

## Sumário

<b>1. INITIAL PROVISIONS</b> .....	2
<b>2. OBLIGATIONS OF THE THIRD PARTY IN THE PROCESSING OF PERSONAL DATA</b> .....	2
<b>3. FORMS OF DATA PROCESSING</b> .....	2
<b>4. PRINCIPLES GOVERNING THE PROCESSING OF PERSONAL DATA</b> .....	3
<b>5. PERSONAL DATA INCIDENTS</b> .....	3
<b>6. COMPLIANCE AND ETHICAL STANDARDS</b> .....	3
<b>7. NON-DISCLOSURE AGREEMENT</b> .....	4
<b>8. INFORMATION RETENTION</b> .....	4
<b>9. INTERNATIONAL TRANSFER OF DATA</b> .....	4

# DATA PROTECTION AND COMPLIANCE POLICY

This Data Protection and Compliance Policy ("Policy") applies to contractual relationships with INTELBRAS S/A – INDÚSTRIA DE TELECOMUNICAÇÃO ELETRÔNICA BRASILEIRA, enrolled with the Brazilian National Registry of Legal Entities (CNPJ) under No. 82.901.000/0001-27, hereinafter referred to as "INTELBRAS", whether such relationships are formal or informal, in which the Parties act as Controller and/or Processor in the processing of personal data.

## 1. INITIAL PROVISIONS

1.1 Glossary: Throughout this Policy, the terms listed below shall have the following meanings:

- Holder - Natural person to whom the Personal Data that are subject to processing refer.
- Personal Data - Any data related to an identified or identifiable natural person, such as: IP, geolocation, name, RG, CPF, address, telephone, bank account, vehicle data, among others.
- Sensitive Personal Data - It is Personal Data that presents racial or ethnic origin, religious conviction, political opinion, union affiliation, data referring to health or sex life, genetic or biometric data.
- Operator: a natural or legal person, whether governed by public or private law, who processes personal data on behalf of the controller.
- Third Party: any natural or legal person that maintains a relationship with the Intelbras and, as a result of such relationship, whether formal or informal, is involved in the processing of personal data.
- Treatment - It is every operation carried out with Personal Data, such as collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, elimination, evaluation, information control, communication, transfer, diffusion or extraction.

1.2 Integral Part: This Policy is an integral and inseparable part of the contractual relationship with Intelbras and may be formalized through the execution of the respective agreement, the express acceptance of these terms within the Intelbras' systems to which the Third Party has access, or through the electronic execution of this document itself as a standalone instrument.

## 2. OBLIGATIONS OF THE THIRD PARTY IN THE PROCESSING OF PERSONAL DATA

2.1 Responsibility for Data Processing: The Third Party undertakes, towards Intelbras and its respective successors and assignees, to process personal data in accordance with the requirements of this Policy and solely for the purposes set forth in the agreement entered with Intelbras, in compliance with Brazilian Federal Law No. 13,709/2018 (General Data Protection Law – LGPD) and all other applicable legislation. The Third Party further agrees to indemnify, reimburse and hold harmless such persons from and against any losses, damages or claims incurred or suffered as a result of any breach of privacy and data protection obligations.

2.2 Costs and Expenses: The Parties hereby acknowledge and declare that they are responsible for all costs and expenses arising from the activities performed under this Policy, in compliance with the data protection and privacy legislation in force in Brazil.

