

# **PERSONAL DATA PROTECTION STANDARD FOR SUPPLIERS, SERVICE PROVIDERS AND PARTNERS OF THE CPFL ENERGIA GROUP**

SUMMARY

1. PRELIMINARY CONSIDERATIONS AND OBJECTIVE .....3

2. KEY CONCEPTS AND DEFINITIONS .....4

3. GENERAL OBLIGATIONS .....5

3.1. DUTIES .....5

3.2. PROHIBITIONS .....7

4. SPECIFIC OBLIGATIONS.....8

4.1. OBLIGATIONS OF DATA PROCESSORS .....8

4.2. OBLIGATIONS OF DATA CONTROLLERS .....**Erro! Indicador não definido.**

5. OTHER QUESTIONS .....12

5.1. NON-COMPLIANCE WITH THE POLICY .....12

5.2. CONTACT CHANNEL .....12

5.3. UPDATES .....12

## 1. PRELIMINARY CONSIDERATIONS AND OBJECTIVE

The CPFL Energia Group — which, for the purposes of this document, refers to the holding company CPFL Energia S.A. and all of its directly and indirectly controlled subsidiaries — maintains a strong commitment to ethics, integrity, and the security of individuals and informational assets related to its business activities. This commitment includes a focus on the importance of privacy and the protection of personal data.

In this regard, and in light of the Brazilian General Data Protection Law (“LGPD”), we have adopted — and continue to adopt — a series of measures, mechanisms, and procedures aimed at complying with applicable regulations and best practices on the subject.

As part of these efforts, the selection and engagement of suppliers, service providers, and partners of the CPFL Energia Group (hereinafter collectively referred to as “supplier(s)”) are based on technical, strategic, economic, professional, and ethical criteria. These criteria go beyond the guidelines set forth in our Supplier Code of Ethical Conduct (<http://portalmulti.cpfl.com.br/sites/portaldenoticias/programa-de-integridade/Documents/2.3%20Codigo%20conduta%20Etica%20Fornecedores.pdf>) and also include specific requirements regarding privacy and personal data protection.

Accordingly, this Personal Data Protection Policy aims to establish the minimum conditions required by the CPFL Energia Group for entering into contracts involving the processing of personal data, while also providing practical and clear guidance on the expected conduct of our suppliers, service providers, and partners.













Please note that all rules contained in this document are prerequisites for establishing a partnership with the CPFL Energia Group and must be interpreted in conjunction with the contract, commercial proposal, agreement, or other instrument used to formalize the legal relationship with us.

Therefore, all parties acting as suppliers, service providers, or partners of the CPFL Energia Group must also comply with the provisions of this Policy, ensuring that not only the contracting organization but also all its partners, employees, and third parties supporting the execution of its activities adhere to the rules set forth herein.

We recognize that this subject is still being assimilated and developed by various market participants in Brazil. A proactive, responsible, and collaborative approach by all companies is essential to building a robust and harmonious framework for data protection. For this reason, comments, questions, and suggestions for improving this document are welcome and may be directed to our Data Protection Management team via the channel [privacidade@cpfl.com.br](mailto:privacidade@cpfl.com.br), which will evaluate and respond to inquiries and assist, when necessary, in clarifying points raised in this Policy.

## 2. KEY CONCEPTS AND DEFINITIONS

For a better understanding of this Policy, we present below some key concepts and definitions regarding privacy and personal data protection:

		
PERSONAL DATA	SENSITIVE DATA	TREATMENT
Any information that can identify or make an individual identifiable, either directly (e.g., name, national ID, and taxpayer number) or indirectly (e.g., IP address, geolocation, and device-related information), whether online or offline..	Those related to racial or ethnic origin, religious beliefs, political opinions, trade union membership or affiliation with religious, philosophical, or political organizations, as well as data concerning health, sexual life, genetic or biometric information.	Any activity or set of activities carried out with personal data, whether in a physical or digital environment, including but not limited to collection, recording, access, viewing, dissemination, sharing, storage, and deletion.
		
DATA SUBJECT	DPO	LEGAL BASES
Natural person to whom the personal data refers. In contractual relationships established by the CPFL Group, personal data may relate to clients and prospects, employees and their dependents, shareholders, job applicants, among others.	Individual appointed by the data processing agent to serve as the organization's point of contact for matters related to privacy and personal data protection, assisting in communication with data subjects, the Brazilian Data Protection Authority (ANPD), and other stakeholders.	Legal bases established by the LGPD that authorize the performance of personal data processing activities for specific purposes, duly informed to the data subjects.
		
CONTROLLER	PROCESSOR	SUBCONTRACT(S)
Natural or legal person, under public or private law, who is responsible for making decisions regarding the processing of personal data.	Natural or legal person, under public or private law, who processes personal data on behalf of the controller.	Data processing agent engaged by the Importer, with no affiliation to the Exporter, to carry out the processing of Personal Data following an International Data Transfer.
		
INTERNATIONAL TRANSFER	EXPORTER	IMPORTER
Transfer of personal data to a foreign country or to an international	Data processing agent, located either within the national territory or in a	Data processing agent, located in a foreign country or acting as an international organization, who

organization of which the country is a member.	foreign country, who transfers personal data to the importer.	receives personal data transferred by the exporter.
--	---	---

3. GENERAL OBLIGATIONS

CPFL Energia Group reaffirms and guarantees that any personal data processing activity shall comply with the purposes set forth in the applicable contract, undertaking to act in accordance with the relevant legislation — including, but not limited to, the General Data Protection Law (LGPD) — in a manner that ensures all actions are lawful and do not conflict with current legal requirements.

