

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

## TABLE OF CONTENTS

<b>1. PRELIMINARY CONSIDERATIONS AND PURPOSE</b> .....	<b>3</b>
<b>2. IMPORTANT CONCEPTS AND DEFINITIONS</b> .....	<b>4</b>
<b>3. GENERAL UNDERTAKINGS</b> .....	<b>5</b>
3.1. <i>DUTIES</i> .....	5
3.2. <i>PROHIBITIONS</i> .....	6
<b>4. SPECIFIC UNDERTAKINGS</b> .....	<b>8</b>
4.1. <i>UNDERTAKINGS OF PROCESSORS</i> .....	8
4.2. <i>UNDERTAKINGS OF CONTROLLERS</i> .....	10
<b>5. OTHER ISSUES:</b> .....	<b>12</b>
5.1. <i>NON-COMPLIANCE WITH THE STANDARD</i> .....	12
5.2. <i>CONTACT CHANNEL</i> .....	12
5.3. <i>UPDATES</i> .....	12

## 1. PRELIMINARY CONSIDERATIONS AND PURPOSE

The CPFL Energia Group - which, for the purposes of this document, corresponds to the holding CPFL Energia S.A and all its direct and indirect subsidiaries - is strongly committed to ethics, integrity and security of individuals and information assets related to its commercial activities, which involves valuing personal data privacy and protection.

In this sense, in view of the Brazilian General Data Protection Law ("LGPD"), we have adopted - including on an ongoing basis - a series of measures, mechanisms and procedures aimed at complying with standards and good practices on the subject.

As part of these efforts, we base the choice and hiring of suppliers, service providers and partners of the CPFL Energia Group (for ease of understanding, they will be hereinafter referred to as "supplier(s)") on technical, strategic, economic, professional and ethical criteria that, in addition to the guidelines outlined in our Code of Ethical Conduct for Suppliers (<http://portalmulti.cpfl.com.br/sites/portaldenoticias/programa-de-integridade/Documents/2.3%20Codigo%20conduta%20Etica%20Fornecedores.pdf>) also cover specific requirements in terms of personal data privacy and protection.

Thus, this Personal Data Protection Standard aims **to establish the minimum conditions required by the CPFL Energia Group for the execution of contracts involving the processing of personal data, also providing practical and clear guidelines regarding the expected conduct of our suppliers, service providers and partners.**

Note that all the rules contained in this document are requirements for the partnership with the CPFL Energia Group to take place, and must be interpreted together with the contract, commercial proposal, agreement or instrument used to carry out the legal business with us.

Thus, **all those who take the position of suppliers, service providers or partners of the CPFL Energia Group must also comply with the provisions of this Standard, also ensuring that not only the contracting organization, but all its members, employees and third parties that provide support in the performance of their activities also follow the rules presented herein.**

We recognize that the topic is still being assimilated and matured by the various agents in the Brazilian market, and a proactive, responsible and joint action by all companies is essential for the construction of a harmonious and robust scenario on the subject. Therefore, we welcome comments, questions and suggestions for improvement of this document, which may be sent to our Data Protection Management - directly at [privacidade@cpfl.com.br](mailto:privacidade@cpfl.com.br) -, which will evaluate and answer the questions, helping, when necessary, to clarify topics provided for in this Standard.

## 2. IMPORTANT CONCEPTS AND DEFINITIONS

For a better understanding of this Standard, we present below some important concepts and definitions in terms of personal data privacy and protection:



### PERSONAL DATA

All information that can directly (e.g.: name, ID card (RG) and Individual Taxpayer's Register (CPF)) or indirectly (e.g.: IP address, geolocation and device information) identify or make identifiable a natural person, both on and off the internet.



### SENSITIVE DATA

Those related to racial or ethnic origin, religious conviction, political opinion, membership of a union or organization of a religious, philosophical or political nature, in addition to data relating to health, sex life, genetic or biometric data.



### PROCESSING

Any activity or set of activities carried out with personal data, whether in a physical or digital environment, such as collection, registration, access, visualization, dissemination, sharing, storage, deletion etc.



### DATA SUBJECT

Individual to whom the personal data relates. In contractual relationships entered into by the CPFL Group, personal data may relate to customers and prospects, employees and their dependents, shareholders, candidates, among others.



