Data for the purpose of grouping or profiling children and adolescents for targeted commercial advertising to minors, including any form of emotional analysis, is strictly prohibited.

Any product, service, or system intended to be accessed by children and adolescents, or that is likely to be accessed by this audience, must adopt, by default, the highest privacy and Personal Data protection settings available. Legal guardians must also be provided with clear and easily accessible information regarding any identified risks, the security measures implemented, and the parental supervision tools offered by Banrisul.

Parental supervision tools must allow parents or legal guardians to view, configure, and manage the applicable privacy options.

Banrisul will seek to periodically review the protective measures that have been implemented, considering the nature of the product or service, Processing context, risks involved, and applicable regulations for protecting children and adolescents in the digital environment.

5.2 Processing of Personal Data by Third Parties

Whenever Banrisul signs a contract with a Third Party, such as a supplier or business partner, whose scope requires the Processing of Personal Data on Banrisul's behalf, contractual clauses must be established to define the Personal Data protection responsibilities and obligations of each party, including the duty of secrecy and confidentiality over shared data.

The rules and requirements for contracts and/or relationships involving the sharing of Personal Data shall be included in the clauses of the respective contracts, amendments, and/or declaration terms, observing the peculiarities and nature of

each negotiation relationship and, whenever possible, pseudonymous data and other techniques will be used to guarantee the protection and confidentiality of Personal Data.

Prior to signing any relationship/agreement with Third Parties that requires the Processing of Personal Data, the parties involved must be instructed to gain awareness of Banrisul's Personal Data Protection Guidelines and its Privacy Policy, available on the Bank's website, and to comply with the applicable data protection rules, notably the LGPD and regulations issued by competent authorities.

Contracts signed with suppliers and partners must contain clear and specific clauses to ensure that all parties are aware of their obligations regarding Personal Data protection. Non-compliance with any of the contractual requirements must be documented and liabilities may be created on behalf of the Third Party, within the context of the respective relationship.

5.3 Privacy by default in product and service development

In compliance with LGPD guidelines and industry best practices, all products, services, and systems provided by Banrisul must incorporate security, technical, and administrative measures that are aligned with this Policy and capable of ensuring Personal Data protection from the design phase through execution by adopting the concepts of Privacy by Design and Privacy by Default.

5.4 Safety Measures and Good Practices

Banrisul must adopt security, technical, and administrative measures aiming to protect Personal Data against unauthorized access, accidental or intentional manipulation, loss, and destruction. Personal Data processed at Banrisul will only be transmitted when necessary and through secure connections.

The granting of access to Personal Data processed by Banrisul must be restricted to authorized employees who need to Process such Personal Data to perform their duties, observing the principles provided for in this document.

5.5 Deletion and Retention of Personal Data

The business areas responsible for processing Personal Data must define retention periods in accordance with the Data Retention Policy and establish procedures for data deletion once the purpose of Processing has been achieved. The duration of Personal Data storage shall depend on the purpose and nature of the Processing, in compliance with applicable legislation and regulation.

All processed Personal Data must be retained for the period required to fulfill the purposes for which it was Processed and to comply with any inherent or applicable legal, regulatory, and/or contractual obligations.

5.6 Training and Awareness-Raising

Banrisul must conduct periodic training on Privacy and Data Protection, disseminating current policies and procedures, best market practices, and the responsibilities of all those covered by these Guidelines.

Actions must be implemented to train and raise awareness among all those processing Personal Data on behalf of Banrisul regarding the institution's commitment to Data Holders regarding proper Personal Data protection and the enforcement of their rights.

5.7 Security Incidents

Banrisul has Guidelines for Prevention and Response to Personal Data Incidents that establish processes and responsibilities for handling Security Incidents, particularly those posing significant risk or harm to Data Holders. These Guidelines apply to all Banrisul employees and subsidiaries, who must follow preventive measures and internal procedures in the event of Security Incidents, in addition to complying with internal procedures in the event of an identified or suspected Security Incident.

Security Incidents involving Personal Data will be assessed according to established structures and authorities to determine whether notifications must be submitted to the ANPD and/or Data Holders, as required by the LGPD. The notification must comply with the content, format, and deadlines defined in the ANPD Security Incident Notification Regulation and in Banrisul's internal Guidelines.

Due to their confidential nature, the Guidelines for Prevention and Response to Personal Data Incidents are not public, but general information and cybersecurity guidelines are published on the institution's website in the interest of transparency.

5.8 Rights of the Data Holders

Banrisul provides specific channels for receiving requests regarding the rights of Data Holders, ensuring that responses are delivered within the deadline established by the LGPD and under the required safety and quality, without exposing Third Party data and maintaining industrial secrets. The Data Protection Officer (DPO) will act as the communication channel between the Controller (Banrisul), the Data Holders, and the ANPD, and will carry out the activities assigned to him/her.

5.9 International Transfer of Data

Depending on the product or service offered, the nature of the relationship maintained with the Data Holder, the technologies used, or the activities performed by suppliers, business partners, and Banrisul Group companies, Personal Data may

be transferred to other countries, provided that a valid international transfer mechanism is adopted and an adequate level of Personal Data protection is ensured.

