Privacy and Data Protection Commitment

This Privacy and Personal Data Protection Commitment (hereinafter referred to as the 'Commitment') reflects the dedication of the Fidelidade Group (hereinafter referred to as the 'Group') to the protection of Personal Data.

The principles of this Commitment apply to all Fidelidade Group companies, apart from companies that are part of the Luz Saúde Group and must be observed both when sharing or transferring Personal Data between Group companies and when involving external stakeholders.

Fidelidade Group companies in other geographical areas incorporate the principles of this Commitment, with the adaptations required by the legal and regulatory provisions applicable in each of them.

I. PRINCIPLES OF PERSONAL DATA PROTECTION IN THE GROUP

Lawfulness, Fairness, and Transparency: we process Personal Data on an appropriate legal basis nd data subjects are provided with clear, accessible, and comprehensive information regarding such processing.

Purpose Limitation: Personal Data collected and processed solely for specified, explicit, and legitimate purposes, as previously communicated to the data subjects.

Minimization of Personal Data: we only collect Personal Data that is strictly necessary, adequate and relevant in relation to the purposes.

Accuracy: reasonable steps are taken to ensure that Personal Data is accurate and, where necessary, kept up to date, including through the update mechanisms made available within the Group.

Storage Limitation: Personal Data is retained only for as long as is necessary for the purposes for which it was collected and in accordance with the Group's internal rules and legal deadlines.

Integrity and Confidentiality: Appropriate technical and organizational measures are implemented to ensure the security of Personal Data, protecting it against unauthorized or unlawful processing, accidental loss, destruction, or damage.

Accountability: the Group maintains documentation on how, where, and for what purpose personal data is processed, ensuring its evidence is before the supervisory authorities.

II. GOVERNANCE AND RESPONSIBILITIES

Where required by law, Group companies have appointed a Data Protection Officer (DPO). The DPO acts independently and is supported in the performance of their duties by dedicated teams with expertise in Cybersecurity and Compliance.

The Group has also designated representatives within the various business areas of its companies, who act as points of contact for the Data Protection Officer and as promoters of a culture of data protection. All Group employees contribute to this commitment by adhering to best practices in the processing of Personal Data and by complying with their duty of professional secrecy.

III. MAIN CATEGORIES OF DATA WE PROCESS

Personal Data is all information relating to an identified or identifiable natural person (the "Data Subject").

The main categories of Personal Data processed by the Group are as follows:

Categories of Personal Data	Examples (not exhaustive)
Identification and contact details	Name, identification document number, tax identification number, photograph, signature, address, telephone number, and email address
Personal data relating to the insurance policy and to the claim	Policy number, coverage and insured amounts, dates and locations of claims, photographs, videos, or other means of proof
Health details	Data contained in the Individual Health Questionnaire, degree of disability or invalidity, lifestyle, data resulting from medical examinations in the context of claims settlement
Risk information	Risk profile, claims history, financial situation, household
Behavioral information	Information relating to connection data (IP address, cookies, logs) collected in the context of the Customer's web/mobile browsing on the Group's websites/mobile sites/apps

IV. SHARING OF PERSONAL DATA

Internal: The Group has established information security rules and implemented appropriate controls. Access to Personal Data is strictly limited to authorised employees and only to the extent necessary for the performance of their professional duties.

International Data Transfers: we use mechanisms to ensure the lawfulness and security of international transfers, such as: Standard Contractual Clauses; Supplementary measures of a technical and organizational nature, such as encryption or pseudonymization; Risk analysis and maintenance of transfer records, assessing the suitability of the destination country on a case-by-case basis.

External: we enter into Agreements with service providers, partners, or reinsurers that ensure the implementation of appropriate technical and organizational measures. Whenever we use subcontractors, we issue clear instructions for the processing of Personal Data and ensure adequate safeguards, in accordance with the Group's Statements, values, and Environmental, Social, and Governance (ESG) principles.

Authorities and Legal Obligations: Personal Data may be disclosed to supervisory, regulatory, tax, judicial, or other competent administrative authorities, whenever such disclosure is necessary to comply with applicable legal or regulatory obligations.

V. ETHICS AND DIGITAL RESPONSIBILITY

The Fidelidade Group is governed by the ethical use of Personal Data, ensuring the responsible use of emerging technologies, such as Artificial Intelligence (AI). We conduct privacy and ethics impact assessments, with a human-centered approach based on principles of transparency, fairness, non-discrimination, and human control. All employees involved in the development or use of AI solutions receive specific training on responsible practices.

VI. COMPLIANCE AND CONTINUOUS IMPROVEMENT

We ensure compliance with legislation and best practices through:

- Training and awareness raising;
- Impact assessments and records of processing activities;
- Data Protection by Design and by Default;
- Implementation of a process for detecting and responding to Personal Data breaches.

VII. TIPS TO STRENGTHEN YOUR PROTECTION

Read the Data Protection Information carefully;

Minimize the personal information you share;

Check and adjust your choices (such as accepting or refusing communications - opt-in/opt-out);

Be aware of phishing attempts (fraudulent messages to obtain sensitive information). Carefully check the sender's email address and analyze the content of the message, identifying spelling errors or suspicious links.

Stay informed about privacy news and developments to better understand your rights.

VIII. AMENDMENTS TO THE DECLARATION

Version	Date	Changes made	Author
1.0	24/09/2025	Initial version of the document	*Isabel Lage, Fidelidade Group General Counsel*