



## POLITICA DE PROTECCIÓN DE DATOS PERSONALES

<b>OBJETIVO:</b>	<p>Contar con una política que describa la organización y principales lineamientos, principios y responsabilidades de ENGIE Energía Perú S.A. (en adelante, "EEP") para dar un adecuado tratamiento de los Datos Personales a los que pudiera tener acceso en el marco del desarrollo de sus actividades.</p> <p>En ese sentido, la presente política tendrá por objetivo el cumplimiento de las disposiciones contenidas en: (i) la Ley N° 29733, Ley de Protección de Datos Personales, así como su Reglamento y modificatorias (en adelante, la "Ley"); así como, en (ii) la Política del Grupo ENGIE denominada "Group Data Privacy Policy" (en adelante, la "Política del Grupo ENGIE").</p>
<b>ALCANCE:</b>	<p>La presente política será aplicable al tratamiento de los Datos Personales contenidos en los Bancos de Datos Personales de titularidad de EEP (sea que el tratamiento de dichos Datos Personales lo realice EEP de manera directa y/o a través de terceros) que se realice en el territorio nacional. En ese sentido, la presente política deberá ser cumplida por todos los colaboradores y contratistas de EEP.</p> <p>Adicionalmente, en el presente documento se describe los procedimientos internos a seguir en los siguientes casos:</p> <ol style="list-style-type: none"><li>1. Inscripción o modificación del Banco de Datos Personales ante la Autoridad Nacional de Protección de datos Personales (en adelante, la "APDP").</li><li>2. Ejercicio de Derechos ARCO por parte del Titular de Datos Personales.</li><li>3. Revocación del consentimiento del Titular de Datos Personales.</li><li>4. Respuesta a incidentes vinculados al tratamiento de Datos Personales.</li></ol>
<b>DEFINICIONES:</b>	<p>Para efectos de la presente política serán aplicables las siguientes definiciones:</p> <ol style="list-style-type: none"><li>1. <b>Banco de Datos Personales:</b> Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso de titularidad de EEP.</li><li>2. <b>Datos Personales:</b> Información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.</li><li>3. <b>Datos Sensibles:</b> Datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual.</li><li>4. <b>Derechos ARCO:</b> Derechos de acceso, rectificación, cancelación u oposición de tratamiento de datos personales ejercido por el titular de los datos personales conforme a lo establecido en la Ley.</li><li>5. <b>Incidentes de Seguridad:</b> Cualquier situación relacionada con el tratamiento de datos personales en la que se sospeche o se tenga certeza de (i) la alteración de los datos personales, (ii) la pérdida de los datos personales, así como (iii) el tratamiento o acceso no autorizado de los datos personales.</li><li>6. <b>Nivel Suficiente de Protección para los Datos Personales:</b> Nivel de protección que abarca por lo menos la consignación y el respeto de los principios rectores de la Ley, así como medidas técnicas de seguridad y confidencialidad, apropiadas según la categoría de datos de que se trate.</li><li>7. <b>Sistema de Gestión de Protección de Datos Personales:</b> Conjunto de recursos, actividades, procesos, políticas y estrategias, estructuradas de tal manera que aseguran un Nivel Suficiente de Protección de los Datos Personales tratados para el desempeño de las actividades de EEP, según lo dispuesto en la Ley y Política del Grupo ENGIE.</li><li>8. <b>Titular de Datos Personales o Data Subject:</b> Es la persona natural a quien corresponde los Datos Personales.</li><li>9. <b>Titular del Banco de Datos Personales o Data Controller:</b> Es la persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del Banco de Datos Personales, el tratamiento de estos y las medidas de seguridad. Para efectos de la presente política se entenderá a EEP como el titular del banco de datos personales.</li><li>10. <b>Transferencia de Datos Personales:</b> Toda transmisión, suministro o manifestación de Datos Personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una entidad pública o a una persona natural distinta del Titular de Datos Personales.</li><li>11. <b>Tratamiento de Datos Personales:</b> Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los Datos Personales.</li></ol>
<b>ROLES</b>	<p>Para efectos de la presente política serán aplicables los siguientes roles:</p> <ol style="list-style-type: none"><li>A. <b>Data Protection Manager ("DPM"):</b> El DPM desempeñará las siguientes funciones:<ul style="list-style-type: none"><li>✓ Asegurar la implementación efectiva de la Política del Grupo ENGIE y de la Ley, y controlar su aplicación.</li></ul></li></ol>



