DATA PROTECTION AND PRIVACY POLICY

RNA – Rede Nacional de Assistência, S.A
☎ (+351) 210 443 600 | Alameda Fernão Lopes, 16, 6º, Miraflores, 1495-190, Algés
Taxpayer Number: 509 113 010 | Registered at the Lisbon C.R.C under the same number
Share Capital 1.200.000.00€

INDEX

PURPOSE

RNA has always been guided by full transparency and complete respect for the privacy, confidentiality, and protection of the personal data it processes in the course of its activities, and therefore now reinforces its position on this matter. Accordingly, RNA has adopted a set of measures aimed at ensuring the protection of and compliance with applicable personal data protection legislation.

This Privacy and Personal Data Protection Policy, hereinafter referred to as the "Policy", applies to the processing of personal data of its clients and other data subjects with whom RNA maintains relationships in the course of its activities.

In order to comply with the current applicable legal framework, namely the General Data Protection Regulation (GDPR) and Law No. 58/2019 of 8 August, which ensures the implementation of the GDPR within the Portuguese legal system, RNA has developed and implemented a Personal Data Protection System aimed at ensuring regulatory compliance and enabling it to demonstrate and evidence such compliance, in accordance with the principle of accountability.

Through this Policy, RNA defines, describes, and discloses how it uses personal data subject to processing operations, namely regarding the categories of data, how and why they are used, to whom they may be transferred, and the measures adopted to protect their integrity, availability, and confidentiality.

By using any of our platforms or by completing any of our forms, you must read and accept these conditions.

RELEVANT DEFINITIONS

- **Personal Data:** any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier. Personal identifiers include, for example, a name, an identification number, location data, online identifiers, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person;

- **Processing:** any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction;

- **Pseudonymisation:** the processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

- **Controller:** the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its designation may be provided for by Union or Member State law;

- **Processor:** a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller;

- **Recipient:** a natural or legal person, public authority, agency, or another body to which personal data are disclosed, whether a third party or not. However, public authorities that may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall comply with the applicable data protection rules according to the purposes of the processing;

- **Consent:** any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, or their legal representative, signify agreement to the processing of personal data relating to them, by a statement or by a clear affirmative action;

- **Personal Data Breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed;

- **Sensitive Data:** personal data requiring heightened protection due to the risk of discrimination. This includes racial or ethnic origin, religious beliefs, political opinions, trade union membership, health data, sex life, and genetic or biometric data. Processing is restricted and requires explicit consent or specific legal grounds;

- **Biometric Data:** personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a natural person, which allow or confirm the unique identification of that person, such as facial images or fingerprint data;

- **Health Data:** personal data related to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about their health status.

LEGAL PRINCIPLES

All data processing operations comply with the fundamental legal principles in the field of data protection and privacy, namely:

- **Principle of Lawfulness**: Personal data shall be processed where one of the following legal bases applies: the data subject has given consent; processing is necessary for the performance of a contract; compliance with a legal obligation; protection of the vital interests of the data subject; reasons of public interest; or legitimate interests pursued by the Controller;

- **Principle of Transparency**: The circumstances relating to the processing of personal data shall be communicated to the respective data subjects in a clear manner and expressed in plain language;

- **Principle of Purpose Limitation**: Personal data shall be processed solely for specified, explicit, and legitimate purposes and shall not be further processed in a manner incompatible with those purposes;

- **Principle of Proportionality**: RNA Seguros shall only process personal data that are adequate, relevant, and limited to what is necessary for the purposes for which they are processed;

- **Principle of Integrity and Confidentiality**: Personal data shall be processed in a manner that ensures appropriate security and confidentiality, and shall be duly protected against unauthorised access and use;

- **Principle of Storage Limitation**: Personal data shall be kept in a form which permits identification of data subjects only for as long as necessary for the purposes for which the data are processed.

DATA CONTROLLER / PROCESSOR

RNA acts as a Controller in cases where it determines the purposes and means of processing, namely with regard to the management of its platforms, forms, and applications, as well as in relation to its employees.