## 3. FORMS OF DATA PROCESSING

3.1. Purpose of Processing: The Third Party shall process personal data exclusively for the purposes of performing the agreement or complying with legal and regulatory obligations, and shall ensure that such personal data is not processed for any other activities and that no personal data is processed in a manner that differs from the limitations set forth below:

- a. Property of personal data: The transfer of personal data between the Parties may occur in relation to the following categories of data subjects: employees, legal representatives, directors, customers, users of products and software, business partners, including commercial representatives, buyers, suppliers and service providers.
- b. Purpose of the Transfer: The transfer of personal data may only be carried out for purposes authorized by law, in particular for the performance of the contractual object entered into between the Parties, compliance with legal obligations related to the purchase and sale of products and services, provision of technologies and solutions necessary for Intelbras or the Third Party activities, provision of services at Intelbras' premises or other locations, employment relationships, including the granting of benefits, and commercial relationships involving retail, resale, distribution and commercial representation, as well as other commercial partnerships, agreements and contractual arrangements.
- c. Categories of Data: The personal data transferred may include personal data, sensitive personal data (including health data), financial or banking data, and product-related data, such as serial numbers and IP addresses, among others.
- d. Recipients. Any personal data transferred as a result of this relationship between the Parties may only be shared with professionals directly involved in fulfilling the purposes outlined above.

## 4. PRINCIPLES GOVERNING THE PROCESSING OF PERSONAL DATA

4.1 Principles: Without prejudice to the principles governing data processing activities set forth in Article 6 of the Brazilian General Data Protection Law (Lei Geral de Proteção de Dados – LGPD), the relationship between the Parties shall also be governed by the following principles:

- a. Purpose Limitation: Personal data may be processed only for purposes expressly authorized by their respective data subjects.
- b. Data Quality and Proportionality: Personal data must be accurate and, where necessary, kept up to date. Personal data shall be adequate, relevant and not excessive in relation to the purposes for which they are transferred and subsequently processed.
- c. Transparency: Data subjects shall be provided with clear, adequate and easily accessible information regarding the processing of their personal data and the respective responsible parties, whether acting as Controller or Processor.
- d. Security and Confidentiality: The Parties shall adopt appropriate technical and organizational security measures commensurate with the risks associated with the processing of personal data under this Agreement, in order to protect against risks such as accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, among others. Any person acting under the authority of the Parties, including a processor, shall process personal data only upon authorization and in accordance with the instructions of the data controller.
- e. Rights of Access, Rectification, Erasure and Objection: As provided in Articles 6 and 7 of the Brazilian General Data Protection Law, data subjects may request access to their personal data in accordance with applicable laws and regulations, including guidance issued by the Brazilian Data Protection Authority (ANPD).

## 5. PERSONAL DATA INCIDENTS

5.1 Incident Notification: In the event of any incident, or even the threat of an incident, it shall be the responsibility of the Third Party to immediately notify Intelbras with which it maintains a relationship, through the contacts indicated below. The Third Party shall adopt all legal and administrative measures necessary to mitigate risks and any potential damages:

INTELBRAS	<a href="mailto:privacidade@intelbras.com.br">privacidade@intelbras.com.br</a>
-----------	--

5.2 Privacy Policy: For further details, please refer to the Privacy Policy available on the website. The Third Party hereby acknowledges and agrees to all of its provisions:

INTELBRAS	<a href="http://www.intelbras.com/pt-br/politica-de-privacidade">www.intelbras.com/pt-br/politica-de-privacidade</a>
-----------	--

## 6. COMPLIANCE AND ETHICAL STANDARDS

6.1. Compliance: SUPPLIER shall exercise all of its rights and perform all of its obligations under this Agreement in an ethical manner, in strict compliance with all applicable laws and regulations and in accordance with the best principles, which the SUPPLIER declares to be aware of and agrees to observe and cause its Affiliates, employees, representatives and subcontractors to observe.

6.1.1. SUPPLIER undertakes to preserve INTELBRAS' good name, image and reputation and shall refrain from any conduct that may cause reputational, legal or ethical damage to INTELBRAS.

6.2. Product and legal compliance: SUPPLIER shall ensure that all Products marketed, sold or distributed comply with all applicable intellectual property, consumer protection, environmental, safety and regulatory laws. Any acceptance, approval or inspection by INTELBRAS shall not be construed as a waiver or limitation of SUPPLIER's responsibility to comply with applicable laws.

