Corporate Policy

Privacy & Data Protection

1 OBJECTIVE

The purpose of this Policy is to establish general guidelines to be followed by FORESEA concerning privacy and protection of personal data, considering that, in certain processes, while conducting their business, FORESEA needs to Process Personal Data.

Rules and procedures related to the subject matter of this Policy shall be addressed in detail in specific guidelines on each of the topics.

2 APPLICATION

This Policy is applicable to FORESEA, including their subsidiaries that do not have a Board of Directors, to all members, Officers and members of the Board of Directors, in any jurisdiction.

In addition, this Policy serves as a guide for the members of the boards of directors appointed by FORESEA, in subsidiaries or affiliates, so that, in line with all other directors, they approve and implement a policy on privacy and data protection containing the principles, concepts and all other guidelines defined and explained in this policy, without neglecting, however, to promote the complements and other guidelines which are necessary for adaptation to the characteristics of their respective businesses and to the contributions of all other directors.

3 ACRONYMS AND DEFINITIONS

Anonymization: process and technique through which data loses the possibility of direct or indirect association with an individual. Anonymized data is not considered Personal Data.

Business: a group of operations and/or investments intended to serve and satisfy customers, offering them specific goods and/or services, in defined markets and economic sectors.

CA-FORESEA: Board of Directors of FORESEA. Executive collegiate, deliberative body, responsible for approving the strategic direction and monitoring the company's performance, deliberating on other matters within its competence and exercising the control functions that are relevant to them.

CEO: Chief Executive Officer of DrilCo.

Consent: one of the legal grounds supporting the processing of Personal Data through which the Subject express their free, informed and unmistakable Manifestation, agreeing with the Processing of their Personal Data for a given purpose.

Controller: legal entity governed by public or private law, who is responsible for decisions regarding the Processing of Personal Data.

Crisis Committee: established by the CEO of FORESEA in the event of an Information Security Incident involving the leak of Personal Data whose severity may impact FORESEA's reputation and business.

Guiding Documentation: every formal document of FORESEA supplying content on decisions, rules and corporate guidelines which are vital to steer the work of FORESEA with legitimacy, traceability and applicability and must be observed and practiced by a certain defined universe of Members.

Incident or Breach of Personal Data: includes, but is not limited to any loss, exclusion, theft or unauthorized access to Personal Data, either controlled or processed by FORESEA.

LGPD: General Law for the Protection of Personal Data, Law No. 13,709/2018, is the Brazilian law that regulates the activities of processing personal data, including in digital media, by individuals or legal entities governed by public or private law, aimed at protecting the fundamental rights of freedom and privacy and the free development of the personality of individuals.

Partner: service providers, business partners and all those who are not classified as members and who interact with FORESEA's information.

Person in Charge or Data Protection Officer (DPO): individual designated as a formal/official data protection officer, as provided for in the LGPD.

Personal Data Processing or Processing: any operation or set of operations performed concerning Personal Data or sets of Personal Data, through automated or non-automated means such as collection, record, organization, structuring, conservation, adaptation or modification, recovery, inquiry, use, disclosure by transmission, diffusion or any other form of availability, comparison or interconnection, limitation, deletion or destruction.

Personal Data Subject or Subject: identified or identifiable unique individual to whom a specific Personal Datum is referred.

Personal Datum: any information related to a singular individual either identified or identifiable, who may be identified, either directly or indirectly, by reference to an identifier such as a name, identification number, location data, on-line identifier or to one or more factors which are specific to physical, physiological, genetic, mental, economic, cultural or social identity of such an individual.

Privacy Committee: ad-hoc forum to be created within the scope of FORESEA's Management, having, as members, the Legal VP, accumulating the role of Committee coordinator, and eventually all other persons in charge appointed by the CEO of FORESEA.

Processor or Operator: an individual or legal entity, governed by public or private law, which Processes Personal Data on behalf of the Controller.

Sensitive Personal Datum: every Personal Data which may produce any kind of discrimination such as that on racial or ethnic origin, religious belief, political opinion, affiliation to a trade union or organization of a religious, philosophical or political nature, datum related to health or sexual orientation, genetic or biometric datum.

Third party: individual or legal Entity acting on behalf of, in the interest or for the benefit of the Company, providing services or other goods, as well as commercial partners providing services to the company that are directly related to obtaining, retaining or facilitating businesses, or conducting company matters, including, but not limited to distributors, agents, brokers, forwarding agents, intermediates, supply chain partners, consultants, resellers, contractors and providers of professional services.

