PERSONAL DATA PRIVACY POLICY

PERSONAL DATA PRIVACY POLICY

1. OBJECTIVE

To establish the guidelines, strategies and responsibilities in the governance of personal data privacy at Randoncorp to ensure compliance in the processing of personal data.

2. APPLICATION AND SCOPE

This Policy applies to all Randoncorp.

3. REFERENCES

- Randoncorp's Code of Ethical Conduct.
- Compliance Policy.
- Risk Management Policy.
- Information Security Policy.
- Law No. 13.709/2018 (General Data Protection Law).
- Directive 95/46/EC (General Data Protection Regulation).

4. DEFINITION

Company: RANDONCORP S.A.

Consent: formal authorization from the data subject for the processing of their personal data, with awareness of the purpose and the possibility of revocation.

Controller: a natural or legal person, public or private, who is responsible for decisions regarding the processing of personal data.

Data processing: any operation carried out with personal data, such as those related to the collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, elimination, evaluation or control of information, modification, communication, transfer, dissemination or extraction.

Data Protection Officer (DPO): person appointed by the controller to act as the communication channel with data subjects and government authorities, responsible for guiding and supervising personal data protection within the organization.

Data subject: natural person to whom the personal data that are the object of processing relate.

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

Randoncorp: For the purposes of this Policy, it refers to the Company and its controlled and affiliated companies located in Brazil and abroad, including their branches, offices, subsidiaries, and/or any establishment that is, directly or indirectly, linked to it. Additionally, for the exclusive purposes of this Policy, Randoncorp also includes non-economic entities (foundations, associations, institutes, and pension funds) maintained exclusively by any of Randoncorp's BUs.

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

Processing Agents: the controller and the processor.

Processor: a natural or legal person, public or private, who processes personal data on behalf of the controller.

Sensitive Personal Data: personal data on racial or ethnic origin, religious conviction, political opinion, membership of a trade union or organization of a religious, philosophical or political nature, data relating to health or sex life, genetic or biometric data, when linked to a natural person.

5. PRINCIPLES

The principles of personal data privacy governance observe good faith and the continuous improvement of processes in the protection and processing of data. At Randoncorp, the principles are the basis for the processing of personal data and must be applied as follows:

a) Purpose: To carry out the processing of data with legitimate, legal, specific, explicit and informed purposes, and without the possibility of further processing in a way that is incompatible with these established purposes.

b) Adequacy: To process the data in an appropriate, limited and compatible manner with the purposes informed to the holder.

c) Accurate: To limit the processing of data to the minimum necessary for the achievement of its purposes, and not excessive in relation to these purposes.

d) Free access: To facilitate and guarantee that data subjects can be consulted on the form and duration of the processing, as well as on the completeness of their personal data.

e) Data quality: To guarantee the accuracy, clarity, relevance and updating of the data to the data subjects, according to the need and for the fulfillment of the purpose of its processing.

f) Transparency: To ensure that data subjects have clear, accurate and easily accessible information about the performance of the processing.

g) Safety: To use and maintain up-to-date technical and administrative measures to protect personal data, ensuring the security and confidentiality of such data.

h) Prevention: To adopt practices to prevent the occurrence of damage due to the processing of personal data.

i) Respect: To establish procedures to make it impossible to carry out processing for unlawful or abusive discriminatory purposes.

j) Accountability: To demonstrate the adoption of effective measures capable of proving the observance and compliance with the standards of personal data protection and, even, the effectiveness of these measures.

6. GUIDELINES

6.1 PROCESSING OF PERSONAL DATA

Any type of processing of personal data must apply the principles set out in this policy and comply with the provisions contained in current data protection legislation. The requirements for the processing of personal data established in each regulation must be observed according to the place of processing.

The access to the type of processing of personal data must be facilitated so that the data subject has transparent and detailed knowledge of the purpose and duration of the processing, and of the identification of the controller and respective responsibilities. The description of the nature of the personal data processed must consider the data provided by the data subject and the data collected automatically.

6.1.1 Main Hypotheses of Processing of Personal Data

a) **Legal obligation**: for the exclusive fulfillment of a legal or regulatory obligation by the controller, and the purpose (legal framework) must be evidenced.

b) **Contractual obligation**: when necessary for the execution of a contract or preliminary procedures related to a contract to which the data subject is a party, and the contractual relationship must formally exist.

c) **Judicial proceedings**: for the regular exercise of rights in judicial, administrative or arbitration proceedings, and must be in accordance with the terms established in the legislation in force.

d) **Credit protection**: specifically for credit protection in accordance with the provisions of the relevant legislation, and fairness in the processing of this information must be ensured.

e) **Protection of life**: for the protection of life or physical safety of the data subject or third parties, and the need and purpose must be formalized.

f) **Legitimate interest**: when necessary to meet the legitimate interests of the controller and must be explicit and informed to the data subject.

g) **Consent**: upon the formal provision of consent by the data subject with knowledge of the purpose, and the traceability of this act must be maintained. The formal revocation of the data subject's consent should also be facilitated.

The processing of sensitive personal data contains restrictions, and must be strictly protected in every operation carried out with this data. For the processing of sensitive personal data, the possible hypotheses in each local legislation must be observed.

The processing of personal data of children and adolescents must be carried out with the specific consent of at least one of the parents or their legal guardian. This data processing must also be carried out in your best interest and in compliance with the relevant legislation for the full protection of children and adolescents.

All processing of personal data based on legitimate interests and/or consent must be descriptive in a regulation and disclosed to the data subject. The processing of personal data contrary to this policy and current data protection legislation is not permitted.

Contracts signed by Randoncorp companies must contain specific personal data protection clauses, which will establish the duties and obligations of the processing agents involved in the personal data processing operation, respecting the principles, rights of data subject and the regime data protection provisions provided for in relevant legislation.