6.3. Human Rights, Labor and Non-Discrimination: SUPPLIER declares that it and its Affiliates do not use, tolerate or benefit from slave labor, forced labor, degrading working conditions or child labor, except as legally permitted for apprentices. SUPPLIER further undertakes to respect freedom of association, promote a safe and healthy work environment, prevent discrimination and harassment, and safeguard human dignity, in accordance with applicable laws and the INTELBRAS Code of Ethics and Conduct. SUPPLIER represents that neither it nor its Affiliates are involved in any ongoing or threatened claims related to such matters.

6.4. Anti-Corruption and Anti-Bribery: Each Party agrees to comply with all applicable anti-corruption and anti-bribery laws, including, without limitation, Brazilian Federal Law No. 12,846/13, the U.S. Foreign Corrupt Practices Act (FCPA), the U.K. Bribery Act and any other applicable international regulations.

6.4.1. SUPPLIER represents that neither it nor its directors, officers, employees or representatives have offered, promised, authorized or paid, directly or indirectly, any undue advantage or anything of value to any INTELBRAS employee, public official, regulatory authority or third party for the purpose of obtaining or retaining business or securing any improper advantage.

6.4.2. Any breach of this clause shall constitute material breach and shall entitle INTELBRAS to immediately terminate this Agreement, without prejudice to other legal remedies.

6.5. Reporting and Complaint Channel: SUPPLIER undertakes to report any irregularities, violations or suspected misconduct of which it becomes aware through INTELBRAS' official Complaint Channel, available at:

Complaint Channel [www.intelbras.com/pt-br/canal-de-denuncia](http://www.intelbras.com/pt-br/canal-de-denuncia)

## 7. NON-DISCLOSURE AGREEMENT

7.1. Confidential Information: The information supplied or disclosed between the Parties within this Agreement, hereinafter referred to as "Confidential Information" and "Trade Secrets", is generally described as the intellectual property of each Party, including, without limitation, its current or future products, maps, accounting or financial information, technical, strategic or business information, names of customers and/or suppliers, addresses and other similar data, contracts, practices, procedures and other commercial information, prototypes, devices, sketches, designs, component lists, electrical diagrams, software, reports, strategies, plans, documents, drawings, machines, tools, models, patent descriptions, samples, materials, as well as any information disclosed by any means of communication or obtained during visits to the facilities of either Party. Verbal information, when recorded or transmitted by audio files, must be protected and stored confidentially by their holders, and shall not be shared with third parties.

7.2. Mutual Obligations and Responsibilities: As a result of access to the Confidential Information, the Parties mutually agree and undertake to adopt all necessary measures to protect the Confidential Information received and to prevent any misuse thereof, whether intentional or negligent. The Parties further agree not to publish or disclose any article, advertisement, publicity or any other material related to any Confidential Information disclosed under this Agreement. All Confidential Information disclosed in connection with this Agreement shall remain exclusively in the possession of the Parties, their employees, representatives, administrators and consultants, and each Party undertakes to inform such persons of the existence of this Agreement and of the confidential nature of the information disclosed herein.

7.2.1. The Parties acknowledge that the disclosure of Confidential Information under this Agreement is made on a non-exclusive basis, and that each Party may, at any time and without limitation, disclose its own Confidential Information to third parties, provided that such disclosure is subject to confidentiality obligations like those set forth in this Agreement. Upon request of the Disclosing Party, the Receiving Party shall promptly return all documents received and destroy all documents produced that contain Confidential Information, on the date stipulated by the Disclosing Party.

7.2.2. The Parties further agree to notify each other immediately and in writing of any misuse, unauthorized disclosure, misappropriation or any breach of this Agreement of which they become aware.

7.3. Intellectual property: For purposes of this Agreement, intellectual property includes trademarks, patents, inventions, data, ideas, practices, routines, research, product components, product designs and all forms of proprietary knowledge, whether written, electronic, magnetic or stored in any other medium.

