1. PURPOSE

SIMPAR S.A. (“Company” or “SIMPAR Group”) recognizes the importance of the privacy of our employees, clients, suppliers, partners and other people with whom we interact and is therefore committed to this issue.

The purpose of this Policy is to establish standards in compliance with Federal Law No. 13709/2018 (“General Personal Data Protection Law” or “LGPD”) in relation to all personal data processed by the Company, as well as other laws that refer to the subject of data protection, provided that they are applicable to the business of the group's companies.

Therefore, this policy describes the rules applicable to the processing of personal data, and establishes the pillars for the construction of the Privacy and Personal Data Protection Program (“Program”).

2. FIELD OF APPLICATION

This policy applies to SIMPAR S.A. and all the companies it controls (“Company” or “SIMPAR Group”). It also applies to third parties who have a relationship with the Company and its businesses.

3. REFERENCE DOCUMENTS

- SIMPAR Code of Conduct;
- Anti-Corruption Policies;
- Risk Management Policy;
- Personal Data Handling Policy;
- Information Security Policy;
- Privacy by Design Procedure;
- Personal Data Incident Response Procedure;
- Policy for the Use and Management of Consent; and
- Policy for Sharing Data with Third Parties.

4. DEFINITIONS

For the purposes of this Policy, the following definitions apply:

Anonymization: process by which data relating to the Data Subject cannot be identified, taking into account the use of reasonable technical means available at the time of its processing.

Privacy Notice: document through which the main information relating to the Processing of Data Subjects' Personal Data is provided, which may be External (aimed at clients and the general public) or Internal (aimed at employees).

National Data Protection Authority (“ANPD”): is the public administration agency responsible for regulating, supervising and applying administrative penalties related to Personal Data Protection.

Senior Management: see responsibilities described under "Management and Governance", represented in the person of the Chief Executive Officer and/or Chief Financial Officer of each company.

Legal Basis: term that refers to the legal hypotheses that authorize the Processing of Personal Data and Sensitive Personal Data set out in articles 7 and 11 of the LGPD, respectively.

Personal data: any information relating to an identified or identifiable individual. An identifiable individual is one who can be directly or indirectly identified, in particular by reference to an identifier such as a name, an identification number, location data, electronic identifiers, or to one or more factors specific to that person's physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Sensitive Personal Data: Sensitive Personal Data is information that may represent a high risk to the security and/or freedoms of the Data Subject or that may give rise to unlawful discrimination when processed. Sensitive personal data includes any personal data relating to racial or ethnic origin, religious conviction, political opinion, membership of a trade union or religious, philosophical or political organization, as well as data relating to health or sex life, genetic or biometric data.

System authentication data: any personal data used as a credential to determine access to a system or to confirm the identification of a user, such as login accounts, tokens and passwords.

Teenagers' data: involves data from data subjects aged 12 or over and under 18.

Children's data: involves data from data subjects up to twelve (12) years of age.

Elderly data: involves data from data subjects aged 60 or over.

Data protected by legal, judicial or professional secrecy: personal data whose secrecy derives from a legal rule or court decision, or whose secrecy derives from the exercise of a role, ministry, office or profession, and whose disclosure may cause damage to third parties.

Person in Charge of Personal Data Processing ("Data Controller"): a person or organization formally appointed by the Company to be responsible for the management of the Privacy Program, to act as a communication channel between the Controller, the Data Subjects and the National Data Protection Authority (ANPD), among the performance of other activities specific to the role.

Non-Compliance with the Privacy Program: any failure to comply with the points described in this Policy, which may give rise to risks of damage to Data Subjects and/or risks to the Company.

LGPD: General Data Protection Law - Federal Law No. 13709/2018.

Controller: individual or legal entity governed by public or private law, who is responsible for decisions regarding the Processing of Personal Data, such as the form and duration of said Processing. The Company will be the Controller when it takes decisions on the Processing of Personal Personal Data, as is the case, for example, with the Personal Data of all SIMPAR Group employees.

Operator: individual or legal entity governed by public or private law, who carries out the Processing of Personal Data on behalf of the Controller.