International transfer may occur, among other scenarios, due to the use of technology services, infrastructure, cloud storage, information security, technical support, fraud prevention, data analysis, transaction processing, contract performance, financial transactions, payment services, insurance, foreign exchange, investments, anti-money laundering, fraud combating, compliance with legal or regulatory obligations, or to respond to inquiries from competent authorities, when permitted or required by applicable legislation.

The business areas responsible for operations involving international transfers of Personal Data must ensure said transfers are previously assessed, justified, documented, and carried out in compliance with the LGPD, ANPD regulations, and applicable internal standards, adopting a valid transfer mechanism, such as an adequacy decision or standard contractual clauses, as appropriate. The principles of necessity, purpose, adequacy, security, transparency, prevention, and accountability must also be observed.

Whenever Third Parties are involved in the international transfer of Personal Data, Banrisul must require compatible standards of security, confidentiality, governance, Personal Data protection, and respect of Data Holders' rights. To achieve this, appropriate contractual, technical, and organizational measures must be implemented, as applicable, to protect Personal Data against unauthorized access, loss, alteration, improper disclosure, or any form of inadequate or unlawful Processing.

Data Holders' rights must remain protected regardless of the country where their Personal Data is processed, and the business areas involved are responsible for maintaining evidence of the international transfer's compliance, consulting responsible bodies whenever questions arise regarding applicable mechanism, risks involved, or necessary protective measures.

5.10 Data Protection Impact Assessment (DPIA)

Banrisul will prepare a Data Protection Impact Assessment (DPIA) for Processing operations that may generate elevated risk to Data Holders' rights and freedoms, containing a description of the Processing, all identified risks, and mitigation measures that have been implemented, in accordance with the LGPD and ANPD regulations.

The business areas managing these activities, supported by the Data Protection Officer (DPO), are responsible for identifying the operations that require a DPIA and for keeping it up to date.

6. Privacy and Data Protection Governance Program

Banrisul has established a Privacy and Personal Data Protection Governance Program that covers the policies, procedures, and practices adopted to ensure its adherence to personal data protection and privacy principles, as well as to comply with the regulatory framework, permeating all institutional activities.

7. Review Frequency

The Personal Data Protection Guidelines may be amended whenever Banrisul deems it necessary or to comply with legal or regulatory requirements.

Banrisul is committed to regularly reviewing and updating this Policy to reflect best practices observed in the sector, as well as information obtained from continuous monitoring and periodic evaluations of Personal Data Processing.

Glossary

Processing Agent: the Controller and Operator who carry out the Processing of Personal Data.

National Data Protection Authority or ANPD: a special-status autonomous agency linked to the Ministry of Justice and Public Security, responsible for overseeing, implementing, and enforcing compliance with the LGPD across Brazil.

Banrisul or Bank: Banrisul and subsidiaries of Grupo Banrisul.

Consent: the free, informed, and unquestionable manifestation by which Data Holders agree with the Processing of their Personal Data for a specific purpose.

Controller: a natural or legal person, public or private, responsible for decisions regarding the Processing of Personal Data.

Personal Data: any information relating to an identified or identifiable natural person.

Sensitive Personal Data: information that may reveal aspects of a person's privacy related to racial or ethnic origin, religion, political opinion, membership to unions or religious, philosophical or political organizations, and data concerning the health or sex life, as well as genetic or biometric data of a natural person.

Data Protection Officer: the person indicated by the Controller or Operator who shall act as the communication channel between the Controller, Data Holders, and the National Data Protection Authority (ANPD).

Legal Basis for Processing: conditions set forth in Article 7 (Personal Data) and Article 11 (Sensitive Personal Data) of the LGPD that authorize the Processing of Personal Data.

Security Incident: any confirmed adverse event related to the violation of the confidentiality, integrity, availability, and authenticity properties of Personal Data security.

Valid International Transfer Mechanism: conditions set forth in Article 33, items I - IX, of Law 13,709, of August 14, 2018 (LGPD), that authorize an international transfer of Personal Data.

Operator: a natural or legal person, public or private, responsible for decisions Processing Personal Data on behalf of the Controller.

Personal Data Processing Operation or OTD: a macro–Personal Data Processing activity that is mapped, recorded, and classified under at least one of the legal grounds provided in Article 7 (Personal Data) or 11 (Sensitive Personal Data) of the LGPD by Banrisul.

Privacy by Design: a methodology requiring that any project involving the Processing of Personal Data embeds Personal Data privacy and protection throughout its entire lifecycle.

Privacy by Default: a methodology requiring that the strictest privacy settings be applied automatically, without any action or intervention needed by the user to protect their Personal Data.

Third Party: the Bank's suppliers, service providers, partners and their respective agents and employees, who, within the scope of their contracts, carry out the Processing of Personal Data due to joint activities conducted with the Bank, as Processing Agents.

Data Holder: an individual (natural person) to whom the Personal Data that is the object of Processing refers.

International Data Transfer: the transfer of Personal Data to a foreign country or an international organization of which Brazil is a member.

Processing of Personal Data: any operation carried out with Personal Data, including collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, deletion, evaluation or

control of information, modification, communication, transfer, dissemination or extraction.

Updated in October/2026