4 DESCRIPTION

4.1 Personal Data Protection Principles

This section describes the principles observed by FORESEA while Processing Personal Data to meet data protection standards within the corporate scope and be in compliance with applicable laws and regulations in the relevant countries where they hold business activities or operations.

4.1.1 Legality, Transparency and Non-Discrimination

FORESEA does not Process Personal Data without a legal reason to do so. Personal Data are processed fairly, with transparency and in compliance with applicable laws and regulations. Processing Personal Data is only allowed when its purpose falls within one of the following allowed legal cases:

- necessary for the celebration of an agreement or related preliminary procedures, to which the Data Subject is a party;
- requirement resulting from act or regulation to which FORESEA is subject;
- need of regularly exercising a right in legal, administrative or arbitration proceedings;
- legitimate interest in the Processing;
- to protect life or the physical integrity of the data subject or third parties;
- to protect health, solely, and a procedure performed by healthcare professionals; or
- upon given Consent by the Data Subject, if no other legal circumstance applies to such specific case.

When the Processing of Personal Data does not fall with the cases above, FORESEA must obtain Consent from Data Subject to Process their Personal Data and ensure such Consent is obtained in a specific, free and unmistakable manner. FORESEA will collect, store and manage all Consent responses in an organized, accessible manner, so that proof of Consent can be provided when necessary. The Data Subject has the possibility of withdrawing their Consent at any time with the same ease as it was provided.

In some circumstances FORESEA needs to process Sensitive Personal Data, for which the consent of the Personal Data Subject is required, except in the cases below in which the Processing is necessary for:

- compliance with a legal or regulatory obligation;

- the regular exercise of rights such as the defense or filing of lawsuits, administrative or arbitration actions;
- fulfillment of obligations and the exercise of rights in terms of employment, social security and social protection;
- protection of life or physical integrity of the Data Subject, including medical data with preventive, occupational purposes;
- promoting or maintaining equal opportunities between individuals of different racial or ethnic origins,
- addressing matters related to criminal convictions and breaches or to related protection measures under the control of the public authority or when the Processing is authorized by the laws of the Federal Government or of a Member State that provides for the appropriate safeguards for the rights and freedoms of the Personal Data Subjects.

To Process Sensitive Personal Data, FORESEA adopts security standards which are more solid than those used for all other Personal Data.

4.1.2 Limitation and Adequacy of the Purpose

Personal Data is Processed in a manner compatible with the original purpose for which it was collected. If Personal Data Subjects identify a Processing that is different from the allowed purpose, they may request that the Processing be suspended.

4.1.3 Necessity principle (data minimization)

FORESEA only processes Personal Data to the extent required to reach a specific purpose.
Personal Data may only be shared with a different area or company in the event of suitable legal support.

4.1.4 Accuracy (data quality)

FORESEA adopts reasonable measures to ensure any Personal Data in their possession is kept accurate and updated in relation to the purpose for which it was collected, and the Personal Data Subject is ensured the possibility of requiring exclusion or correction of unnecessary, inaccurate or outdated data.

4.1.5 Withholding and limitation of data storage

FORESEA keeps Personal Data stored only for the time required for the purposes for which it is processed.

4.1.6 Integrity and confidentiality (free access, prevention and security)

FORESEA ensures appropriate technical and administrative measures are applied to Personal Data to protect it against unauthorized or illegal Processing, as well as against accidental loss, destruction or damages.

4.1.7 Accountability and Rendering of Accounts

Compliance with this Policy is shown through the implementation of measures including, but not limited to:

- assurance that Personal Data Subjects may exercise their rights as they are described in item 4.5 Rights of Personal Data Subjects;
- record of Personal Data, containing a description of the purpose of the Processing, eventual sharing and period of withholding, including a record of incidents and breaches of Personal Data;
- assurance that, as Operators, Third Parties are acting according to this Policy and with the applicable laws and regulations;
- assurance that FORESEA is complying with all of the requirements and requests from the regulatory agency to which they are subject.

4.2 Security Standards

4.2.1 Importance of Protection and Security of Personal Data

FORESEA is committed with the implementation of Information Security standards and with the protection of Personal Data, including the right to self-determination of information, confidentiality, integrity and availability, as well as authenticity, responsibility and non-repudiation.

4.2.2 Obligation of secrecy concerning personal data

All Members with access to Personal Data ensure the confidentiality of Personal Data under their responsibility upon consent in a document to be defined for such a purpose.

4.2.3 Privacy of personal data by conception or standard

Upon implementing new processes, procedures or systems involving Personal Data Processing, FORESEA adopts measures to ensure Data Protection rules are followed from the conception stages to the launch/implementation of such projects.