Likewise, for the execution of contracts between any companies within the CPFL Energia Group and their suppliers, service providers, or partners — and whenever the contracted activity(ies) involve the processing of personal data — it is mandatory to observe the following general rules and commitments (without prejudice to the principles established in the LGPD, other applicable legislation, and the guidelines issued by the Brazilian National Data Protection Authority – ANPD):

3.1. DUTIES

The following are the duties of all suppliers, service providers, and partners of the CPFL Energia Group:

1. USE MINIMUM DATA NECESSARY	2. ENSURE THE SECURITY OF THE INFORMATION HANDLED
Use only the minimum amount of personal data necessary to achieve the business purpose, assuming sole responsibility for any processing of personal data carried out in violation of the laws and regulations governing the contract.	<ul style="list-style-type: none"><li>• Adopt technical, administrative, and information security measures necessary to protect personal data and prevent its misuse (whether accidental or unlawful), as well as unauthorized access to the information processed under the contract.</li><li>• Ensure, within its technical and operational capabilities, the inviolability, confidentiality, availability, and integrity of personal data, by implementing mechanisms such as (but not limited to):<ul style="list-style-type: none"><li>✓ Access control and restriction through the designation of authorized and responsible personnel for data processing;</li><li>✓ Encryption of information;</li><li>✓ Establishment of a data protection governance structure, including contingency and risk mitigation plans.</li><li>✓ Compliance with minimum information security and data protection standards.</li></ul></li></ul>
3. DOCUMENT ACTIONS AND MAINTAIN RECORDS OF PROCESSING ACTIVITIES	4. COOPERATE WITH THE CPFL GROUP TO ENSURE LEGAL COMPLIANCE AND PROPER CONTRACT PERFORMANCE

Maintain a detailed inventory of access to personal data and records of connections and access to applications, including the time, duration, identity of the employee or individual responsible for the access, and the file accessed — even when such access is carried out to comply with legal obligations or determinations issued by a competent authority.

Maintain records of all personal data processing operations performed, with detailed and up-to-date information, also including any international transfers of personal data, the destination country or organization, and the safeguards and mechanisms adopted to meet applicable legal requirements.

Establish a cooperative and proactive relationship with the CPFL Energia Group for resolving matters involving the processing of personal data related to the performance of the contract, providing all necessary documentation to demonstrate compliance with the obligations set forth in the contract and applicable legislation, and maintaining a designated contact channel within the organization authorized to respond to inquiries regarding personal data processing.

**5. PROVIDE ASSISTANCE TO THE CPFL GROUP TO MEET OFFICIAL REQUESTS**

The Supplier shall provide assistance to the CPFL Energia Group company, within the limits of the obligations imposed by the Brazilian General Data Protection Law (LGPD) or other applicable regulations, in the event that the ANPD or any other governmental authority (Judiciary, Public Prosecutor's Office, ANEEL, Senacon, Procon, etc.), or the data subject, requests information regarding the compliance of personal data processing arising from the contract. Such assistance shall be provided within the deadline specifically indicated by the CPFL Energia Group company.

If the Supplier receives official orders and/or communications (whether issued by judicial bodies, governmental authorities, the Public Prosecutor's Office, Procon, among others) requiring the disclosure of any information arising from the executed contract, the Supplier shall immediately notify the CPFL Energia Group company of such request and its terms. If legally prohibited from notifying the CPFL Energia Group company, the Supplier shall comply with the order (provided it is lawful) and inform the company of the action taken at the earliest possible opportunity.

**6. INTERNATIONAL DATA TRANSFER**

In the event that the performance of the services under the contract requires the international transfer of personal data to the Supplier, service provider, partner, or any of their Subprocessors, such international transfer shall be carried out in accordance with the applicable data protection legislation, particularly the provisions of Resolution CD/ANPD No. 19/2024 ("Resolution"), Article 33 of the LGPD, and the appropriate security and data protection controls as guided by the ANPD.

If the mechanism used for the international data transfer is the Standard Contractual Clauses (Annex I of this Policy), pursuant to the Resolution, the Supplier, service provider and/or partner shall ensure the inclusion of the following information in the standard clause:

- ✓ Name of the Data Importer and Exporter;
- ✓ Legal qualification of the Importer and Exporter;
- ✓ Principal address of the Importer and Exporter;
- ✓ Email address for contact with the Importer and Exporter;
- ✓ Contact details of the Importer and Exporter for the Data Subject;
- ✓ Other relevant information for the international data transfer;
- ✓ Main purposes of the transfer;
- ✓ Categories of data to be transferred;
- ✓ Retention period.

CPFL reserves the right to request, at any time, evidence of compliance with the provisions of this section. The Supplier shall provide such evidence within five (5) business days.

**3.2. PROHIBITIONS**

The following are strictly prohibited for any Supplier, service provider, or partner of the CPFL Energia Group:

1. UNAUTHORIZED SHARING	2. NON-COMPLIANCE WITH LAW
Transferring and/or sharing personal data accessed under the contract with third parties other than employees, agents, contractors, and subcontractors (if any) assigned to perform the activities provided for in the contract.	Failing to observe the minimum legal requirements applicable to the international transfer of personal data processed under the contract, as well as binding guidelines issued and/or approved by the National Data Protection Authority (ANPD).

3. USE OF INADEQUATE MEANS
Sharing documents of any nature or exchanging information containing personal data under this contract through electronic means not approved by the information security department of the CPFL Energia Group company. The use of personal devices to access or store sensitive data is prohibited unless duly authorized and protected.

4. SPECIFIC COMMITMENTS

In addition to the general commitments mentioned above, our suppliers, service providers, and partners must observe the specific rules set forth below, depending on the category of data processing agent to which they belong (either as **CONTROLLERS** or **PROCESSORS**), in accordance with the nature of their activities and the relationship established with the CPFL Energia Group, as defined below:



CONTROLLER

A natural or legal person responsible for making strategic-level decisions regarding the processing of personal data as established in a contract, including defining aspects such as the purpose of the processing, the types of data involved in the activity, the retention period of the personal data, among others.



PROCESSOR

A natural or legal person who engages in the processing of personal data in accordance with lawful instructions provided by the counterparty under contract, and who is prohibited from using any personal data accessed for their own benefit. This party may only make decisions at an operational level and does not have autonomy to define the manner or purpose of the use of personal data transmitted as a result of the contract.

