PERSONAL DATA PROTECTION POLICY

I. PURPOSE

Inform the Company's entire personnel on the requirements set forth in the Personal Data Protection Act (Law No. 29733) and the Regulations thereto, and ensure compliance with such requirements.

II. SCOPE

This policy covers all processes involving the provision of the personal data of the personnel, job applicants, clients, potential clients, service providers and third parties of Rimac Seguros y Reaseguros / Rimac S.A., a Health Care Provider, hereinafter referred to as the "Company".

III. DEFINITIONS

- **APDP:** National Personal Data Protection Authority.
- **Consent:** Prior, freely given, express and informed consent of the data subject to process his/her personal data.
- **Privacy Notice:** Verbal or written communication generated by the Personal Data Bank Controller, addressed to the personal data subject, informing on the processing of his/her personal data.
- **Personal Data Bank:** An automated or non-automated organized collection of personal data intended for a particular purpose, regardless of the form of its creation, formation, storage, organization and access; the same personal data may belong to more than one personal data bank.
- **Non-automated Personal Data Bank:** A non-computerized collection of data, structured according to specific criteria, allowing access to personal data without disproportionate efforts.
- **Blocking:** Measure by which the person in charge of the personal data bank prevents access to data by third parties and such data may not be processed during the blocking period.
- **Cancellation:** Action or measure described in the law as "deletion", when referring to personal data, involving the elimination or deletion of the personal data from a data bank.
- **Personal Data:** Any numerical, alphabetical, graphic, photographic, acoustic or any other type of information pertaining to individuals that identifies them or makes them identifiable.
- **Health-related Personal Data:** Information concerning the past, present or predicted physical or mental health of an individual, including the degree of disability and genetic information.
- **Public Data:** Data other than semiprivate, private or sensitive data.
- **Indispensable Data:** Personal data of data subjects that are mandatory to establish or maintain a legal relationship with the Company.
- **Optional Data:** Data required by the Company to offer additional services.
- **Sensitive Data:** Personal data referring to the racial or ethnic origin of a person; income; health-related data; political opinions, religious or philosophical beliefs or moral views; trade-union membership; and data concerning health or sex life, among others.
- **ARCO Rights:** Right of Access, Right of Rectification, Right of Cancellation, and Right of Opposition.
- **Days:** Business days.
- **Personal Data Processor:** Any individual, private-law legal entity or public entity which alone or jointly with others processes personal data upon the request of the personal data bank controller by virtue of a legal relationship with such controller that defines the scope of the processor's activities. It includes a processor that carries out this work without the existence of a personal data bank.

- **Cross-border Transfer of Personal Data:** International transfer of personal data to a recipient in a country other than the country of origin of the personal data, regardless of the support they are in, the means by which the transfer was made, or how they are processed.
- **Habeas Data:** A person's right to know, update and rectify any data collected about him/her in data banks and in files of public and private entities.
- **Anonymization Procedure:** The processing of personal data in such a way that the data subject cannot be identified or is not identifiable. This procedure is irreversible.
- **Dissociation Procedure:** The processing of personal data in such a way that the data subject cannot be identified or is not identifiable. This procedure is reversible.
- **Rectification:** It is the generic action intended to affect or modify a personal data bank, either to update it or to include information in it or specifically to rectify its contents with correct data.
- **Person responsible for the Personal Data Bank:** A person responsible for each personal data bank and for enforcing compliance with the law on the subject.
- **Data Controller:** The person who decides on the processing of personal data.
- **Personal Data Subject:** An individual to whom the personal data relates.
- **Personal Data Bank Controller:** It determines the purpose and content of the personal data bank, the processing of such data and the security measures (the Company).
- **Processing of Personal Data:** Any operation or technical procedure, whether or not by automated means, such as collection, recording, organization, storage, conservation, preparation, alteration, retrieval, consultation, use, blocking, erasure, disclosure by transmission or dissemination or otherwise making available, alignment or combination of personal.
- **Transfer of Personal Data:** Any transmission, supply or communication of national or international personal data to a private-law legal entity, a public entity or an individual other than the personal data subject.

IV. RESPONSIBILITIES

DATA

- Register the personal data banks with the competent national Authority and keep them updated.
- Register the cross-border transfer of data.
- In coordination with the Legal and Information Security Areas, keep updated the Personal Data Protection Policy in line with the strategic objectives of the business, the legislation and the regulations in force, and ensure that it is published and disseminated.
- Define the persons who will be in charge of the Data Banks / Sub-Data Banks managed by the Company.
- Provide information relating to personal data processing to the National Personal Data Protection Authority when required by it, and allow access by it to the personal data banks managed by the Company.
- Validate attention to ARCO rights at the Authority's request.

Information Security

- It acts as the security Representative of the personal data banks. In this regard, it shall have the following responsibilities:
  a) Ensure that the Personal Data Protection Policy is aligned with the strategic objectives of the business, the legislation and the regulations in force.
  b) Coordinate compliance with and implementation of the necessary security controls, in coordination with the Business and Technology areas, defined in this policy.
  c) Periodically review the effectiveness of the security controls adopted for the protection of the personal data banks and take actions for improvement.
  d) Inform the DATA Area on the transfer of data outside the national territory (cross-border transfer), the capture of new personal data as a result of the implementation of IT projects, in order to formalize the changes with the Authority.