4.3 Personal Data Controller-Processor Relationship

As the Personal Data Controller, FORESEA ensures Personal Data is being correctly processed by the Processor and in accordance with applicable laws.
As the Processor, FORESEA is required to follow the guidance of whoever is acting as the Controller.

4.4 Policy on the international transfer of Personal Data

Whenever Personal Data is processed in countries other than those where they were collected, the laws and regulations which apply to the international data transfer of each country are complied with. FORESEA ensures the existence and updating of agreements for the international transfer of Personal Data.

4.5 Rights of Personal Data Subjects

In addition to the rights of Personal Data Subjects described throughout this Policy, the Subject may also:

- oppose the Processing, if it is grounded on legitimate interest;
- obtain information on how their Personal Data will be processed and the access to Personal Data that FORESEA holds on them;
- request the correction of their Personal Data if they are inaccurate, incorrect or incomplete;
- request the deletion, blocking and/or anonymization of their Personal Data in given circumstances, such as when it is no longer needed for FORESEA to hold their Personal Data for the purposes for which they were collected;
- withdraw their Consent at any time if the Processing of Personal Data is based on the Consent of an individual for a specific purpose;
- request the portability of Personal Data to a different service or product supplier, upon express request in given circumstances;
- request the revision of decisions solely made based on the automated Processing of Personal Data; and
- file a complaint with FORESEA if you have reason to believe that any one of your rights has been breached and, if their response is not satisfactory to you, pursuant to the requirements of the LGPD, file a complaint with the applicable Data Protection Authority.

4.6 Outsourced Service Providers

Outsourced service providers processing Personal Data under FORESEA's instructions are subject to the obligations imposed on Operators according to the applicable laws. FORESEA ensures that the service agreement includes data protection clauses requiring the implementation of security measures, as well as appropriate technical and administrative controls to ensure the confidentiality and security of Personal Data and specify that the Processor is authorized to process Personal Data only when formally requested by FORESEA.

4.7 Data breach management

All incidents and potential breaches of personal data are reported to FORESEA's Person in Charge of Data Protection. All Members are aware of their personal responsibility of timely submitting and escalating possible issues, as well as reporting breaches or suspected Breaches of Personal Data as soon as they are identified.

4.8 Data Protection Audits

FORESEA ensures there are revisions from time to time in order to confirm that initiatives involving Privacy, their system, actions, processes, precautions and other activities, including Personal Data protection management are effectively implemented and kept and are in compliance with applicable laws and regulations.

4.9 General Provisions

Members are responsible for being familiar with and understanding all of the Guiding Documents applicable to them. Similarly, the Leaders are in charge of ensuring that all Members of their team understand and follow the Guiding Documents which are applicable to FORESEA.

Members who have questions concerning this Policy, including its scope, terms or obligations, must seek their respective Leaders, and, if necessary, FORESEA's Data Protection team.

Breaches of any of FORESEA's Guiding Documentation may result in serious consequences to FORESEA and Members involved. Therefore, any failure to comply with this Policy or to report any knowledge of breach of this Policy may result in disciplinary action to any Member involved.

4.10 Awareness and Certification

All FORESEA members and all other audiences covered by this document must be aware of this Policy on Privacy & Data Protection within a maximum of 90 days after its date of approval.

5 RESPONSIBILITIES

5.1 CA-FORESEA

- To approve this Policy and its future amendments; and
- To be liable for the appropriate use of Personal Data in their activities.

5.2 Culture, Communication, People and Sustainability Committee ("CCCPS")

- Revise and give their opinion on this Policy and its amendments to the Board of Directors;
- Be liable for the appropriate use of Personal Data in their activities; and
- Follow up the implementation and execution of Personal Data Protection practices determined in this Policy.

5.3 CEO of FORESEA

- Revise and recommend the approval of this Policy and its amendments to the Board of Directors;
- Provide compliance with this Policy;
- Be liable for the appropriate use of Personal Data in their activities;
- Communicate and encourage FORESEA's members about the importance of Personal Data protection and ensure compliance with the guidelines set out in this Policy; and
- Report to the CCCPS, either directly or through the Legal and Governance VP, the events related to the leaking of Personal Data and the decisions of the Privacy Committee.

5.4 Legal and Governance VP

- Approve the Documents for Guiding Local Personal Data Protection that fall within their competence, in line with this Policy;
- Indicate and act as the direct Leader of the Person in Charge of Data Protection, supporting them in the fulfillment of their duties;
- Report the concerns related to the implementation of privacy initiatives to the CEO;
- Revise, on an annual basis, or at a shorter interval, when necessary, the privacy initiatives adopted by FORESEA;
- Ensure that the necessary resources to implement and manage data protection initiatives are provided for in the budget for the Data Protection department; and
- Establish the Privacy Committee in case of incidents whose severity may impact FORESEA's Business.