Privacy by Design: approach used in the development of a system or project to include privacy and Personal Data protection issues from the outset.

Privacy Program or Program: set of rules, internal guidelines and governance bodies/structures aimed at establishing internal parameters for handling personal data, mitigating risks and ensuring the Company's compliance with data protection laws and best practices on the matter.

Pseudonymization: is the Processing by which Personal Data loses the possibility of direct or indirect association with an individual, if not for the use of additional information, kept separately, in a controlled and secure environment.

Project: developing or making significant changes to products or services provided by the Company.

Criticality Assessment Questionnaire (QAC): document that seeks to identify information related to Personal Data Processing operations in the Project, in order to allow the assessment and classification of the level of criticality.

Balancing Test Questionnaire: document that seeks to identify information related to the use of legitimate interest or fraud prevention as the Legal Basis for Processing Personal Data in the Project.

Personal Data Protection Impact Report ("PDPIR"): document that contains a description of the Personal Data Processing processes that may give rise to risks to civil liberties and fundamental rights, as well as measures, safeguards and risk mitigation mechanisms.

Securiti: official Personal Data Management and Processing tool approved by the Company, to officially meet all the requirements of compliance with the LGPD and other applicable laws on the matter.

Data Subject: Individual to whom the Personal Data refers.

Third Party: all service providers, outsourced workers, business partners and suppliers of the Company.

Processing: any operation carried out with Personal Data, by automated or non-automated means, such as: collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, deletion, evaluation or control of information, modification, communication, transfer, dissemination or extraction.

Large-scale processing of personal data: involves processing the data of at least 2 million data subjects. If the data processing is less than this amount, the existence or not of "large-scale processing" must be determined based also on the volume of data involved, as well as the duration, frequency and geographical extent of the processing, taking into account the methodology adopted by the ANPD.

Data processing that significantly affects the interests and rights of data subjects: data processing that could potentially prevent the data subject from exercising rights guaranteed by Brazilian law, or accessing essential products/services, or even cause material or moral damage to data subjects, such as (but not limited to) discrimination, violation of physical integrity, right to image and reputation, financial fraud or identity theft.

Automated data processing: involves the use of algorithms or other technologies to carry out automated data processing, which may carry out operations or make decisions relating to personal data (e.g. classification, evaluation, approval or rejection of personal data, based on predefined criteria).

Data processing involving the use of emerging and/or innovative technologies: involves the use, for example, of technologies such as artificial intelligence, machine learning and generative AI, facial recognition systems, autonomous vehicles and/or any

innovations that may have practical applications with a high degree of business interest, with the potential to impact society, but which have not yet been fully explored and their risks are not fully known.

Data processing involving surveillance or control of areas accessible to the public and systematic monitoring, such as tracking the location of individuals: involves the processing of personal data for the purpose of monitoring or controlling the presence of people in public or private areas, with the possible use of tools such as security cameras, drones, GPS tracking devices, among others.

Processing of data aimed at forming a behavioral profile of individuals: processing that involves the use of behavioral data to generate profiling, which may or may not be the basis for automated decisions.

5. GUIDING PRINCIPLES FOR THE PROTECTION OF PERSONAL DATA

The SIMPAR Group will ensure that all its Personal Data Processing activities comply with the principles of the of the LGPD listed below:

Principles	Guidelines
Good Faith	The Processing of Personal Data should always be based on **good intentions,** ethics and respect for Data Subjects.
Purpose and Adequacy	The Processing of Personal Data must be limited to **legitimate, specific, explicit** purposes that have been informed to the Data Subject, and must only take place in ways that are compatible with these purposes.
Necessity	The collection and use of Personal Data must be limited to the **minimum necessary** to fulfill the defined purposes. Furthermore, such information must be stored for as short a time as possible / necessary.
Free Access and Quality	Data Subjects must be guaranteed **free and easy** access to information on the form and duration of Processing and the completeness of their Personal Data, ensuring that it is accurate, clear, relevant and up-to-date.
Security and Prevention	The security and confidentiality of Personal Data must be guaranteed through Technical and Organizational Measures in order to **prevent** the occurrence of Security Incidents involving Personal Data.
Transparency	Data Subjects must be provided with clear, **precise and easily accessible information** about the processing of their data and

	the respective agents involved, in compliance with the Company's commercial and industrial secrets.
Non-discrimination	Personal data will **never** be processed for discriminatory, unlawful or abusive purposes.
Responsibility and Accountability	**Records** must be kept of all Personal Data Processing activities and the respective measures taken to adapt these activities to the rules on privacy and protection of Personal Data, including proof of the effectiveness and efficiency of these measures.