### DATA PROTECTION OFFICER

Person appointed by the processing agent to act as the organization's point of contact in matters relating to personal data privacy and protection, assisting in communication with data subjects, the ANPD (Brazilian Data Protection Authority) and other agents.



### LEGAL BASIS

Events set forth by the LGPD that authorize the performance of personal data processing activities for specific purposes and provided that duly informed to the data subjects.



### CONTROLLER

Individual or legal entity, governed by public or private law, that makes the decisions referring to the processing of personal data.



### PROCESSOR

Individual or legal entity, governed by public or private law, that performs the personal data processing on behalf of the controller.

### 3. GENERAL UNDERTAKINGS

The CPFL Energia Group reinforces and guarantees that any processing activity will meet the purposes set out in the contract, undertaking to act in accordance with the applicable legislation - including, but not limited to the LGPD -, in order to ensure that all its provisions are lawful and do not violate current legislation.

In the same sense, for the execution of a contract between any companies that are part of the CPFL Energia Group, their suppliers, service providers or partners - and whenever the activity(ies) agreed in the contract give rise to personal data processing - it is mandatory to observe the following rules and general undertakings (without prejudice to the principles contained in the LGPD, other separate laws and the guidelines issued by the Brazilian Data Protection Authority - ANPD):

#### 3.1. DUTIES

The duties of every supplier, service provider and partner of the CPFL Energia Group are:

##### 1. USE MINIMUM DATA

Use only the personal data that is minimally necessary to achieve the business purpose, being solely responsible for the processing of personal data carried out in disagreement with the laws and standards that govern the contract

##### 2. GUARANTEE THE SECURITY OF THE INFORMATION PROCESSED

- Take technical, administrative and information security measures necessary to protect personal data and prevent (accidental or illicit) misuse and unauthorized access to information processed under the contract.
- Ensure, within its technical and operational possibilities, the inviolability, confidentiality, availability and integrity of personal data, with the adoption of mechanisms such as those exemplified below or similar one (among others):
  - ✓ control and restriction of access through the definition of authorized persons and persons responsible for the processing;
  - ✓ information encryption;
  - ✓ structuring of governance for personal data protection with contingency and risk mitigation plans.

##### 3. DOCUMENT ACTIONS AND KEEP RECORD OF PROCESSING OPERATIONS

##### 4. COOPERATE WITH THE CPFL GROUP FOR COMPLIANCE WITH THE LAW AND PROPER PERFORMANCE OF THE CONTRACT

Keep a detailed inventory of the accesses to personal data and the records of connection and access to applications, containing the time, duration, identity of the employee or person responsible for the access and the file accessed, including when such access is made to comply with legal obligations or determinations defined by competent authority;

Keep a record of all personal data processing operations carried out, with detailed and updated information, also covering indication of international transfers of personal data that may have been carried out, country/organization of destination and guarantees and mechanisms adopted to meet applicable legal requirements.

Establish a cooperative and proactive relationship with the CPFL Energia Group to resolve issues involving the processing of personal data related to the performance of the contract, providing all the necessary documentation to demonstrate compliance with the obligations established in the contract and in the applicable legislation, maintaining a contact channel within the organization authorized to answer queries about the processing of personal data.

### 5. OBSERVE NECESSARY REQUIREMENTS FOR CROSS-BORDER TRANSFER

Ensure that the personal data cross-border transfer - if it is necessary solely and exclusively for the provision of services established in the contract - is carried out in accordance with one of the mechanisms provided for by the LGPD and other applicable data protection laws and regulations, also observing guidelines that may be issued by the ANPD.

Ensure that the overseas Personal Data recipient:

- ✓ Complies with the data processing rules set in the Brazilian General Data Protection Law (Federal Law 13709/2018);
- ✓ Takes the necessary technical and administrative measures to protect the Personal Data against destruction, change and/or unauthorized disclosure or access;
- ✓ Ensures that any third party that may have access to Personal Data also adopts the same technical and administrative measures adopted by such third party to perform the activities; and
- ✓ Sends, on demand, information related to the processing of personal data in order to comply with regulatory bodies demands (e.g. ANPD, Aneel) or for defense before judicial or administrative bodies and to comply with the rights of the Personal Data holders.