5.5 Person in Charge of Data Protection

- Propose the implementation and revision of this Policy, whenever necessary, to the Legal and Governance VP;
- Act so that FORESEA complies with the laws and regulations related to Personal Data protection, and also with their policies, guidelines and internal procedures related to the subject;
- Lead, coordinate and supervise Personal Data protection strategy and guide the implementation of the action required to comply with the requirements set out by applicable laws and regulations of Personal Data protection;
- Participate and guide, under the privacy point-of-view, corporate projects involving Personal Data Processing, in order to validate adherence to the requirements of the applicable laws and regulations, in addition to ensuring privacy as a standard to be adopted and its incorporation when conceiving the required security arrangements;
- Hold training sessions, programs for the awareness and communication of the Personal Data privacy subject fully across FORESEA;
- Prepare and keep the Guiding Documentation related to privacy that falls within their competence updated;
- Coordinate the performance of a data privacy impact analysis ("DPIA": Data Protection Impact Analysis);
- Define, revise and update privacy notices;
- Follow up and support the implementation of action plans to correct eventual privacy-related frailties; and
- Address and monitor requests from Personal Data Subjects according to current laws and regulations and with FORESEA's Guiding Documentation, in order to ensure they are responded within the deadline;
- Discuss and make technical decisions on new Personal Data Processing activities based on Personal Data protection impact reports;
- Cooperate and liaise with the National Personal Data Protection Authority (Brazil), when required.

5.6 Privacy Committee

- Provide advisory and deliberative support, on an executive basis, in cases of Personal Data incidents;
- Be liable for the appropriate use of Personal Data in their activities;
- Evaluate the report on the Personal Data incident, and decide on the technical and disciplinary measures to be applied in cases of incidents involving Personal Data; and

- Act in coordination with the Crisis Committee, to be set up by the CEO of FORESEA in the event of an Information Security Incident involving the leaking of Personal Data whose severity may impact FORESEA's business and reputation.

5.7 Leaders

- Be liable for the appropriate use of Personal Data in activities in their respective areas, according to the applicable laws, and also that their subordinates behave according to this Policy;
- Revise and keep the mapping of Personal Data of their area updated, at least once a year (or always in the event of significant changes), with the support of the Data Protection Department; and
- Ensure that, upon using Consent to Process Personal Data, that it is collected and managed so that the option given by the Datum Subject is respected and produces evidences which are necessary for submission to the authorities or to the Subject him/herself, when necessary.

5.8 Information Security Team

- Be liable for the appropriate use of Personal Data in their activities;
- Analyze breaches and leaks of Personal Data, and also collect technical evidences;
- Monitor and implement security measures to ensure compliance with the applicable laws and regulations;
- Publish privacy notices in outside websites and programs;
- Revise and keep the Guiding Documentation related to Information Security that falls within their competence updated;
- Define a procedure and templates to formalize Personal Data incidents;
- Provide technical support and analyze new tools and systems focusing on exposure of Personal Data; and
- Ensure the application of security measures which are proportional to the risk generated by Personal Data Processing and in line with the expected protection of the Personal Data Subject, ensuring integrity, availability and confidentiality of such information.

5.9 Legal Team

- Be liable for the appropriate use of Personal Data in their activities;
- Act so that the agreements that include the assignment or processing of Personal Data contain data protection clauses which are adequate to the applicable laws and regulations;
- Provide legal support in the event of Personal Data leaks;
- Provide legal support in the interpretation of the laws and regulations relating to Personal Data protection;

- Support the renegotiation of agreements/amendments with suppliers and customers who Process Personal Data; and
- Support interfacing with National Personal Data Authorities.

5.10 All FORESEA members

- Be liable for the appropriate use of Personal Data in their activities;
- Comply with the applicable laws and regulations, and also with FORESEA's Guiding Documentation related to Personal Data protection and application of appropriate IT security measures;
- Report to the Person in Charge of Data Protection the occurrence of any Personal Data or data security incidents, as well as any related deficiencies identified or possible privacy risks; and
- Take part in data protection training activities.

6 REFERENCE DOCUMENTS

- FORESEA's Code of Conduct.
- Information Technology and Security Policy.
- Federal Law No. 13,709/2018, General Data Protection Law.

7 REFERENCE PROCESSES MAPS

NA

8 ANNEXES

NA