6. GENERAL GUIDELINES AND GOVERNANCE STRUCTURE

6.1. NORMATIVE STRUCTURE OF THE PROGRAM

The regulatory structure of the Company's Privacy Program is made up of a set of documents drawn up by the technical departments, approved by the internal governance bodies and registered in the Company's document management system.

6.2. MANAGEMENT AND GOVERNANCE

The SIMPAR Group's Privacy Program shall be managed and governed by those responsible below:

6.2.1. Senior Management

Senior Management is responsible for acting directly in the management of risks (low, medium and high) related to the Processing of Personal Data, understanding and taking responsibility for the following stages: identification, evaluation, treatment and monitoring, seeking to ensure the best decision-making for the Company.

When necessary, and in compliance with current regulations and bylaws, Senior Management reports directly to the governance bodies, such as the Board of Directors and Audit Committee, among others. Senior Management is also responsible for ensuring that there is an adequate structure in place to manage the Privacy Program.

6.2.2. Personal Data Controller

The party responsible for processing personal data, also known as the Data Protection Officer or DPO, must have legal and technical knowledge related to the protection of personal data and experience in the field. The professional or organization acting as Data Protection Officer must have a reasonable degree of independence from the rest of management and their duties shall not include activities that could conflict with the Company's responsibility towards Data Subjects.

The role of the Data Protection Officer must ensure the Company's compliance with applicable laws and other privacy and Personal Data protection policies. Their main duties include:

a) Manage the Privacy Program;
b) Developing, maintaining and proposing reviews of the SIMPAR Group's privacy policies;
c) Acting as the SIMPAR Group's point of contact with the ANPD and the Card Holders;
d) Receive and manage requests from Data Subjects; and
e) Reviewing Personal Data Protection Impact Reports ("RIPD"), ascertaining and reviewing the risks of the activities.

The data controller, supported by the Internal Controls, Risks and Compliance Department (CRC) and by some business and/or technical departments, is responsible for providing advisory support to senior management in their decision-making on the Personal Data Processing activities carried out by the Company.
Finally, the data controller must help clear any doubts and guide other members of the Company during the execution of their activities, when they involve Personal Data Processing operations.

6.2.3. Internal Controls, Risks and Compliance Area - CRC

The Company's Internal Controls, Risks and Compliance Department shall be responsible, together with the data controller and, when necessary, with the support of some business and technical departments, for analyzing the risks involved in activities related to the processing of personal data.
They will also be responsible for other activities, such as:

a) analyzing projects involving Personal Data;
b) approving the privacy notices of the business units, prior to their actual publication, with the preparation of the data controller;
c) carrying out general activities related to the Privacy Program;
d) reviewing the Program's policies/procedures;
e) applying disciplinary measures for non-compliance with policies/procedures related to the Program;
f) ensuring that internal investigations aimed at evaluating possible non-compliance with laws related to privacy/processing of personal data are carried out impartially and independently;
g) ensuring the recording and support of activities related to the Program; and
h) reporting to the Audit Committee on the Program's indicators and risks related to the topic.

6.2.4. Privacy Ambassadors

Privacy Ambassadors are focal points who can be assigned to departments of the Company to act as a direct contact for the Compliance Officer and the CRC department. Ambassadors are responsible for facilitating communications, training and gathering information relating to their departments.

These agents will be appointed by the CRC department and may or may not form an Ambassador Committee, which will be responsible for supervising compliance with the Program's guidelines, as well as making recommendations on the Processing of Personal Data, through prior alignment with the CRC area and, when necessary, with the Data Controller.