7.4. Information Property: All Confidential Information shall remain in the exclusive property of the Disclosing Party. Disclosure of Confidential Information shall not be construed as granting any license or rights under patents, copyrights, trademarks or other intellectual property.

7.5. Non-Accuracy of Information: Each Party acknowledges that Confidential Information is provided "as is", without any representation or warranty as to its accuracy or completeness, and that no liability shall arise from its use, except as expressly agreed in a definitive agreement.

7.6. Term: The confidentiality obligation shall remain in force during the term of this Agreement and for a period of up to five (5) years after its termination.

7.7. Compensation: Any breach of these provisions shall entitle the injured Party to seek fair compensation, including injunctive relief and preliminary measures, without prejudice to any other applicable remedies.

## 8. INFORMATION RETENTION

8.1. Elimination: The Parties undertake to eliminate any personal data processed as a result of the Agreement that has been used for a purpose already fulfilled or that is no longer necessary, except for data required to comply with legal or regulatory obligations, which may be retained, provided that the legal basis justifying such retention is expressly informed.

## 9. INTERNATIONAL DATA TRANSFER

9.1. Commitment to International Data Transfer Regulations: The Parties declare that they are aware of the provisions of Resolution CD/ANPD No. 19, dated August 23, 2024, which regulates the international transfer of personal data pursuant to

the Brazilian General Data Protection Law (Law No. 13,709/2018 – LGPD), and undertake to fully comply with their obligations, ensuring the appropriate level of personal data protection required by Brazilian law.

9.1.2. The Parties acknowledge that, in the event of an international transfer of personal data arising from the performance of this Agreement, they hereby acknowledge and agree to be bound by the standard contractual clauses issued by the ANPD, as set forth below.

## 10. INTERNATIONAL DATA TRANSFER REGULATION

10.1. **Parties Identification:** By this contractual instrument INTELBRAS acts as the Exporter/Data Controller, and the other party to the main contract, acts as the Importer/Processor.

10.2. **Object:** These Clauses apply to the International Data Transfers from the Exporter to the Importer, in accordance with the purpose of the contract, whose primary objective is the execution of said contract. Data storage shall occur in accordance with the Retention Policies of the Parties and in compliance with applicable legal obligations.

10.3. **Onward transfers:** These Clauses apply to the International Data Transfers from the Exporter to the Importer, in accordance with the purpose of the contract, whose primary objective is the execution of said contract. Data storage shall occur in accordance with the Retention Policies of the Parties and in compliance with applicable legal obligations.

10.4. **Responsibilities of the Parties:** Without prejudice to the duty of mutual assistance and the general obligations of the Parties, the Designated Party below, in the role of Controller, shall be responsible for fulfilling the following obligations under these Clauses:

- a) Responsible for publishing the document referred to in Clause 14:  
 Exporter     Importer
- b) Responsible for handling data subject requests referred to in Clause 15:  
 Exporter     Importer
- c) Responsible for notifying security incidents as referred to in Clause 16:  
 Exporter     Importer

10.4.1. For the purposes of these Clauses, if it is later verified that the Designated Party under item 4.1 is acting as a Processor, the Controller shall remain responsible for:

- a) fulfilling the obligations established in Clauses 14, 15, and 16 and other provisions under the National Legislation, especially in the case of omission or breach by the Designated Party;
- b) complying with determinations issued by the ANPD;
- c) ensuring data subject rights and compensating for any damage caused, as outlined in Clause 17.

### Section II – Mandatory Clauses

10.5. **Purpose:** These Clauses serve as a mechanism to enable the secure international flow of personal data. They establish minimum guarantees and valid conditions for the execution of International Data Transfers and aim to ensure the adoption of adequate safeguards to comply with the principles, data subject rights, and the data protection regime provided under the National Legislation.