6.1.2 International Transfer

The international transfer of personal data must comply with the degree of data protection of the recipient country, ensuring adequate compliance with the local data protection legislation of the sending country. The international sharing of personal data between Randoncorp units must be formalized by a personal data transfer agreement.

6.1.3 Sharing of Personal Data between Randoncorp Companies

All Randoncorp companies must sign a Term of Adhesion to the Personal Data Privacy Policy, committing to faithfully apply and comply with all personal data protection activities.

The sharing of personal data between Randoncorp is allowed to fulfill the purpose of data processing informed to the data subject, maintaining the traceability of this act.

6.1.4 Cooperation with Regulators and Inspectors

Randoncorp is committed to fully cooperating with regulatory and supervisory agents, seeking to demonstrate its adherence to the best practices in personal data privacy and to assist in the development of a regulatory environment that respects the privacy of personal data, ensuring that our practices and policies comply with applicable laws and regulations.

6.2 STORAGE AND DELETION OF PERSONAL DATA

The personal data stored at Randoncorp must be protected, in a secure environment, and kept only during the need and purpose of processing and must be eliminated after the end of its processing.

Each department within Randoncorp companies must define and record, in its official documents, the retention periods for personal data under its responsibility, considering applicable legislation, the purposes of processing, and the relevant legal bases. Compliance with these periods must be monitored and periodically reviewed, ensuring that the data is deleted at the end of the established period or when the processing purpose has ceased, as provided in this policy.

The termination of the processing of personal data may occur in the following situations:

a) the purpose has been achieved, or the data is no longer necessary or relevant to the achievement of the specific purpose.
b) end of the statutory processing period.
c) request by the data subject (including the right to revoke consent).

d) determination of the governmental authority, when there is a violation of the provisions of the data protection legislation.

The entire term (duration) of the processing of personal data based on legitimate interests and/or consent must be set out in a regulation. The storage of personal data in violation of this policy and current data protection legislation is not permitted. At the end of the period of processing of personal data, the deletion of data or set of data stored in a database, regardless of the procedure employed, must be carried out.

6.3 RIGHTS OF THE DATA SUBJECTS

Randoncorp ensures that the data subject has the right to exercise any of their rights provided by law, at any time and upon request. They also adopt security measures to protect personal data from unauthorized access and accidental or unlawful situations, maintaining incident management.

The service channels for exercising these rights must be accessible and available in Portuguese, English, and Spanish, taking into account Randoncorp's international operations.

The request pertinent to the processing of personal data must be addressed to the Risk Management and Compliance area responsible for privacy governance.

6.4 DATA PROTECTION

Randoncorp makes every effort to protect data from misuse, interference, loss, unauthorized access, modification or disclosure by adopting security measures in accordance with the guidelines of our Information Security Policy. For data residing in places other than their processing, good information security and data protection practices must be applied, in compliance with local legislation.

7. POLICY VIOLATION

Failure to comply with this Policy or failure to report its violation may result in disciplinary measures for any of those involved in accordance with the Company's policies rules

If you suspect or witness any practice that violates the guidelines of this Policy, please report it through our Ethics Channel. This communication channel guarantees the anonymity of the whistleblower and protection against any form of retaliation, fostering a safe environment for reporting irregularities related to privacy and personal data protection. The Ethics Channel can be accessed in the following link: www.canalconfidencial.com.br/randoncorp.

8. RESPONSIBILITIES

Board of Directors

- To approve the personal data privacy policy.
- To support the acculturation of personal data privacy.

Executive Committee

- To conduct ongoing evaluation of the effectiveness of the data privacy governance model.
- To support the acculturation of personal data privacy.

Privacy and Information Security Committee

- To monitor the mitigation of privacy and information security risks.
- To provide solutions on issues, good practices, and topics to support the privacy and information security governance team.
- To prioritize budgets, initiatives, and investments related to privacy and information security.
- To support the dissemination of a culture of personal data privacy and information security.
- Suggest names for the position of Data Protection Officer (DPO).

Data Protection Officer (DPO)

- To be the point of contact with the owners, regulatory agencies and government authorities.
- To propose the strategy and carry out the overall oversight of privacy governance, serving as the privacy advocate to executives and the primary contact person for the Board of Directors.
- To ensure the support of the Executive Committee for the formalization and execution of initiatives related to personal data privacy.
- To validate all documentation required to comply with the personal data protection.
- To manage budgets related to privacy, initiatives, and investments.

Risk Management and Compliance Area

- Keep the personal data privacy policy up to date.
- To establish personal data privacy governance.
- To disseminate the culture of personal data privacy.
- Assess the effectiveness of the controls adopted to mitigate privacy risks.

9. DOCUMENT CONTROL

This Policy was approved by the Board of Directors on 03/03/2021, and enters into force on this date.

Responsible for the document:

Author	Review	Approval
Risk Management and Compliance	Data Protection Officer	Board of Directors

Version	RCA	Date	Modifications
1ª	921	03/03/2021	03/03/2021
2ª	964	10/11/2022	10/11/2022
3ª	981	14/12/2023	14/12/2023
4ª	999	12/12/2024	12/12/2024
5ª | Versão	1020	11/12/2025	Definitions: inclusion of new definitions – Company, Consent, DPO, International Transfer, Processing Agents, Processor, Randoncorp. Item 6.2: inclusion of the second paragraph. Item 6.3: adjustment of wording in the first paragraph and inclusion of the second. Item 7: improvement of the wording in the second paragraph to reinforce the anonymity of reports to the Ethics Channel. Item 8: adjustment of the wording of the responsibilities of the Privacy and Information Security Committee and the Risk Management and Compliance Area

ID

RANDONCORP