6.2.5. Audit Committee

The Audit Committee shall operate under the exact terms of its Internal Regulations and is responsible for supervising adherence to legal, statutory and regulatory standards, the adequacy of risk management processes and the effectiveness of the Privacy Program.

When necessary, the Audit Committee shall report to the Board of Directors under the terms of its Rules of Procedure and Bylaws.

In order to carry out its duties, the Audit Committee shall have operational autonomy and a budget, within the limits approved by the Board of Directors, under the terms of the Company's Bylaws.

6.3. BASIC GUIDELINES OF THE PRIVACY PROGRAM

a) All Personal Data Processing operations carried out by the SIMPAR Group must follow the principles set out in the LGPD, in its article 6, described in item 5 of this instrument;

b) Every Personal Data Processing operation must be based on one of the legal hypotheses provided for in the LGPD (article 7 for Simple Personal Data or article 11 for Sensitive Personal Data);

c) The Company shall keep a record of its personal data processing activities, preferably containing the following information that allows identification: (i) the flow of personal data at each stage of its life cycle; (ii) the profile of the data subject; (iii) the types of data processed; (iv) the purpose of processing; (v) those internally responsible for the activity; (vi) the volume of personal data involved; (vii) the applicable legal processing hypothesis; and (viii) other information necessary to ensure that the SIMPAR Group is in compliance with the applicable laws and/or to enable management and direct the strategic actions of the Privacy Program;

d) Operations involving the sharing of Personal Data with third parties must be recorded and adequately protected through the application of personal data protection clauses. These operations must follow the provisions of the SIMPAR Group's Policy for Sharing Personal Data with Third Parties;

e) All new products, projects and initiatives involving the processing of Personal Data must be analyzed under the terms of the Privacy by Design Procedure;

f) Personal Data processing operations that require consent must be guided by the instructions described in the Company's Policy for the Use and Management of Consent;

g) The Personal Data processed must have a set duly justified retention period, and may be deleted after the end of the predetermined period. The retention periods must take into account the Company's internal needs, and must be set out in a separate document that compiles all the minimum retention periods; and

h) Information on the processing of personal data must be disclosed by means of Privacy Notices and/or other means that provide the necessary transparency to the Data Subject.

6.4. RIGHTS OF DATA SUBJECTS

The Company is committed to complying with the LGPD, especially with regard to the rights of data subjects:

Data Subject's Rights	Description
Right to Confirmation of the Existence of Processing	Guarantees that Data Subjects are able to obtain, at any time and upon request, confirmation of the existence or not of the Processing of their Personal Data.
Right of Access to Personal Data	Guarantees that Data Subjects are able to verify the form and duration of the Processing, as well as on the completeness of their Personal Data, in a free and simple manner.
Right to Correct Incomplete, Inaccurate or Outdated Personal Data	Guarantees that the Personal Data of Data Subjects is accurate, clear, relevant and up-to-date, according to the need and for the fulfillment of the purpose of its Processing.
Right to Anonymization, Blocking or Deletion of Personal Data	Guarantees that Data Subjects have the right to anonymization, blocking or deletion of Personal Data that is unnecessary, excessive or processed in breach of the LGPD.
Right to Portability	Guarantees that Data Subjects may have their Personal Data transferred to another service or product provider, upon express request, in accordance with ANPD regulations, observing commercial and industrial secrets.
Right to Information	Guarantees that Data Subjects may have access to information, including on the public and private entities with which their Personal Data has been shared.
Right to Withhold Consent and Right to Revoke Consent	Guarantees that Data Subjects may be informed of the possibility of withholding consent and the consequences of withholding consent. It also covers the possibility of revoking

	consent when this is the applicable legal basis.
Right to Review an Automated Decision	Guarantees that Data Subjects have the right to review decisions made solely on the basis of automated processing of personal data affecting their interests, including decisions aimed at defining their personal, professional, consumer and credit profiles or aspects of their personality.