10.6. **Definitions:** For the purposes of these Clauses, the definitions from Article 5 of Law No. 13.709/2018 (LGPD) and Article 3 of the ANPD's Regulation on International Data Transfers shall apply, without prejudice to other normative acts issued by ANPD.

10.7. **Applicable Law and Supervision By ANPD:** The International Data Transfer subject to these Clauses shall be governed by the National Legislation and supervised by ANPD, including its authority to apply preventive measures, administrative sanctions, or even limit, suspend, or prohibit transfers governed by these Clauses or by a Linked Contract.

10.8. **Interpretation:** Any interpretation of these Clauses shall:

- a) Always favor the Data Subject and align with the National Legislation;
- b) Apply the meaning of terms that most closely reflect the National Legislation in case of doubt;
- c) Not allow any clause (including Linked Contracts or Section IV provisions) to be interpreted with the goal of limiting or excluding responsibility regarding obligations established by law;
- d) Give precedence to Sections I and II in the event of conflicts with Sections III and IV or any Linked Contract.

10.9. **Third Party Adherence:** By mutual agreement, a third-party data processing agent may adhere to these Clauses as Exporter or Importer by signing a written instrument that becomes part of this document.

9.1 The adhering party shall have the same rights and obligations as the original Parties according to its role (Exporter or Importer).

10.10. **General Obligations of the Parties:** The Parties undertake to adopt and, when necessary, demonstrate the adoption of effective measures capable of proving compliance with these Clauses and the National Legislation, including the effectiveness of such measures. In particular, they must:

- a) Use Personal Data only for the specific purposes described in Clause 2, with no possibility of further processing incompatible with these purposes, and always in compliance with the limitations, guarantees, and safeguards herein;

- b) Ensure the compatibility of the processing with the purposes informed to the Data Subject, considering the context of the processing;
- c) Limit the processing to the minimum necessary to achieve the purposes, using only relevant, proportional, and non-excessive data;
- d) Ensure that Data Subjects, as provided in Clause 4, have:
  - (d.1) clear, precise, and easily accessible information on the processing and the respective agents, considering commercial and industrial secrecy;
  - (d.2) facilitated and free access to the form and duration of the processing and the entirety of their Personal Data;
  - (d.3) the accuracy, clarity, relevance, and up-to-date nature of their Personal Data;
- e) Adopt appropriate security measures compatible with the risks involved in the International Data Transfer governed by these Clauses;
- f) Not process Personal Data for illicit or abusive discriminatory purposes;
- g) Ensure that any person acting under their authority, including subcontractors or any agent collaborating for free or for payment, processes data only in accordance with their instructions and the provisions herein;
- h) Maintain records of Personal Data processing operations related to the International Data Transfer governed by these Clauses and provide such documentation to ANPD upon request.

11. **Sensitive Personal Data:** If the International Data Transfer involves Sensitive Personal Data, the Parties shall apply additional safeguards, including specific security measures proportional to the risks involved, the nature of the data, and the rights and interests to be protected, as described in Section III.

12. **Personal Data of Children and Adolescents:** If the International Data Transfer involves Personal Data of children and adolescents, the Parties shall apply additional safeguards, ensuring that the processing is carried out in the best interests of the child or adolescent, in accordance with National Legislation and relevant international instruments.

13. **Lawfulness of Data Use:** The Exporter warrants that the Personal Data was collected, processed, and transferred to the Importer in accordance with National Legislation.

14. **Transparency:** The Designated Party shall publish on its website a document containing clear, precise, and easily accessible information about the International Data Transfer, including at least:

- a) the method, duration, and specific purpose of the transfer;
- b) the destination country of the transferred data;
- c) identification and contact details of the Designated Party;
- d) joint use of data by the Parties and its purpose;
- e) the responsibilities of the agents involved in the processing;
- f) the rights of the Data Subject and how to exercise them, including a contact channel and the right to file a complaint before ANPD;
- g) Onward Transfers, including the recipients and purposes.