RNA – Rede Nacional de Assistência, a legal entity with tax identification number (NIF) 509 113 010, with registered office at Alameda Fernão Lopes, no. 16 – 6th floor, Miraflores, 1495-190 Algés, contact: geral@rna.com.pt.

On the other hand, RNA also acts as a Processor: with regard to the provision of assistance services to persons and property, claims management, and other services within the scope of its activity, RNA acts at all times as a Processor on behalf of the Insurer or other Client Entity, which determines the purposes and means of processing, in accordance with the General Data Protection Regulation. In such cases, the Privacy and Personal Data Policy of the relevant Controller Entity should be consulted.

CATEGORIES OF PERSONAL DATA

In the course of its activities, RNA carries out personal data processing operations that are necessary for the provision of its products and services, namely when a policy is taken out, when its platforms are used, when documentation required for claims handling is submitted, or when contact is made with RNA.

The categories of personal data processed by RNA may include the following:

- Name;
- Address;

- Date of birth;
- Relationship with the insured, policyholder, or beneficiary;
- Tax identification number (NIF);
- Mobile contact;
- Email address;
- Policy details;
- Vehicle registration number;
- Health data, such as: current medical conditions, diagnostic test results, medical reports, hospitalisation reports, discharge notes, certificates of incapacity, information on previous clinical conditions, medical history, information on regular medication, and relevant lifestyle information;
- Bank details;
- Academic qualifications;
- Biometric data;
- Images captured through video surveillance systems;
- Information regarding the use of our platforms — namely: information on visits to our platforms, data collected through cookies and other tracking technologies (such as IP address or domain), browser version, location data, and web logs.

With regard to data that may fall within the scope of special categories of data, RNA shall only carry out processing operations upon the explicit consent of the data subject, given in writing or through a clear affirmative act, except where processing is necessary for compliance with a legal obligation, the protection of the vital interests of the data subject, or for reasons of substantial public interest.

PURPOSES OF PROCESSING AND LEGAL BASIS

The personal data processed by RNA Seguros are intended to pursue the purposes described below and are based on the legal grounds indicated for each purpose:

Purpose	Legal Basis	Retention Period
Contract management, including pre-contractual measures	Pre-contractual measures and performance of a contract; consent of the data subject; compliance with a legal obligation.	Statutory limitation period after termination of the insurance contract
Claims management		Statutory limitation period

	Performance of a contract; protection of vital interests; substantial public interest; consent of the data subject; compliance with a legal obligation	
Marketing	Consent of the data subject	Until withdrawal of consente
Human resources management, including recruitment, payroll processing, professional training, disciplinary procedures, occupational health; working time and attendance control; monitoring of electronic communications, internet access and telephone calls; voice recording	Pre-contractual measures and performance of a contract; compliance with a legal obligation	Statutory limitation period
Compliance with legal obligations, including disclosure to authorities, supervisory and regulatory bodies, and Courts	Compliance with a legal obligation; legitimate interests, including fraud prevention and detection and the exercise of rights of defence in legal proceedings	Statutory limitation period or the period applicable to each specific obligation

RECIPIENTS

In the course of its activities, RNA Seguros may disclose the personal data it processes, namely to the following entities:

- Service providers of various types;
- Business partners;
- Supervisory, regulatory, judicial or law enforcement authorities, namely ASF, ATA, ACT, AdC, Courts, and police authorities;
- Sectoral organisations, namely APS.

RNA Seguros ensures that all its suppliers are contractually bound to implement appropriate technical and organisational measures to ensure the security and confidentiality of the data transmitted to them by RNA Seguros.

INTERNATIONAL TRANSFERS

The data collected and/or processed by RNA may, in the course of its activities, be transferred to Processors located outside the European Union.

In such cases, RNA seeks to ensure contractually that all international Processors adopt appropriate technical and organisational measures to guarantee the security and confidentiality of the data transmitted by RNA, in compliance with applicable Data Protection legislation.