### 6. PROVIDE ASSISTANCE TO THE CPFL GROUP TO MEET OFFICIAL REQUIREMENTS

Provide assistance to the CPFL Energia Group company, within the limits of the obligations imposed by the LGPD or other applicable regulations, if the ANPD or any other governmental authority (Judicial Branch, Prosecution Office, ANEEL, Senacon, Procon etc.), or even the data subject requests information regarding the compliance with the processing of personal data arising from the contract, respecting the deadline indicated punctually by the CPFL Energia Group company.

If it receives orders and/or official communications (either from judicial bodies, government authorities, the Prosecution Office, Procon, among others) to reveal any information arising from the signed contract, the supplier must immediately notify the CPFL Energia Group company regarding the request and its terms. If it is legally unable to inform the CPFL Energia Group company, the supplier must comply with the command (provided it is lawful), informing about the action taken at the first possible opportunity.

## 3.2 PROHIBITIONS

Any supplier, service provider and partner of the CPFL Energia Group is prohibited from:

### 1. IMPROPER SHARING

### 2. VIOLATION OF THE LAW

---

Transfer and/or share the personal data to which it has access to third parties other than employees, agents, contractors and subcontractors (if any) assigned to perform the activities provided for in the contract.

Failing to observe minimum legal requirements applicable to the processed personal data cross-border transfer under the contract entered into, as well as binding guidelines issued and/or approved by the Brazilian Data Protection Authority (ANPD).

---

### **3. USING INADEQUATE MEANS**

---

Sharing documents of any kind or nature or exchanging information that contains personal data arising from this contract by electronic means not approved by the information security area of the company that is part of the CPFL Energia Group.

---

## 4. SPECIFIC UNDERTAKINGS

In addition to the general undertakings mentioned above, our suppliers, service providers and partners must be aware of the specific standards presented below, depending on the category of processing agent in which they fall (whether **CONTROLLERS** or **PROCESSORS**), according to the activity and relationship established with the CPFL Energia Group and the definitions below:



### CONTROLLER

Individual or legal entity responsible for making relevant decisions (at a strategic level) on the processing of personal data established in the contract, defining aspects such as the purpose of the processing, the data involved in the activity, the storage time of the personal data etc.



### PROCESSOR

Individual or legal entity that acts in the processing of personal data, following the lawful guidelines determined by the opposing party in the contract, not being able to use for their own benefit personal data that may be accessed. It can make decisions only at an operational level, without having the autonomy to define the form and purpose of using the personal data transmitted as a result of the contract.

### 4.1. UNDERTAKINGS OF PROCESSORS

In the capacity of PROCESSORS, the suppliers, service providers and partners of the CPFL Energia Group must observe the following specific undertakings, without prejudice to other provisions defined in the contract, legislation and applicable regulations:

#### 1. ACT ACCORDING TO INSTRUCTIONS ISSUED BY THE CPFL ENERGIA GROUP

Carry out processing activities strictly in accordance with the guidelines and instructions of the CPFL Energia Group company, never using the personal data to which they have access in fulfilling the contract for their own benefit or that of others, for commercial purposes or advantages and purposes not provided for in the instrument signed.

If it disagrees with any instruction or guidance received, the supplier must notify the CPFL Energia Group company in writing, justifying the reasons for its disagreement.

#### 2. ENGAGE THIRD PARTIES ONLY WHEN STRICTLY NECESSARY

Transfer and/or share information obtained as a result of the relationship entered into with the CPFL Energia Group only when the sharing is strictly necessary to fulfill the purpose of the contract, being aware that the CPFL Energia Group may, at its sole discretion, oppose the contracting of sub-processor third parties, without any compensation being due to the parties involved.

#### 3. BE LIABLE FOR THIRD PARTIES ENGAGED IN ACTIVITIES

Ensure that all those who may be engaged in activities related to the fulfillment of the contract are subject to the same level of obligations indicated by the legislation and by the CPFL Energia Group, assuming full responsibility for the acts performed by third parties involved in the activities.

#### 4. TRANSFER OBLIGATION

Ensure that the obligations of personal data secrecy and protection extend to its employees, agents, contractors and subcontractors (if any), ensuring that the people designated to perform the activities are bound by a confidentiality obligation in relation to the personal data to which they have access.