4.1. OBLIGATIONS OF DATA PROCESSORS

When acting in the capacity of DATA PROCESSORS, the suppliers, service providers, and partners of the CPFL Energia Group shall comply with the following specific obligations, without prejudice to other provisions set forth in the applicable contract, legislation, and regulations:

1. ACTING IN ACCORDANCE WITH INSTRUCTIONS ISSUED BY THE CPFL ENERGIA GROUP

Carry out data processing activities strictly in accordance with the guidelines and instructions provided by the relevant company within the CPFL Energia Group, and under no circumstances use the personal data accessed during the performance of the contract for personal benefit or the benefit of third parties, for commercial purposes, or for any purposes not expressly provided for in the executed agreement.

Should the supplier disagree with any instruction or guidance received, it must notify the relevant CPFL Energia Group company in writing, providing justification for its objection.

2. ENGAGE THIRD PARTIES ONLY WHEN STRICTLY NECESSARY

Transfer and/or share information obtained as a result of the relationship established with the CPFL Energia Group only when such sharing is strictly necessary for the fulfillment of the contractual purpose, acknowledging that the CPFL Energia Group may, at its sole discretion, object to the engagement of third-party subprocessors, without any compensation being due to the parties involved.

3. LIABILITY FOR THIRD PARTIES ENGAGED IN THE ACTIVITIES

Ensure that all individuals or entities eventually engaged in activities related to the performance of the contract are subject to the same level of obligations as those established by applicable legislation and by the CPFL Energia Group, and

4. ENSURE THE TRANSMISSION OF OBLIGATIONS

Ensure that confidentiality and personal data protection obligations are extended to its employees, agents, contractors, and subcontractors (where applicable), guaranteeing that all individuals designated to perform



assume full and unrestricted responsibility for the acts performed by such third parties in connection with the contracted activities.

the activities are bound by confidentiality obligations regarding any personal data to which they may have access.

## **5. ENSURE DATA INTEGRITY**

Ensure the integrity of the information received, refraining from rectifying, deleting, or restricting the processing of personal data on its own initiative, and only doing so upon duly documented instructions issued by the relevant company within the CPFL Energia Group.

## **6. RESPOND TO REQUESTS**

Complete any and all materials requested by the CPFL Energia Group company related to applicable data protection and security standards (self-assessment), within the deadline established by the CPFL Energia Group company, taking full responsibility for the accuracy of the information provided in such documents. The supplier shall also make itself available to respond to requests, interviews, audits, and site visits necessary to verify the measures implemented for the protection of personal data (due diligence).

## **7. PROVIDE ASSISTANCE IN CASE OF INCIDENTS**

In the event of an incident involving personal data related to the performance of the contracted services, the supplier shall immediately report the occurrence to the relevant CPFL Energia Group company, within no more than one (1) business day from the date of the incident. The report must be submitted to the CPFL Group's Data Protection Officer and must include, at a minimum, the following information: (a) Corporate name of the Contracting Party and the respective contract manager; (b) Corporate name of the Contractor and the respective contract manager; (c) Type of contract, date of execution, and a summary of the contracted scope; (d) Date and time of the incident; (e) Date and time the incident was discovered; (f) List of types of personal data affected by the incident; (g) Number of affected data subjects (incident volume) and, whenever possible, identification of those individuals; (h) Contact details of the Data Protection Officer or, if unavailable, the person responsible for providing further information about the incident; (i) Description of the possible consequences of the incident; (j) Actions taken to mitigate adverse effects and prevent recurrence; (k) Measures being taken to remedy the damage; and (l) Post-incident analysis to identify the root cause and improve information security and data protection practices.

If not all of the above information is available at the time of the initial report, the supplier shall provide a follow-up communication as soon as the necessary details become available to clarify the incident.

## **8. FORWARD DATA SUBJECT REQUESTS**

Upon receiving any request related to data subject rights under the LGPD, whether from the data subject or from third parties (including public authorities), concerning personal data processed under the contract, the supplier shall inform the data subject that only the CPFL Energia Group is authorized to respond to such requests. The supplier must direct the data subject to the appropriate channel for exercising their rights, as provided in the Privacy Notice (<https://www.cpfl.com.br/institucional/privacidade/aviso-de-privacidade/Paginas/default.aspx>), and shall immediately forward the request to the relevant CPFL Energia Group company.

## **9. ASSUME LIABILITY**

Assume responsibility for any damage (whether direct or indirect) arising from the improper processing of personal data that is exclusively attributable to the supplier — including, but not limited to, non-compliance with data protection laws and regulations applicable to its area of operation, breach of rules or directives issued by the CPFL Energia Group, security incidents involving personal data, or processing activities that exceed what is necessary for the performance of the contract.

## **10. DELETION OF DATA UPON COMPLETION**

Proceed with the definitive deletion (including any copies) of the personal data processed under the agreement upon its termination or upon request by any company within the CPFL Energia Group — except where there is a legal basis for retaining such information, in which case the data shall be deleted as soon as retention is no longer necessary under applicable law — and provide written confirmation

The supplier shall indemnify the CPFL Energia Group for any evidencing the deletion of the information from all judicial or extrajudicial expenses, administrative fines, and electronic systems and/or physical archives. damages incurred. The CPFL Energia Group reserves the right to file a third-party complaint (denúnciação da lide) as provided for in Article 125, II of the Brazilian Code of Civil Procedure (CPC).

4.2. OBLIGATIONS OF CONTROLLERS

In certain situations, the business model and the operations of suppliers, service providers, and partners of the CPFL Energia Group with the entities of the CPFL Energia Group will require such companies to make specific decisions regarding the processing of personal data necessary for the performance of the contractual purpose, which results in both contracting parties being considered as DATA CONTROLLERS under the law.