DATA SUBJECT RIGHTS

Data subjects may exercise, at any time, the following rights:

- **Access** the right to access the personal data processed and to be informed of the conditions under which such processing is carried out, and to request access to such data;

- **Rectification** the right to obtain from the Controller, without undue delay, the rectification of inaccurate personal data concerning them;

- **Erasure** the right to obtain from the Controller the erasure of personal data where: the data are no longer necessary for the purposes for which they were collected; consent is withdrawn and there is no other legal basis for processing; the data subject objects to the processing and there are no overriding legitimate grounds; the data have been unlawfully processed; or erasure is required to comply with a legal obligation to which the Controller is subject;

- **Restriction of Processing** the right to obtain restriction of processing where: the accuracy of the personal data is contested; the processing is unlawful and the data subject opposes erasure; the data are no longer necessary for the purposes of processing but are required by the data subject for the establishment, exercise or defence of legal claims;

- **Data Portability** the right to receive personal data concerning them in a structured format and, where technically feasible, to request the direct transmission of those data to another controller;

- **Objection** the right to object, at any time and under certain conditions, to the processing of their personal data;

- **Automated Decision-Making** the right not to be subject to decisions based solely on automated processing, including profiling, except under certain conditions and based on specific legal grounds.

DATA PROTECTION OFFICER

RNA has appointed a Data Protection Officer (DPO) to address requests relating to the exercise of data subject rights.

The DPO may be contacted at the following email address:

encarregado.protecao.dados@rna.com.pt

The Data Protection Officer is responsible for:

- Informing, training, raising awareness, and promoting understanding across the organisation regarding the principles governing the processing of personal data and the obligations arising from the applicable legal framework, including the General Data Protection Regulation and all relevant Union and Member State provisions;
- Monitoring compliance with the applicable legal framework;
- Providing advice regarding Data Protection Impact Assessments;
- Cooperating with supervisory authorities;
- Developing procedures and policies to ensure the implementation of all necessary measures for compliance with the applicable legal framework.

RNA ensures that the DPO is appointed based on their professional qualities, in particular their expertise in law and data protection practices, and that they perform their duties with complete independence and impartiality.

RNA further ensures that the DPO is provided with the necessary resources to perform their duties effectively.

The DPO is also supported by other departments that contribute to ensuring compliance with the applicable legal framework, namely:

- **IT and Systems Department / Information Security Officer** – responsible for risk assessments, continuous monitoring of information security measures, reporting incidents that may constitute personal data breaches, implementing technical and organisational measures to ensure compliance with the GDPR, and executing measures required to respond to data subject rights requests;

- **Departments involved in project implementation**, namely Commercial, Marketing, Organisation, Networks, and Quality – responsible for assessing the impact of new business activities on data subject rights, disseminating information to business partners, ensuring compliance with regulated contracting procedures, and informing the DPO of processing operations arising from new business activities.

RIGHT TO LODGE A COMPLAINT

Data subjects have the right to lodge a complaint regarding the processing of their personal data with the following entities:

- Data Protection Officer: encarregado.protecao.dados@rna.com.pt
- Comissão Nacional de Proteção de Dados (CNPD): www.cnpd.pt

SECURITY MEASURES

Both RNA and its Processors are committed to the protection of personal data and have implemented various security measures in order to protect personal data against disclosure, loss, misuse, alteration, unauthorised processing or access, as well as against any other form of unlawful processing.

Employees who, in the course of their duties, process personal data are subject to professional secrecy obligations, including after the termination of their functions, and are bound to comply with the provisions of this Policy, as well as with the applicable personal data protection legislation.

INCIDENT NOTIFICATION

A personal data breach (data breach) is a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

In accordance with Article 33(1) of the General Data Protection Regulation, the Controller is required to notify the CNPD of a personal data breach. Therefore, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons, such notification must be made within 72 hours after becoming aware of it.

REVIEW AND UPDATE

This Policy shall be reviewed by the Legal and Compliance Department whenever there are legislative changes, changes to processing operations, the implementation of new technologies, or the emergence of high risks. The most up-to-date version shall be made available on the website.

VERSION CONTROL

Version:	Prepared by:	Approved by:	Effective date:	Notes:
1	Compliance Department	Board of Directors	22 November 2019	Initial version
2	Compliance Department	Board of Directors	12 February 2026	Version 2.0