#### 5. ENSURE INTEGRITY

#### 6. MEET REQUEST



Ensure the integrity of the information received, not rectifying, erasing or restricting the processing of personal data on its own initiative, but only with instructions duly documented by the CPFL Energia Group company.

Fill in any and all material requested by the CPFL Energia Group company related to the applicable security and data protection standards (self-assessment), within the deadline indicated by the CPFL Energia Group company, being responsible for the veracity of the information declared in such documents and making itself available to respond to requests, interviews, audits and 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 fulfillment of the contracted subject matter, immediately report it to the CPFL Energia Group company, with a maximum tolerance of 1 business day from the date of the event, through communication to the data protection officer of the CPFL Group, which must contain, at least, the following information: (a) Name/corporate name of the Contracting Party and the respective contract manager; (b) Name/corporate name of the Contractor and the respective contract manager; (c) type of contract, date of execution and summary of the contracted subject matter; (c) (sic) date and time of the incident; (d) date and time of the awareness; (e) list of the types of personal data affected by the incident; (f) number of affected users (Incident volume) and, whenever possible, the list of these individuals; (e) list of data subjects affected; (f) contact details of the Data Protection Officer or, if there is no Data Protection Officer, the person from whom it is possible to obtain further information about what happened; (g) description of the possible consequences of the incident; (h) actions taken to mitigate adverse effects and prevent their recurrence; (i) measures being taken to repair the damage.

If you do not have all the information listed above at the time of sending the communication, you must complete the communication as soon as you have the necessary information to provide clarification on what happened.

## **8. TRANSFER REQUEST**

Upon receiving a request for rights guaranteed by the LGPD from data subjects or third parties (including public authorities) in relation to the personal data processed as a result of the contract, you must inform the data subject that only the CPFL Group can respond to their request, indicating to the data subject the channel to exercise the rights arising from the processing of data, and observing the provisions of the Privacy Notice (<https://www.cpfl.com.br/institucional/privacidade/aviso-de-privacidade/Paginas/default.aspx>) immediately send such request to the CPFL Energia Group company.

## **9. BE LIABLE**

Be liable for any (direct or indirect) damage resulting from the undue processing of personal data that is exclusively attributable to it - such as non-compliance with the laws and regulations governing data protection related to its segment of activity or the rules/determinations of the CPFL Group, security incident situations involving personal data, acts that exceed the limits of what is necessary in relation to the processing of personal data for the fulfillment of the contract, among others -, and must reimburse any judicial or extrajudicial expenses, administrative fines and losses and damages, provided that the CPFL Energia Group will be entitled to impleader as provided for in article 125, II of the Brazilian Civil Procedure Code.

## **10. DELETE DATA AT THE END**

Proceed with the definitive deletion (including any copies) of personal data processed as a result of the contract after the termination of the contract or when requested by the CPFL Energia Group company - unless there is a legal basis for preserving the information, which must be eliminated as soon as the retention is no longer necessary under the terms of the applicable law -, sending a written record proving the deletion of the information from its databases and electronic systems and/or physical files.

## 4.2. UNDERTAKINGS OF CONTROLLERS

In certain situations, the business model and the performance of the CPFL Energia Group's suppliers, service providers and partners with members of the CPFL Energia Group will require such companies to make certain decisions regarding the personal data processing operations necessary to fulfill the subject matter of the contract, which causes both contracting parties to be considered CONTROLLERS pursuant to the law.

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

### 1. ENSURE QUALITY, LEGITIMACY AND LEGALITY

Ensure the quality of personal data and transparency about the processing in relation to the data subject, as well as meeting requests made directly by the data subject, by the contracting company(ies) that are part of the CPFL Energia Group, by the ANPD or any other governmental authority (Judicial Branch, Prosecution Office, Aneel, Senacon, Procon, among others).

### 2. ENSURE RIGHTS TO PERSONAL DATA SUBJECTS

Ensure to the personal data subject their rights set forth in article 18 of the LGPD (such as confirmation of the existence of processing, access, correction, revocation of consent, objection) to the extent of their participation in the processing of personal data arising from the contract.