In this regard, without prejudice to the other obligations agreed upon in a specific contractual instrument and the general commitments established in item 3 above, the CONTROLLERS undertake to:

<b>1. ENSURE QUALITY, LEGITIMACY, AND LAWFULNESS</b>	<b>2. ENSURE DATA SUBJECT RIGHTS</b>
Ensure the quality of personal data and transparency regarding its processing in relation to the data subject, as well as respond to requests made directly by the data subject, the contracting company(ies) within the CPFL Energia Group, the ANPD (Brazilian Data Protection Authority), or any other governmental authority (Judiciary, Public Prosecutor’s Office, ANEEL, SENACON, PROCON, among others).	Ensure that data subjects may exercise their rights under Article 18 of the LGPD (such as confirmation of processing, access, rectification, withdrawal of consent, objection), to the extent of each party’s involvement in the processing of personal data under the contract.
<b>3. TAKE APPROPRIATE MEASURES IN CASE OF INCIDENTS</b>	<b>4. LIABILITY FOR DAMAGES CAUSED</b>
<p>Adopt the measures provided for in applicable legislation—especially regarding notification of data subjects and the National Authority—in the event of a personal data breach occurring during the performance of its activities. The CPFL Energia Group company must be informed of the event through a communication containing, at a minimum, the following information:</p> <ul style="list-style-type: none"><li>(a) date and time of the incident;</li><li>(b) date and time the party became aware of the incident;</li><li>(c) types of personal data affected;</li><li>(d) number of affected users (incident volume) and, if possible, a list of those individuals;</li><li>(e) contact details of the party’s Data Protection Officer or, if unavailable, the person responsible for providing further information;</li><li>(f) description of the possible consequences of the incident for the other party;</li><li>(g) measures being taken to mitigate the risks.</li></ul> <p>A recurring “Security Incident Resolution and Actions Report” must be submitted, informing the CPFL Energia Group of the actions and measures taken during the resolution of the incident.</p>	<p>The Controller shall be liable for all personal data processing activities it performs in the course of its business operations, as well as for the lawfulness of such processing (compliance with applicable legislation and assurance of security). The Controller shall be accountable before the National Data Protection Authority or any other authority that may request information related to its data processing activities, except in cases where it did not carry out the processing, did not violate the law, or where any damage results solely from the fault of the data subject or third parties.</p> <p>In the event that the Controller is a provider of personal data, it shall also be liable for the origin of the shared information (when such information is the subject of the contract or necessary for its performance), for the security of the personal data, and for all obligations arising from its activities, as well as from the applicable laws and regulations governing personal data protection.</p>

---

If not all the above information is available at the time of the initial communication, it must be provided progressively to ensure the greatest possible promptness. The initial communication must be made within a maximum of one business day from the moment the incident becomes known, unless a shorter period is established by the ANPD.

---

## **5. ENSURE ADEQUATE SECURITY AND PREVENTION STANDARDS**

---

To ensure an adequate level of security in the processing of information under the contract, the supplier shall, among other measures:

- Maintain strategies to protect login authentication;
  - Ensure traceability of access (including servers, backend, edge, chatbot platforms, management platforms, and any other databases or software used);
  - Enable secure coding practices, following a secure development model (e.g., Secure Software Development Lifecycle - SSDLC);
  - Provide regular or ad hoc training to employees on information security and data protection practices;
  - In the event of international data transfers or processing of personal data outside Brazil through service providers, ensure that such providers comply with the same obligations set forth in this section.
-

## 5. OTHER PROVISIONS

Finally, our suppliers, service providers and partners should pay attention to the following issues:

### 5.1. NON-COMPLIANCE WITH THE POLICY

Failure to comply with one or more provisions of this Personal Data Protection Policy, as well as with other contractual instruments executed between the parties, may result in the immediate termination of the contractual relationship without any compensation being owed by the CPFL Energia Group, in addition to the application of contractual penalties, judicial sanctions, and administrative sanctions imposed by regulatory authorities (such as consumer protection agencies and the ANPD). These sanctions may include warnings, fines calculated based on revenue, public disclosure of the violation, and suspension of activities.

It is important to note that the provisions of this Policy shall remain enforceable and in effect for as long as any personal data processing operations continue, even after the termination of the contract or other agreements entered into with the CPFL Energia Group.

### 5.2. CONTACT CHANNEL

The CPFL Energia Group invests in various relationship initiatives aimed at aligning suppliers with its business principles. Accordingly, the provisions of this Policy must be observed in conjunction with other policies and standards applicable to supplier relationships, which are available at: <https://www.cpfl.com.br/institucional/fornecedores/Paginas/default.aspx>.

If you have any questions regarding this Policy or your obligations and responsibilities as a personal data processing agent—or if you believe you are unable to comply with the applicable legislation and the guidelines established by the CPFL Energia Group—please contact our Data Protection Management team at: [privacidade@cpfl.com.br](mailto:privacidade@cpfl.com.br)

### 5.3. UPDATES

This Personal Data Protection Policy for Suppliers, Service Providers, and Partners may be amended at any time. Recipients of this document are expected to remain up to date with their obligations by regularly consulting the CPFL Energia Group's website for the latest version and revision history.

In the event of substantial changes to this Policy that significantly impact data processing operations or the relationships established between the CPFL Energia Group and its suppliers, service providers, and partners, reasonable efforts will be made to notify stakeholders of such updates, prioritizing the most widely used communication channels for engagement with the relevant audience.

Last update: 17/03/2025

ANNEX I

STANDARD CONTRACTUAL CLAUSES FOR INTERNATIONAL DATA TRANSFER

[=]; and

[Qualification]; and

Exporter and Importer, together referred to as the "Parties" and individually referred to as the "Party".