Business and Technology Areas

- Implement the security controls defined in this policy in coordination with the risk management and support areas.

Personnel

- Comply with this policy and the procedures derived therefrom.
- Notify any incident that may compromise the privacy of our clients' information or any improper use of the information that may affect our clients or the Company's reputation.

Legal Counsel

- Provide legal advice to the different areas of the Company to answer their inquiries regarding the specifications established in the Personal Data Protection Act and its Regulations.

Person responsible for the Personal Data Bank

- Provide resources and guidance for personal data protection.

Person in charge of the Personal Data Bank

- Inform the DATA Area on any changes (capture of new personal data, elimination and/or modification of personal data already existing, anonymization processes, among others) in the personal data banks, so that the respective updates may be formalized with the competent Authority.
- Ensure compliance with the Company's personal data protection policy.
- Authorize the transfer of the personal data information contained in the data banks to third parties.
- Ensure that the transfer of personal data information is contractually formalized at the time it is made.
- Respond to the inquiries made by a person requesting ARCO rights in respect of the data bank / sub-data bank under his/her responsibility.

V. POLICY DEVELOPMENT

ADMINISTRATIVE ORGANIZATION

1. The Company must define the persons responsible for and in charge of each personal data bank / sub-data bank, who shall be directly responsible for and shall ensure compliance with this policy.
2. The Data Bank Controller is the Company as a legal entity.
3. The representative of the Data Bank is the Vice President of Personal Insurance and Marketing for Rimac Seguros y Reaseguros, and the Vice President of Human Resources for RIMAC S.A., a health care provider.

MANAGEMENT AND PROCESSING OF PERSONAL DATA BANKS

4. The creation, updating or deletion of the data banks must consider:
   a) The implementation of procedures for the creation, updating, elimination and transfer of personal data banks.
   b) The creation of personal data banks requires the previous implementation of the security controls necessary to comply with this policy and with Law No. 29733 and its supplementary provisions.
   c) The creation and modification of data banks and/or the personal data capture mechanisms must be previously approved by the DATA Area.

5. The following must be considered in obtaining personal data and the consent of the personal data subject:
   a) The Company prohibits the collection of personal data through fraudulent, disloyal or unlawful means.
   b) Before processing any personal data, the person in charge of each data bank must ensure that the consent of the personal data subject has been obtained.
   c) Before capturing any personal data, the informed, unambiguous and express consent of the data subject must be obtained.
   d) Such consent may be obtained orally in the case of personal data; however, it must be obtained in writing in the case of sensitive data.
   e) Personal data shall be collected if this is necessary and lawful in connection with the purposes determined. Furthermore, the quality of the data contained in the personal data bank must be guaranteed and the security measures necessary to prevent the tampering, loss and diversion of personal data must be implemented.
   f) For the processing of personal data of minor children, the consent of their parents or guardians, as the case may be, shall be required, with the exceptions established by the Act and its Regulations. In the case of persons older than 14, the express consent of their parents or guardians shall not be required if data approved by the law are to be processed.
   g) No consent shall be required if the personal data:
      - are collected for the performance of functions inherent in the Company, within the respective area of competence, either contractual, pre-contractual, labor, negotiation and professional, when the data are available from public sources or in the exceptional cases contemplated by Law No. 29733 and its supplementary provisions.
      - will be the subject of dissociation or anonymization procedures.
   h) If personal data are obtained without the prior consent of the data subject and no exception applies for requesting them, measures must be implemented to obtain the consent for their processing. Moreover, the first contact with the client may be established only if the consent to contact him/her is previously obtained.

6. The transfer of Personal Data must consider the following:
   a) The persons in charge of each data bank / sub-data bank shall ensure that the data subject has given his/her consent for any transfer of personal data, with the exceptions established by the Act and its Regulations.
   b) Any transfer of personal data, both at the national and international level, shall be made with the authorization of the person in charge of the personal data bank / sub-data bank and the means used to make such data transfer shall comply with the security information policy in force. If it is necessary to make a cross-border transfer of personal data, the persons responsible for each data bank and for Information Security shall ensure that the recipient country offers adequate protection levels in accordance with the applicable law.
   c) If a cross-border transfer is made, this must be notified to the DATA Area for registration.

7. The hiring of third parties for personal data processing must consider the following:
   a) Any third party with which the Company shares personal data information shall, as part of the service currently provided, comply with all the provisions set forth in the Personal Data Protection Act and its Regulations, which shall be formalized through a contract to be executed by both parties.
   b) Each area is responsible for regularizing the current contracts with third parties through the inclusion of the necessary addenda setting forth the terms required by law. If applicable, upon request, the Company's legal counsel shall advise the persons responsible for the respective areas on the terms dealt with and defined in the contract.