### 3. TAKE THE APPROPRIATE MEASURES IN CASE OF INCIDENTS

Take the measures provided for in the applicable legislation - especially with regard to notice to the data subjects and the Brazilian Authority - in the event of a security incident involving personal data that occurs in the performance of their activities, informing the CPFL Energia Group company about the event, by means of a communication containing, at least, the following information: (a) date and time of the incident; (b) date and time of acknowledgment by the Party; (c) list of the types of personal data affected by the incident; (d) number of affected users (incident volume) and, if possible, the list of these individuals; (e) contact details of the Party's Data Protection Officer or, if there is no Data Protection Officer, the person from whom it is possible to obtain further information about what happened; (f) description of the possible consequences of the Incident for the other Party; (g) measures being taken to mitigate risks.

If you do not have all the information listed at the time of sending the communication, you must send it gradually, in order to ensure the greatest possible celerity, given that the initial communication must be carried out within a maximum period of 1 business day from the knowledge of the incident, unless a shorter period is stipulated by the ANPD.

### 4. BE LIABLE FOR REPAIRING THE DAMAGE CAUSED

The Controller is responsible for all the processing of personal data that it carries out in its commercial activities, as well as for its appropriateness (compliance with legislation and security guarantee), answering to the Brazilian Data Protection Authority or any other body that may request information related to its processing activities, unless it has not carried out the processing, violated the law or in cases where any damage results from the exclusive fault of the data subject or third parties.

In the event that it is a supplier of personal data, it is liable, including for the origin of the information shared (when these are the subject matter of the contract or necessary for the performance of the contract), for the security of personal information and for all obligations arising from its activity and also from the laws and regulations that govern the protection of personal data.

## 5. ENSURE ADEQUATE SECURITY AND PREVENTION STANDARDS

To ensure an adequate level of security for the processing of the information processed as a result of the contract, the supplier must, among other things:

- Have strategies to protect login authentication;

- Ensure access traceability (servers, backend, edge, chatbot platform, management platform, among any other databases and software used);
- Enable coding, following the SDLC (Security Development Life Cycle) model, as well as perform vulnerability/EHT tests;
- Ensure that no personal data arising from the performance of the contract will be stored, transported or kept on a laptop or any other mobile device or storage media (including USB, USB sticks, DVDs and CDs), unless such devices are encrypted.

In case of international transfer or processing of personal data out of Brazil through service providers, ensure that they comply with the same obligations provided for in this topic.

---

## 5. OTHER ISSUES:

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

### 5.1. NON-COMPLIANCE WITH THE STANDARD

Failure to comply with one or more rules of this Personal Data Protection Standard, as well as other contractual instruments entered into between the parties, may result in the immediate termination of the contractual relationship without any amount being owed by the CPFL Energia Group in any way, in addition to compensatory contractual fines, payment judgments applicable by the Judiciary Branch and administrative sanctions imposed by regulatory bodies (such as consumer protection agencies and the ANPD), which range from warnings to payment of fines calculated based on billing, disclosure of the violation and suspension of activities.

It is worth remembering that the provisions contained in this Standard will continue to be enforceable and to take effect as long as there is any processing of personal data, even after the end 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 actions that seek to align suppliers with its business principles. Thus, the provisions of this Standard must be observed in conjunction with the other policies and rules established in the context of suppliers' relations, which are available on <https://www.cpfl.com.br/institucional/fornecedores/Paginas/default.aspx>.

In case of doubts about this Standard or about your obligations and responsibilities as a personal data processing agent, or if you deem that you are unable to comply with the provisions of the applicable legislation and the guidelines established by the CPFL Energia Group, contact our Data Protection Management directly at [privacidade@cpfl.com.br](mailto:privacidade@cpfl.com.br)

### 5.3. UPDATES

This Personal Data Protection Standard for Suppliers, Service Providers and Partners may be amended at any time, and it is important that the recipients of this document undertake to keep up to date with their obligations, consulting, whenever possible, the website of the CPFL Energia Group to check the history of changes to this document.

In the event of changes that materially modify this Standard and cause significant impacts to the processing operations and relationships entered into by the CPFL Energia Group and its suppliers, service providers and partners, we will use reasonable measures to inform you of the update of this document, favoring the communication channel most widely used for interaction with the public in question.

Last update: 06/30/2021