14.1. This document may be made available as a specific page or highlighted section within the Privacy Policy or an equivalent document.

14.2. Upon request, the Parties must provide the Data Subject with a free copy of these Clauses, observing commercial and industrial secrecy.

14.3. All information provided to Data Subjects under these Clauses must be written in Portuguese.

15. **Data Subject Rights:** The Data Subject has the right to obtain from the Designated Party, regarding Personal Data subject to the International Data Transfer governed by these Clauses, at any time and upon request, the following (pursuant to National Legislation):

- a) confirmation of processing;
- b) access to the data;
- c) correction of incomplete, inaccurate, or outdated data;
- d) anonymization, blocking, or deletion of unnecessary or excessive data, or data processed in violation of these Clauses or National Legislation;
- e) data portability to another service or product provider, as regulated by ANPD, respecting commercial and industrial secrecy;
- f) deletion of Personal Data processed with the Data Subject's consent, except as provided in Clause 20;
- g) information on public and private entities with which the Parties shared data;
- h) information about the possibility of not providing consent and the consequences of refusal;
- i) withdrawal of consent through a free and simple procedure, without prejudice to prior lawful processing;
- j) review of decisions made solely based on automated processing affecting their interests, including profiling;
- k) information about the criteria and procedures used in automated decisions, observing commercial and industrial secrecy.

15.1 The Data Subject may object to processing based on a legal exemption from consent if such processing violates these Clauses or National Legislation.

15.2 Requests under this Clause and Clause 14.3 must be answered within 15 (fifteen) days, unless ANPD regulations provide a different deadline.

15.3 If a request is sent to a Party that is not the Designated Party, the receiving Party shall:

- a) inform the Data Subject of the proper contact channel for the Designated Party; or
- b) forward the request to the Designated Party as soon as possible to ensure timely response.

15.4 The Parties must promptly inform all Processing Agents with whom data has been shared about any correction, deletion, anonymization, or blocking performed, unless it is impossible or requires disproportionate effort.

**15.5** The Parties shall provide mutual assistance to meet Data Subject requests.

**16. Security Incident Notification:** The Designated Party must notify ANPD and the Data Subjects within 3 (three) business days of any security incident that may pose a risk or significant harm to Data Subjects, in accordance with National Legislation.

**16.1** The Importer must maintain records of security incidents, pursuant to the National Legislation.

**17. Liability And Compensation for Damages:** Any Party that causes material, moral, individual, or collective damage through the processing of Personal Data in violation of these Clauses or National Legislation shall be liable for reparations.

17.1 The Data Subject may seek compensation from either Party for damages arising from violations of these Clauses.

17.2 The protection of the Data Subject's rights and interests may be pursued in court, individually or collectively, under applicable law.

17.3 The Processor shall be jointly liable for damages caused by processing when it fails to comply with these Clauses or does not follow lawful instructions from the Controller, subject to Clause 17.5.

17.4 Controllers directly involved in processing that results in damage shall also be jointly liable, subject to Clause 17.5.

17.5 A Party shall not be held liable if it can prove:

- a) it did not perform the processing attributed to it;
- b) it processed the data but did not violate these Clauses or National Legislation;
- c) the damage was caused exclusively by the Data Subject or a third party not involved in Onward Transfers or subcontracting.

17.6 Under National Legislation, the judge may reverse the burden of proof in favor of the Data Subject if the claim appears credible, the Data Subject faces difficulty in producing evidence, or producing such evidence would be excessively burdensome.

17.7 Collective actions seeking compensation under this Clause may be brought in court, as provided by applicable law.

17.8 A Party that compensates for the Data Subject may seek reimbursement from the other responsible Parties, according to their share of liability.

**18. Safeguards for Onward Transfers:** The Importer may only perform Onward Transfers of Personal Data subject to these Clauses with express authorization, as described in Clause 3.