EXERCISE OF THE DATA SUBJECT'S RIGHTS

8. Personal data must be stored in a way that enables the data subject to exercise his/her rights.

9. Mechanisms must be implemented to enable the data subject or the representatives of minor children to submit requests in respect of the following:

   Right of information:

   - The purpose for which their data will be processed.
   - The parties who are or can be the recipients.
   - The identity and address of the personal data bank controller.
   - The transfer of the personal data.
   - The consequences of providing their personal data and of refusing to provide them.
   - The time during which the data will be preserved.

   Right of Access:

   - Obtain, free of charge, the information about them that is being processed in data banks.
   - The manner in which their data were collected.
   - Reasons for collection.
   - The party who requested the collection.
   - The transfers made or expected to be made.

   Right of Rectification, Cancellation and Opposition:

   - When any omission, mistake or false information has been detected.
   - When they are no longer necessary or appropriate for the purpose for which they were collected. When the term established for their processing has expired.
   - The Company reserves the right to keep the information to comply with special rules on money laundering prevention.
   - Any request for rectification must be accompanied by the pertinent supporting documentation.

10. For response procedures, regardless of the means (physical or electronic), evidence of the inquiry made and the answer given must be kept. The claims filed in respect of personal data processing must be informed to the Information Security Unit to coordinate the corrective action plans.
11. The response to requests and claims filed by personal data subjects must consider the following terms:

Request	Response Time
Information	08 days from the day following the submission of the request.
Access	20 days from the day following the submission of the request.
Rectification, Cancellation, Opposition	10 days from the day following the submission of the request.

Rights Protection (APDP)	15 days after the request from APDP (Personal Data Protection Authority) is notified

PERSONNEL'S DUTIES

12. Unacceptable use of information relating to personal data.

    The following activities are prohibited and are considered an unacceptable use of the information relating to personal data. This list attempts to provide a framework for the activities representing an unacceptable use and is merely illustrative:

    a) Use or process the information for its own or third-party benefit and without the authorization of the data subject.
    b) Use personal data information to carry out activities that are contrary to the applicable laws.
    c) Share personal data information with other workers and/or third parties, either directly or indirectly, without the prior consent of the persons in charge of the data banks / sub-data banks and without observing the policies established herein.
    d) Give confidential information to third parties, either directly or indirectly, without the consent of the Company.
    e) Collect personal data by using fraud, deceits, and means not permitted by the Peruvian laws.

13. Duty of Secrecy and Confidentiality.

    All the workers and/or third parties who are involved in any stage of the personal data processing are required to maintain the confidentiality and professional secrecy, when applicable, for an indefinite period of time.

DATA BANK SECURITY

14. Data Bank Information Security Management
    a) The personal data collected by the Company shall be considered **CONFIDENTIAL INFORMATION.**
    b) Personal data protection must be incorporated into the Information Security Policy in order to ensure observance of the control measures required to comply with the applicable regulations.

15. Technical Security Measures in the Use of Information and Communication Technologies (TIC)
    a) The security controls required by Law No. 29733 (Complex Type) and defined in the Company's Information Security Policy must be implemented in the use of Information Technologies such as Data Banks, Business Applications, Communication Equipment, Servers, Operating Systems, among others, which support the management of the personal data processing activities.

16. Physical Security Measures for Personal Data Protection
    a) As regards the storage of physical data banks containing sensitive data, the information must be stored in an isolated room protected by lock or a similar mechanism, where the responsibility for the access system lies with the User Area.

    b) As regards the storage of physical data banks with non-sensitive data, the personal data bank must be stored in a cabinet, box, drawer, locker or similar device that is

protected by lock or a similar mechanism, the responsibility for which lies with the User Area.

TRAINING AND MONITORING IN PERSONAL DATA PROTECTION

17. Incident Management.
    a) The management of incidents compromising personal data must be included in the Company's information security incident response management procedure.

18. Audit
    A compliance audit program must be developed to ensure the mitigation of risks related to personal data protection. This activity must be conducted at least once a year.

19. Training and Commitment
    a) The personal data protection awareness and training program must be included in the Company's Information Security awareness program.

GENERAL

20. Policy Update.
    a) The Information Security Unit is responsible for ensuring that the policy is kept updated and is appropriate to the Company's needs. The policy shall be reviewed, updated or ratified every two (2) years or when significant changes are introduced in the internal processes or the external regulations.
    b) Each policy update shall be accompanied by the respective notice and training of the persons responsible for complying and becoming acquainted with it.
21. Exceptions and Sanctions. The following must be considered:
    a) Any exception to compliance with this policy must be notified to the Information Security Unit for registration and evaluation.
    b) Failure to comply with this document shall be considered a serious fault and shall be sanctioned accordingly as established in the internal work regulations.
    c) Failure to comply with this document shall be sanctioned as provided for in the internal work regulations.

VI. RELATED DOCUMENTS

CODE	NAME
POL-091	Information Security Policy
Regulatory Framework	Personal Data Protection Act No. 29733
Regulatory Framework	Regulations to the Personal Data Protection Act No. 29733
Regulatory Framework	Information Security Directive of the Personal Data Protection Act No. 29733
Regulations to Legislative Decree No. 1353	Legislative Decree that creates the National Authority for Transparency and Access to Public Information: It strengthens the Personal Data Protection System and the regulation of interest management.