**Whereas** , within the framework of the relationship between the Parties, international transfers of personal data may take place;

**Considering** the regulation of international transfers of personal data through Resolution CD/ANPD No. 19/2024 and the need to adapt international transfers of personal data carried out within the scope of the relationship between the Parties to this rule;

**The Parties agree by mutual agreement to enter into these Standard Contractual Clauses for International Data Transfer.**

CLAUSE 1. Identification of the Parties

1.1. By this agreement, the Exporter and the Importer (hereinafter, "Parties"), identified below, have agreed to these standard contractual clauses (hereinafter, "Clauses") approved by the National Data Protection Authority (ANPD), to govern the International Data Transfer described in CLAUSE 2, in accordance with the provisions of the National Legislation.

Name:	
Qualification:	
Main address:	
Email Address:	
Contact for the Data Subject:	
Other information:	
<div>( ) Exporter/Controller</div> <div>( ) Exporter/Processor</div>	

Name:	
Qualification:	
Main address:	
Email Address:	
Contact for the Data Subject:	
Other information:	

( ) Importer/Controller  
( ) Importer/Processor

## CLAUSE 2. Object

2.1. This Clauses shall apply to International Transfers of Personal Data between Data Exporters and Data Importers, as described below.

Description of the international data transfer:	
Main purposes of the transfer:	
Categories of personal data transferred:	
Period of Data storage:	
Other information:	

*(NOTE: fill in as many details as possible with the information regarding the international transfer)*

## CLAUSE 3. Onward Transfers

(NOTE: choose between "OPTION A" and "OPTION B", as appropriate)

OPTION A. 3.1. The Importer may not carry out an Onward Transfer of Personal Data subject to the International Data Transfer governed by these Clauses, except in the cases provided for in item 18.3.

OPTION B. 3.1. The Importer may carry out an Onward Transfer of Personal Data subject to the International Data Transfer governed by these Clauses, in the cases and according to the conditions described below and the provisions of CLAUSE 18.

Main purposes of the transfer:	
Categories of personal data transferred:	
Data storage period:	
Other information:	

*(NOTE: fill in as many details as possible with information regarding authorized subsequent transfers)*

## CLAUSE 4. Responsibilities of the Parties

(NOTE: choose between "OPTION A" and "OPTION B", as appropriate.)

4.1 Without prejudice to the duty of mutual assistance and the general obligations of the Parties, the Designated Party below, as Controller, shall be responsible for complying with the following obligations set out in these Clauses: a) Responsible for publishing the document provided in CLAUSE 14; ( ) Exporter ( ) Importer b) Responsible for responding to requests from Data Subjects dealt with in CLAUSE 15: ( ) Exporter ( ) Importer c) Responsible for notifying the security incident

provided in CLAUSE 16: ( ) Exporter ( ) Importer (NOTE: in items “a”, “b” and “c”, check the option corresponding to: (i) “Exporter” or “Importer”, in cases where only one of the Parties acts as controller; or (ii) check both options, in cases where both Parties act as controllers. Responsibility for compliance with the obligations referred to in Clauses 14 to 16 cannot be attributed to the Party acting as Processor. Should it subsequently be ascertained that the Designated Party is acting as Processor, the provisions of Clause 4.2 shall apply.

4.2. For the purposes of these Clauses, if the Designated Party pursuant to item 4.1. is the Processor, the Controller remains responsible for:

- a) compliance with the obligations provided in CLAUSES 14, 15 and 16 and other provisions established in the National Legislation, especially in case of omission or non-compliance with the obligations by the Designated Party;
- b) compliance with ANPD’s determinations; and
- c) guaranteeing the Data Subjects’ rights and repairing damages caused, subject to the provisions of Clause 17.

OPTION B. (NOTE: “Option B” is exclusive for international data transfers carried out between processors)

4.1. Considering that both Parties act exclusively as Processors within the scope of the International Data Transfer governed by these Clauses, the Exporter declares and guarantees that the transfer is carried out in accordance with the written instructions provided by the Third-Party Controller identified in the chart below.

Identification information of the third-party controller:
Name:
Qualification:
Main address:
E-mail address:
Contact for the data subject:
Information on related contract:

(NOTE: fill in as many details as possible with the identification and contact information of the Third Party Controller and, if applicable, of the Related Contract).

4.2. The Exporter shall be jointly liable for the damage caused by the International Data Transfer if it is carried out in breach of the obligations of the National Legislation or the lawful instructions of the Third-Party Controller, in which case the Exporter shall be deemed to be the Controller, subject to the provisions of Clause 17.

4.3. In the event of being deemed a Controlling Party as referred to in item 4.2, the Exporter shall be responsible for complying with the obligations set out in Clauses 14, 15 and 16.

4.4. With the exception of the provisions of items 4.2 and 4.3, the provisions of Clauses 14, 15 and 16 shall not apply to the Parties as Processors.

4.5. The Parties shall, in any event, provide all the information at their disposal that proves necessary for the Third-Party Controller to comply with ANPD's determinations and to adequately fulfill the obligations provided for in the National Legislation relating to transparency, compliance with the rights of data subjects and the reporting of security incidents to ANPD.

4.6. The Parties shall promote mutual assistance in order to meet the requests of the Data Subject.

4.7. In the event of receiving a request from a Data Subject, the Party shall: a) respond to the request when it has the necessary information; b) inform the Data Subject of the service channel provided by the Third-Party Controller; or c) forward the request to the Third-Party Controller as soon as possible, to enable a response within the period provided for in the National Legislation.

4.8. The Parties must keep a record of security incidents involving personal data, in accordance with national legislation.

## **Section II - Mandatory Clauses**

*(NOTE: This Section contains Clauses that must be adopted in full and without any change in their text in order to ensure the validity of the international transfer of data)*

### **CLAUSE 5. Purpose**

5.1. These Clauses are presented as a mechanism to enable the secure international flow of personal data, establish minimum guarantees and valid conditions for carrying out the International Data Transfer and aim to guarantee the adoption of adequate safeguards for compliance with the principles, the rights of the Data Subject and the data protection regime provided for in National Legislation.