The rights of the Data Subjects will be addressed by an exclusive channel created for this purpose, which is exclusive and suitable for complying with the law.

a) In the context of responding to requests from Data Subjects, the Company shall take the following guidelines into consideration:
b) Maintain an appropriate channel available for receiving requests at any time of the day, with confirmation of receipt of the request, even if automated;
c) Ensure that evidence is generated at all stages of the process, from the moment the request is received to the moment the response is sent;
d) Ensure cooperation between the business departments involved, to enable a response and the adoption of measures;
e) Comply with the data subject's request in accordance with the applicable legal deadlines; and
f) Facilitate the response procedure, keeping the data stored in formats that make consultation easier.

6.5. PERSONAL DATA PROTECTION IMPACT REPORT - RIPD

The Personal Data Protection Impact Report (RIPD) is an important tool to help the Company comply with the LGPD, as it helps it properly assess the risks that a given activity poses to data subjects, in addition to defining and demonstrating the adoption of appropriate measures to mitigate the risks identified. Taking into account the nature, context and purpose of the Personal Data Processing operation, the RIPD will be carried out whenever a particular activity poses a high risk to the guarantee of one of the general principles listed in the LGPD and to the rights and freedoms of Data Subjects.

Without prejudice to other situations in which the Data Protection Officer deems it necessary, the RIPD must be drawn up when a processing activity is classified as “high” criticality, based on the criticality matrix in Exhibit I.

Such documents must not be published or made available to third parties without the express authorization of the data controller and the CRC department management. However, they must be stored in a tool/network approved by the Company, since they may be subject to requests from the ANPD and/or internal and external audits.

7. TRANSPARENCY HOTLINE

Any questions and/or requests for information on this policy and other policies and procedures of the Company's Privacy Program can be addressed through the Transparency Hotline, by the following means of communication: 0800 726 7250 or conformidade@simpar.com.br (or use the domain of the company you wish to speak about, for example: @jsl, @movida, @grupovamos, etc).

8. NON-COMPLIANCE WITH THE PRIVACY PROGRAM AND THE REPORTING CHANNEL

The Company undertakes to make every effort to adopt technical and administrative measures to protect and prevent the occurrence of damage as a result of the Processing of Personal Data. The Company has a Whistleblower Channel which shall be used to report non-compliance with applicable laws, as well as with the policies/procedures related to the Company's Privacy Program.

This channel follows the best governance practices in the market and operates 24 hours a day, 7 days a week, ensuring that whistleblowers coming forth in good faith remain anonymous. The Whistleblowing Channel is managed by a third-party company, hired for this specific purpose, and can be called at: 0800 726 7111 or contatoseguro.com.br/SIMPAR (or use the domain of the company you wish to speak to, for example: @jsl, @movida, @grupovamos, etc.).

Failure to comply with any provision of this Policy, other rules of the Privacy Program and/or any applicable legal provision shall result in the application of the appropriate sanctions, without prejudice to being subject to other relevant legal measures.

9. FINAL PROVISIONS

This Policy has been approved by SIMPAR's Board of Directors and will come into force on the date of its publication, revoking and replacing any similar and previous guidelines on the same matter.

EXHIBIT I - CRITICALITY MATRIX

Criticality level	Criteria
Low	- Processing of personal data that do not classify as “medium” or “high”.
Medium	- Processing of personal data classified under any of the criteria (general or specific) indicated for “high” criticality level; - Processing of personal financial data; - Processing of authentication data in systems; - Processing of data protected by legal, judicial or professional secrecy; and/or - Processing of data from public or private third-party sources.
High	Criticality will be considered high when at least 1 general criterion is present, plus at least 1 specific criterion: **General Criteria:** - Processing of personal data on a large scale; or - Processing of data that significantly affects the interests and rights of data subjects. + **Specific Criteria** - Data processing involving surveillance or control of publicly accessible areas and systematic monitoring, such as tracking the location of individuals; - Data processing aimed at forming a behavioral profile of an individual; - Automated data processing; - Data processing involving the use of emerging or innovative technologies; and/or - Processing of sensitive data or data involving children, teenagers and/or the elderly.