18.1. In all cases, the Importer must:

- a) ensure that the purpose of the Onward Transfer is compatible with the specific purposes stated in Clause 2;
- b) ensure, via written contractual instrument, that the safeguards of these Clauses are observed by the recipient of the Onward Transfer; and
- c) be held responsible for any violations committed by the recipient of the Onward Transfer.

18.2 The Onward Transfer may also be based on another valid mechanism for International Data Transfers under National Legislation, regardless of the authorization in Clause 3.

**19. Access Request Notification:** The Importer shall notify the Exporter and the Data Subject of any Access Request related to the Personal Data transferred under these Clauses, unless such notification is prohibited by the data processing country's laws.

19.1. The Importer shall take appropriate legal actions, including court measures, to protect Data Subject rights whenever there is a legal basis to challenge the legality of the Access Request or any prohibition on notifying the parties per item 19.

19.2. The Importer shall maintain records of Access Requests, including date, requester, purpose, type of data requested, number of requests received, and legal actions taken, to respond to ANPD and the Exporter.

**20. End of Processing and Data Deletion:** The Parties must delete the Personal Data transferred under these Clauses after the processing ends, within the technical limits of their activities. Data may only be retained for the following purposes:

- a) compliance with legal or regulatory obligations by the Controller;
- b) research by a Research Body, with anonymization whenever possible;
- c) transfer to a third party, provided the requirements of these Clauses and National Legislation are met;
- d) exclusive use by the Controller, provided access is prohibited to third parties, and the data is anonymized.

20.1 For the purposes of this Clause, processing is deemed to have ended when:

- a) the purpose outlined in these Clauses has been achieved;
- b) the data is no longer necessary or relevant to the specified purpose;
- c) the processing period has ended;
- d) the Data Subject makes a valid request;
- e) ANPD orders it, due to violations of these Clauses or National Legislation.

21. **Data Processing Security:** The Parties shall adopt security measures that ensure protection of Personal Data subject to the International Data Transfer governed by these Clauses, even after the processing ends.

21.1 The security measures adopted shall be listed in Section III, taking into account the nature of the data, the characteristics and purpose of the processing, the state of the art, and the risks to Data Subject rights, especially for sensitive data and data of children and adolescents.

**21.2** The Parties shall periodically review and assess their security measures to ensure they remain adequate.

22. **Legislation of the Data Recipient Country:** The Importer declares that it has not identified any laws or administrative practices in the recipient country that prevent it from complying with these Clauses.

22.1 If such laws or regulations change, the Importer shall immediately notify the Exporter, so the Parties can evaluate whether to continue the contract.

23. **Non-Compliance by the Importer:** If the Importer violates any safeguards or cannot comply with these Clauses, it must immediately notify the Exporter, unless prevented by law (see item 19).

23.1 Upon notification or verification of non-compliance, the Exporter shall take appropriate measures to protect Data Subject rights and ensure compliance with these Clauses and National Legislation, which may include:

- a) suspending the International Data Transfer;
- b) requesting the return, transfer, or deletion of the data;
- c) terminating the contract.

24. **Jurisdiction and Choice of Law:** These Clauses are governed by Brazilian law. Any disputes between the Parties shall be resolved before Brazilian courts, subject to the jurisdiction chosen in Section IV.

24.1. Data Subjects may bring legal actions against the Exporter or Importer in Brazil, including in courts located in their place of residence.

24.2. By mutual agreement, the Parties may submit disputes under these Clauses to arbitration in Brazil, in accordance with the Arbitration Law.

### Section III – Security Measures

25. The Parties shall implement the following security measures to ensure the protection of Personal Data subject to the International Data Transfer governed by these Clauses:

- a) Governance and Oversight of Internal Processes;
- b) Technical and Administrative Security Measures, including those to ensure the security of operations such as data collection, transmission, and storage.