### **CLAUSE 6. Definitions**

6.1. For the purposes of these Clauses, the definitions in art. 5 of LGPD, and art. 3 of the Regulation on the International Transfer of Personal Data shall be considered, without prejudice to other normative acts issued by ANPD. The Parties also agree to consider the terms and their respective meanings as set out below:

(a) processing agents: the controller and the processor;

b) ANPD: National Data Protection Authority;

c) Clauses: the standard contractual clauses approved by the ANPD, which are part of Sections I, II and III;

d) Related Contract: contractual instrument signed between the Parties or, at least, between one of them and a third-party, including a Third-Party Controller, which has a common purpose, link or dependency relationship with the contract that governs the International Data Transfer;

e) Controller: Party or third-party ("Third Controller") responsible for decisions regarding the processing of Personal Data;

f) Personal Data: information related to an identified or identifiable natural person;

g) Sensitive Personal Data: personal data on racial or ethnic origin, religious belief, political opinion, affiliation to trade unions or to a religious, philosophical or political organization, data regarding health or sexual life, genetic or biometric data, whenever related to a natural person;

h) Erasure: exclusion of data or dataset from a database, regardless of the procedure used;

i) Exporter: processing agent, located in the national territory or in a foreign country, who transfers personal data to the Importer;

j) Importer: processing agent, located in a foreign country or that is an international organization, which receives personal data from the Exporter;

k) National Legislation: set of Brazilian constitutional, legal and regulatory provisions regarding the protection of Personal Data, including the LGPD, the International Data Transfer Regulation and other normative acts issued by the ANPD;

l) Arbitration Law: Law No. 9,307, of September 23, 1996;



- m) Security Measures: technical and administrative measures able to protect Personal Data from unauthorized access and from accidental or unlawful events of destruction, loss, alteration, communication or dissemination;
- n) Research Body: body or entity of the government bodies or associated entities or a non-profit private legal entity legally established under Brazilian laws, having their headquarter and jurisdiction in the Brazilian territory, which includes basic or applied research of historical, scientific, technological or statistical nature in its institutional mission or in its corporate or statutory purposes;
- o) Processor: Party or third-party, including a Sub-processor, which processes Personal Data on behalf of the Controll;
- p) Designated Party: Party or a Third-Party Controller, under the terms of CLAUSE 4, designated to fulfill specific obligations regarding transparency, Data Subjects' rights and notifying security incidents;
- q) Parties: Exporter and Importer;
- r) Access Request: request for mandatory compliance, by force of law, regulation or determination of public authority, to grant access to the Personal Data subject to the International Data Transfer governed by these Clauses;
- s) Sub-processor: processing agent hired by the Importer, with no link with the Exporter, to process Personal Data after an International Data Transfer;
- t) Third-Party Controller: Personal Data Controller who authorizes and provides written instructions for the carrying out of the International Data Transfer between Processors governed by these Clauses, on his behalf, pursuant to Clause 4 ("Option B");
- u) Data Subject: natural person to whom the Personal Data which are subject to the International Data Transfer governed by these Clauses relate;
- v) Transfer: processing modality through which a processing agent transmits, shares or provides access to Personal Data to another processing agent;
- w) International Data Transfer: transfer of Personal Data to a foreign country or to an international organization which Brazil is a member of; and
- x) Onward Transfer: transfer of Personal Data, within the same country or to another country, by an Importer to a third-party, including a Sub-processor, provided that it does not constitute an Access Request.

## **CLAUSE 7. Applicable legislation and ANPD supervision**

7.1. The International Transfer of Data subject to these Clauses is subject to National Legislation and to the supervision of the ANPD, including the power to apply preventive measures and administrative sanctions to both Parties, as the case may be, as well as the power to limit, suspend or prohibit international transfers arising from these Clauses or a Linked Contract.

## **CLAUSE 8. Interpretation**

8.1. Any application of these Clauses shall occur in accordance with the following terms:

- a) these Clauses shall always be interpreted more favorably to the Data Subject and in accordance with the provisions of the National Legislation;
- b) in case of doubt about the meaning of any term in these Clauses, the meaning which is most in line with the National Legislation shall apply;
- c) no item in these Clauses, including a Related Agreement and the provisions set forth in SECTION IV, shall be interpreted as limiting or excluding the liability of any of the Parties in relation to obligations set forth in the National Legislation; and

d) provisions of SECTIONS I and II shall prevail in case of conflict of interpretation with additional clauses and other provisions set forth in SECTIONS III and IV of this agreement or in Related Agreements.

#### **CLAUSE 9. Docking Clause**

9.1. By mutual agreement between the Parties, it shall be possible for a processing agent to adhere to these Clauses, either as a Data Exporter or as a Data Importer, by completing and signing a written document, which shall form part of this contract.

9.2. The acceding party shall have the same rights and obligations as the originating parties, according to the position assumed of Exporter or Importer and according to the corresponding category of treatment agent.

#### **CLAUSE 10. General Obligations of the Parties**

10.1. The Parties undertake to adopt and, when necessary, demonstrate the implementation of effective measures capable of demonstrating observance of and compliance with the provisions of these Clauses and the National Legislation, as well as with the effectiveness of such measures and, in particular:

a) use the Personal Data only for the specific purposes described in CLAUSE 2, with no possibility of subsequent processing incompatible with such purposes, subject to the limitations, guarantees and safeguards provided for in these Clauses;

b) guarantee the compatibility of the processing with the purposes informed to the Data Subject, according to the processing activity context;

c) limit the processing activity to the minimum required for the accomplishment of its purposes, encompassing pertinent, proportional and non-excessive data in relation to the Personal Data processing purposes;

d) guarantee to the Data Subjects, subject to the provisions of Clause 4:

(d.1.) clear, accurate and easily accessible information on the processing activities and the respective processing agents, with due regard for trade and industrial secrecy;

(d.2.) facilitated and free of charge consultation on the form and duration of the processing, as well as on the integrity of their Personal Data; and

(d.3.) accuracy, clarity, relevance and updating of the Personal Data, according to the necessity and for compliance with the purpose of their processing;

e) adopt the appropriate security measures compatible with the risks involved in the International Data Transfer governed by these Clauses;

f) not to process Personal Data for abusive or unlawful discriminatory purposes;

g) ensure that any person acting under their authority, including sub-processors or any agent who collaborates with them, whether for reward or free of charge, only processes data in compliance with their instructions and with the provisions of these Clauses;

h) keep a record of the Personal Data processing operations of the International Data Transfer governed by these Clauses, and submit the relevant documentation to ANPD, when requested.

