PURPOSE:	To have a policy that describes the organization and main guidelines, principles and responsibilities of ENGIE Energía Perú S.A. (hereinafter, "EEP") to provide adequate treatment of the Personal Data to which it may have access in the framework of the development of its activities. In this regard, the purpose of this policy is to comply with the provisions contained in: (i) Law No. 29733, Personal Data Protection Law, as well as its Regulations and amendments (hereinafter, the "Law"); as well as in (ii) the ENGIE Group Policy called "Group Data Privacy Policy" (hereinafter, the "ENGIE Group Policy").
SCOPE:	This policy shall apply to the processing of Personal Data contained in the Personal Data Banks owned by EEP (whether the processing of such Personal Data is carried out by EEP directly and/or through third parties) that is carried out in the national territory. In this regard, this policy must be complied with by all EEP employees and contractors. Additionally, this document describes the internal procedures to be followed in the following cases: 1. Registration or modification of the Personal Data Bank before the National Authority for the Protection of Personal Data (hereinafter, the "APDP"). 2. Exercise of ARCO Rights by the Personal Data Subject. 3. Revocation of the Personal Data Subject's consent. 4. Response to incidents related to the processing of Personal Data.
DEFINITIONS:	For the purposes of this policy, the following definitions shall apply: 1. **Personal Data Bank:** Organized set of personal data, automated or not, regardless of the support, whether physical, magnetic, digital, optical or others that are created, whatever the form or modality of its creation, formation, storage, organization and access owned by EEP. 2. **Personal Data:** Information about a natural person that identifies him/her or makes him/her identifiable through means that can be reasonably used. 3. **Sensitive Data:** Biometric data that by itself can identify the owner; data referring to racial and ethnic origin; economic income; political, religious, philosophical or moral opinions or convictions; union membership; and information related to health or sexual life. 4. **ARCO Rights:** Rights of access, rectification, cancellation or opposition to the processing of personal data exercised by the owner of the personal data in accordance with the provisions of the Law. 5. **Security Incidents:** Any situation related to the processing of personal data in which there is suspicion or certainty of (i) the alteration of personal data, (ii) the loss of personal data, as well as (ii) the unauthorized processing of or access to personal data. 6. **Adequate Level of Protection for Personal Data:** A level of protection that includes at least the recording of and compliance with the guiding principles of the Law, as well as technical security and confidentiality measures, appropriate to the category of data in question. 7. **Personal Data Protection Management System:** Set of resources, activities, processes, policies and strategies, structured in such a way as to ensure a Sufficient Level of Protection of Personal Data processed for the performance of EEP's activities, as provided for in the Law and ENGIE Group Policy. 8. **Personal Data Owner or Data Subject:** The natural person to whom the Personal Data corresponds. 9. **Owner of the Personal Data Bank or Data Controller:** The natural person, private legal entity or public entity that determines the purpose and content of the Personal Data Bank, its processing and security measures. For the purposes of this policy, EEP shall be understood as the Data Controller. 10. **Transfer of Personal Data:** Any transmission, supply or manifestation of Personal Data, of national or international character, to a private legal entity, to a public entity or to a natural person other than the Data Subject. 11. **Processing of Personal Data:** Any operation or technical procedure, automated or not, that allows the collection, recording, organization, storage, conservation, elaboration, modification, extraction, consultation, use, blocking, deletion, communication by transfer or distribution or any other form of processing that facilitates the access, correlation or interconnection of Personal Data.
ROLES	For the purposes of this policy, the following roles shall apply: A. ***Data Protection Manager*** **("DPM"):** The DPM shall perform the following functions: ✓ Ensure the effective implementation of the ENGIE Group Policy and the Law, and monitor its application. ✓ Support compliance with the provisions of the Law and the Group Policy regarding the processing of personal data. ✓ Ensure the development and implementation of the plan and training EEP staff on this policy. ✓ Inform, recommend and if necessary alert on incidents that may occur in relation to the protection of Personal Data. ✓ To prepare an annual report on its activities and communicate it to the Ethics Committee.