#### **CLAUSE 11. Sensitive personal data**

11.1. If the International Data Transfer involves Sensitive Personal Data, the Parties shall apply additional safeguards, including specific Security Measures which are proportional to the risks of the processing activity, to the specific nature of the data and to the interests, rights and guarantees to be protected, as described in SECTION III.

#### **CLAUSE 12. Personal data of children and adolescents**

12.1. In case the International Data Transfer governed by these Clauses involves Personal Data concerning children and adolescents, the Parties shall implement measures to ensure that the processing is carried out in their best interest, under the terms of the National Legislation and relevant instruments of international law.

### **CLAUSE 13. Legal use of data**

13.1. The Exporter guarantees that Personal Data has been collected, processed and transferred to the Importer in accordance with the National Legislation.

### **CLAUSE 14. Transparency**

14.1. The Designated Party shall publish, on its website, a document containing easily accessible information written in simple, clear and accurate language on the conduction of the International Data Transfer, including at least information on:

- (a) the form, duration and specific purpose of the international transfer;
- b) the destination country of the transferred data;
- c) the Designated Party's identification and contact details;
- d) the shared use of data by the Parties and its purpose;
- e) the responsibilities of the agents who shall conduct the processing;
- f) the Data Subject's rights and the means for exercising them, including an easily accessible channel made available to respond to their requests, and the right to file a petition against the Exporter and the Importer before ANPD; and

Onward Transfers, including those relating to recipients and to the purpose of such transfer.

14.2. The document referred to in item 14.1. shall be made available on a specific website page or integrated, in a prominent and easily accessible format, to the Privacy Policy or equivalent document.

14.3. Upon request, the Parties shall make a copy of these Clauses available to the Data Subject free of charge, complying with trade and industrial secrecy.

14.4. All information made available to Data Subjects, under the terms of these Clauses, shall be written in Portuguese.

### **CLAUSE 15. Rights of the Data Subject**

15.1. The Data subject shall have the right to obtain from the Designated Party, as regards the Personal Data subject to the International Data Transfer governed by these Clauses, at any time, and upon request, under the terms of the National Legislation:

- confirmation of the existence of processing;
- b) access to data;
- c) correction of incomplete, inaccurate or outdated data;
- d) anonymization, blocking or erasure of unnecessary or excessive data or data processed in noncompliance with these Clauses and the provisions of National Legislation;
- e) portability of data to another service or product provider, upon express request, in accordance with ANPD regulations, complying with trade and industrial secrecy;
- f) erasure of Personal Data processed under the Data Subject's consent, except for the events provided in CLAUSE 20;
- g) information on public and private entities with which the Parties have shared data;
- h) information on the possibility of denying consent and on the consequences of the denial;

i) withdrawal of consent through a free of charge and facilitated procedure, remaining ratified the processing activities carried out before the request for elimination;

j) review of decisions taken solely on the basis of automated processing of personal data affecting their interests, including decisions aimed at defining their personal, professional, consumer and credit profile or aspects of their personality; and

k) information on the criteria and procedures adopted for the automated decision.

15.2. Data subject may oppose to the processing based on one of the events of waiver of consent, in case of noncompliance with the provisions of these Clauses or National Legislation.

15.3. The deadline for responding to the requests provided for in this Clause and in item 14.3 is 15 (fifteen) days from the date of the data subject's request, except in the event of a different deadline established in specific ANPD regulations.

15.4. In case the Data Subject's request is directed to the Party not designated as responsible for the obligations set forth in this Clause or in item 14.3., the referred Party shall:

a) inform the Data Subject of the service channel made available by the Designated Party; or

b) forward the request to the Designated Party as early as possible, to enable the response within the period provided in item 15.2.

15.5. The Parties shall immediately inform the Data Processing Agents with whom they have shared data with the correction, deletion, anonymization or blocking of the data, for them to follow the same procedure, except in cases where this communication is demonstrably impossible or involves a disproportionate effort.

15.6. The Parties shall promote mutual assistance to respond to the Data Subjects' requests.

## **CLAUSE 16. Security Incident Reporting**

16.1. The Designated Party shall notify ANPD and the Data Subject, within 3 (three) working days of the occurrence of a security incident that may entail a relevant risk or damage to the Data Subjects, according to the provisions of National Legislation.

16.2. The Importer must keep a record of security incidents in accordance with National Legislation.

## **CLAUSE 17. Liability and compensation for damages**

17.1. The Party which, when performing Personal Data processing activities, causes patrimonial, moral, individual or collective damage, for violating the provisions of these Clauses and of the National Legislation, shall compensate for it.

17.2. Data Subject may claim compensation for damage caused by any of the Parties as a result of a breach of these Clauses.

17.3. The defense of Data Subjects' interests and rights may be claimed in court, individually or collectively, in accordance with the provisions in relevant legislation regarding the instruments of individual and collective protection.

17.4. The Party acting as Processor shall be jointly and severally liable for damages caused by the processing activities when it fails to comply with these Clauses or when it has not followed the lawful instructions of the Controller, except for the provisions of item 17.6.

17.5. The Controllers directly involved in the processing activities which resulted in damage to the Data Subject shall be jointly and severally liable for these damages, except for the provisions of item 17.6.

17.6. Parties shall not be held liable if they have proven that:

a) they have not carried out the processing of Personal Data attributed to them;

b) although they did carry out the processing of Personal Data attributed to them, there was no violation of these Clauses or National Legislation; or

c) the damage results from the sole fault of the Data Subject or of a third-party which is not a recipient of the Onward Transfer or not subcontracted by the Parties.

17.8. Judicial proceedings for compensation for collective damages which intend to establish liability under the terms of this Clause may be collectively conducted in court, with due regard for the provisions in relevant legislation.

17.9. The Party which compensates the damage to the Data Subject shall have a right of recourse against the other responsible parties, to the extent of their participation in the damaging event.

#### **CLAUSE 18. Safeguards for Onward Transfer**

18.1. The Importer shall only carry out Onward Transfers of Personal Data subject to the International Data Transfer governed by these Clauses if expressly authorized, in accordance with the terms and conditions described in CLAUSE 3.

18.2. In any case, the Importer:

a) shall ensure that the purpose of the Onward Transfer is compatible with the specific purposes described in CLAUSE 2;

b) shall guarantee, by means of a written contractual instrument, that the safeguards provided in these Clauses shall be ensured by the third-party recipient of the Onward Transfer; and

c) for the purposes of these Clauses, and regarding the Personal Data transferred, shall be considered responsible for any eventual irregularities committed by the third-party recipient of the Onward Transfer.

18.3. The Onward Transfer shall also be carried out based on another valid modality of International Data Transfer provided in National Legislation, regardless of the authorization referred to in CLAUSE 3.

#### **CLAUSE 19. Access Request Notification**

19.1. The Importer shall notify the Exporter and the Data Subject of any Access Request related to the Personal Data subject to the International Data Transfer governed by these Clauses, except in the event that notification is prohibited by the law of the country in which the data is processed.

19.2. The Importer shall implement the appropriate legal measures, including legal actions, to protect the rights of the Data Subjects whenever there is adequate legal basis to question the legality of the Access Request and, if applicable, the prohibition of issuing the notification referred to in item 19.1.

19.3. To comply with both the ANPD's and the Exporter's requests, the Importer shall keep a record of Access Requests, including date, requester, purpose of the request, type of data requested, number of requests received, and legal measures implemented.

#### **CLAUSE 20. Termination of processing and erasure of data**

20.1. The Parties shall delete the Personal Data subject to the International Data Transfer governed by these Clauses after the end of the processing, within the scope and within the technical limits of the activities, with the retention authorized only for the following purposes:

a) compliance with a legal or regulatory obligation by the Controller;

b) study by a Research Body, ensuring, whenever possible, the anonymization of Personal Data;

c) transfer to a third party, provided that the requirements set forth in these Clauses and in the National Legislation are respected; and

d) exclusive use of the Controller, with access by third parties prohibited, and provided that the data are anonymized.

20.2. For the purposes of this Clause, processing of personal data shall cease when:

- a) the purpose set forth in these Clauses has been achieved;
- b) Personal Data are no longer necessary or pertinent to attain the intended specific purpose set forth in these Clauses;
- c) at the termination of the treatment period;
- d) Data Subject's request is met; and
- e) at the order of ANPD, upon violation of the provisions of these Clauses or National Legislation.

#### **CLAUSE 21. Data processing security**

21.1. Parties shall implement Security Measures which guarantee sufficient protection of the Personal Data subject to the International Data Transfer governed by these Clauses, even after its termination.

21.2. Parties shall inform, in SECTION III, the Security Measures implemented, considering the nature of the processed information, the specific characteristics and the purpose of the processing, the technology current state and the probability and severity of the risks to the Data Subjects' rights, especially in the case of sensitive personal data and that of children and adolescents.

21.3. The Parties shall make the necessary efforts to implement periodic evaluation and review measures to maintain the appropriate level of data security.

#### **CLAUSE 22. Legislation of country of destination**

22.1. The Importer declares that it has not identified any laws or administrative practices of the country receiving the Personal Data that prevent it from fulfilling the obligations assumed in these Clauses.

22.2. In the event of a regulatory change which alters this situation, the Importer shall immediately notify the Exporter to assess the continuity of the contract.

#### **CLAUSE 23. Non-Compliance with the Clauses by the Importer**

23.1. In the event of a breach in the safeguards and guarantees provided in these Clauses or being the Importer unable to comply with any of them, the Exporter shall be immediately notified, subject to the provisions in item 19.1.

23.2. Upon receiving the communication referred to in item 23.1 or upon verification of non-compliance with these Clauses by the Importer, the Exporter shall implement the relevant measures to ensure the protection of the Data Subjects' rights and the compliance of the International Data Transfer with the National Legislation and these Clauses, and may, as appropriate:

- a) suspend the International Data Transfer;
- b) request the return of the Personal Data, its transfer to a third-party, or its erasure; and
- c) terminate the contract.

#### **CLAUSE 24. Choice of forum and jurisdiction**

24.1. Brazilian legislation applies to these Clauses and any controversy between the Parties arising from these Clauses shall be resolved before the competent courts in Brazil, observing, if applicable, the forum chosen by the Parties in Section IV.

24.2. Data Subjects may file lawsuits against the Exporter or the Importer, as they choose, before the competent courts in Brazil, including those in their place of residence.

24.3. By mutual agreement, Parties may use arbitration to resolve conflicts arising from these Clauses, provided that the procedure is carried out in Brazil and in accordance with the provisions of the Arbitration Law.

**Section III - Security Measures**

*(NOTE: This Section should include details of the security measures implemented, including specific measures for the protection of sensitive data and children and adolescents. The measures may include the following aspects, among others, as indicated in the table below).*

(I) GOVERNANCE AND SUPERVISION OF INTERNAL PROCESSES:
(II) TECHNICAL AND ADMINISTRATIVE SECURITY MEASURES, INCLUDING MEASURES TO ENSURE THE SECURITY OF THE OPERATIONS CARRIED OUT, SUCH AS THE COLLECTION, TRANSMISSION AND STORAGE OF DATA:

Local, data.

Signatures.