	✓ Inform the Ethics Committee about any incident involved. ✓ Sign the official documents related to Personal Data Protection required by Law and Group Policy. The DPM may be supported by one or more Data Protection Experts (DPE). B. ***Data Protection Expert or Data Protection Correspondance*** ("DPE"): Person(s) appointed by the DPM as support in the performance of its duties. C. **Personal Data Bank Administrator ("Administrator"):** Is the person responsible for the macro-process or process from which the processing of Personal Data is derived, who will be responsible for describing the processing of Personal Data by filling out the Security Sheet, as well as for following up the compliance with the security measures implemented to ensure the adequate processing of Personal Data. The Governance of this policy applicable to EEP is attached as Annex II.
MAIN OBLIGATIONS RELATED TO THE PROTECTION OF PERSONAL DATA:	EEP establishes the following guidelines in order to comply with the Law and the ENGIE Group Policy: 1. **Compliance:** The processing of Personal Data shall be carried out in accordance with the demands, requirements, deadlines and other provisions of the Law and the ENGIE Group Policy[1]. At all times that the processing of Personal Data is carried out, compliance with the provisions of the Law and the ENGIE Group Policy must be observed. Macro-processes or processes involving the processing and/or transfer of Personal Data must have the approval of the DPM or DPE. 2. **Consent and Purpose:** The Personal Data to which we have access may not be processed (including the prohibition to be transferred to third parties) without the prior consent of the Personal Data Owner, unless the exceptions provided by Law. Likewise, Personal Data may only be processed for the purposes for which they were obtained and previously authorized. Once the purpose for which the processing of the Personal Data was authorized has been fulfilled, and as long as there is no obligation to keep such Personal Data, the Personal Data may be deleted.
	3. **Transborder Flow of Personal Data:** For the transfer of Personal Data outside the national territory, it shall be observed that the recipient country maintains a Sufficient Level of Protection for the Personal Data and that the recipient (importer of the Personal Data) assumes the same obligations as the Data Controller (exporter of the Personal Data). 4. **Personal Data Bank:** To date, EEP has the following Personal Data Banks: | # | Name of the Data Bank | Associated process | |---|---|---| | 01 | Employees | Personnel Administration | | 02 | Suppliers | Supplier Management | | 03 | Access | Property Security Management | | 04 | Medical Records | SSO Management | If the existence of a Personal Data Bank is identified, the following should be considered: a. In case of identifying a new processing of personal data, the BPO in charge of the process will fill out the "Form for new processing of Personal Data" included in the "Personal Data Protection" section of the SIMPLE Portal. Business Quality (BQ) will use the information described in the form to evaluate together with Legal and other areas involved, whether or not it is necessary to submit to the Peruvian Authority for the Protection of Personal Data (APDP), the creation of a new Personal Data Bank or the modification of an existing one. b. The Administrator shall proceed with the description of the Personal Data Bank, for which the following information shall be filled in the Security Sheet: • General information and purpose of the Personal Data Bank. • Personal Data subject to processing (specifying whether the transfer of such information is carried out). • Flow of the processing of the Personal Data. • Security measures of the Personal Data Bank. • Consent and cross-border flow (if applicable).

[1] The processing of Personal Data carried out by EEP is subject to supervision, control, and imposition of sanctions, in case of non-compliance, by the competent authority.

	c. In the case of a Personal Data Bank containing Sensitive Data, its creation can only be justified if its purpose, in addition to being legitimate, is specific and in accordance with the activity or purpose for which it is required. d. Personal Data Banks must be registered before the APDP and must have security measures in place. e. The Administrator shall be in charge of monitoring the compliance with the security measures implemented to ensure the adequate treatment of the Personal Data of the processes under its responsibility. f. The DPM and the DPE shall provide support to the Administrators in their functions to maintain the proper functioning of the Personal Data Protection Management System. **5. <u>Security Measures:</u>** Personal Data Banks must have security measures (organizational, technical and legal) that enable their security and prevent their alteration, loss, treatment or unauthorized access, for which the provisions of Supreme Decree No. 003-2013-JUS, as well as the Information Security Guidelines, approved by Directorial Resolution No. 019-2013-JUS/DGPDP, may be considered. **6. <u>Monitoring:</u>** To ensure compliance with this policy and the requirements of the Law and the ENGIE Group Policy, the DPM, with the support of the DPE, will lead annual reviews to verify the proper treatment of Personal Data used in each EEP process and the operation of the Personal Data Protection Management System.
PROCEDURES:	For a better organization in the fulfillment of roles during the term of this policy, Annex I describes the steps to be followed in the following procedures: "Registration or modification of Personal Data Bank before the APDP". "Attention of ARCO Rights request". "Revocation of the Personal Data Subject's Consent". "Response to Personal Data Incidents".

DISCLAIMER: This document is a translation of the original version in Spanish and is for information purposes only. In case of any discrepancy between this English version and the original in Spanish, the Spanish version will prevail.