## POLITICA DE PROTECCIÓN DE DATOS PERSONALES

- ✓ Apoyar el cumplimiento de lo establecido en la Ley y en la Política del Grupo respecto al tratamiento de los datos personales.
- ✓ Velar por la elaboración y cumplimiento del plan las capacitaciones al personal de EEP sobre la presente política.
- ✓ Informar, recomendar y de ser necesario alertar sobre los incidentes que pueden presentarse en relación con la protección de Datos Personales.
- ✓ Elaborar un reporte anual sobre sus actividades y comunicarlo al Comité de Ética.
- ✓ Informar al Comité de Ética sobre cualquier incidente involucrado.
- ✓ Firmar los documentos oficiales relacionados con Protección de Datos Personales exigidos por la Ley y la Política del Grupo.

El DPM podrá contar con el soporte de uno o más Data Protection Expert (DPE).

- B. **Data Protection Expert o Data Protection Correspondance (“DPE”)**: Persona(s) nombrada(s) por el DPM como soporte en el cumplimiento de sus funciones.
- C. **Administrador del Banco de Datos Personales (“Administrador”)**: Es la persona responsable del macroproceso o proceso del cual se deriva el tratamiento de Datos Personales, quien será el responsable de describir el tratamiento de los Datos Personales a través del llenado de la Ficha de Seguridad, así como de efectuar el seguimiento al cumplimiento de las medidas de seguridad implementadas para asegurar el adecuado tratamiento de los Datos Personales.

Se adjunta, como Anexo II, el Governance de la presente política aplicable a EEP.

EEP establece los siguientes lineamientos con la finalidad de cumplir con la Ley y la Política del Grupo ENGIE:

**PRINCIPALES OBLIGACIONES VINCULADAS A LA PROTECCIÓN DE DATOS PERSONALES:**

1. **Cumplimiento:**  
El tratamiento de Datos Personales se deberá efectuar de conformidad con las exigencias, requerimientos, plazos y demás establecido en la Ley y la Política del Grupo ENGIE<sup>1</sup>.  
En todo momento que se realice el tratamiento de Datos Personales se deberá observar el cumplimiento de lo establecido en Ley y la Política del Grupo ENGIE.  
Los macroprocesos o procesos que involucren el tratamiento y/o transferencia de Datos Personales deberán contar con la aprobación del DPM o DPE.
2. **Consentimiento y Finalidad:**  
Los Datos Personales a los que se tenga acceso no podrán ser tratados (incluyendo la prohibición de ser transferidos a terceros) sin el previo consentimiento del Titular de los Datos Personales, salvo por las excepciones prevista en Ley.  
Asimismo, los Datos Personales sólo podrán ser tratados para los fines que motivaron su obtención y previamente autorizados.  
Luego de que se haya cumplido con la finalidad para la cual fue autorizado el tratamiento de los Datos Personales, y en tanto no exista obligación de conservar dichos Datos Personales, se podrá proceder con su eliminación.

3. **Flujo transfronterizo de Datos Personales:**

Para la transferencia de Datos Personales fuera del territorio nacional se deberá observar que el país destinatario mantenga un Nivel Suficiente de Protección para los Datos Personales y que el receptor (importador de los Datos Personales) asuma las mismas obligaciones del Titular del Banco de Datos Personales (exportador de los Datos Personales).

4. **Banco de Datos Personales:**

A la fecha, EEP cuenta con los siguientes Bancos de Datos Personales:

#	Nombre del Banco de Datos	Proceso asociado
01	Trabajadores	Administración de Personal
02	Proveedores	Gestión de Proveedores
03	Accesos	Gestión de Seguridad Patrimonial
04	Historias Clínicas	Gestión de SSO

En caso de identificarse la existencia de un Banco de Datos Personales se deberá considerar lo siguiente:

- a. En caso de identificar un nuevo tratamiento de datos personales, el BPO del proceso encargado llenará el “Formulario para nuevo tratamiento de Datos Personales” incluido en la sección de “Protección de Datos Personales” del Portal SIMPLE.  
Business Quality (BQ) utilizará la información descrita en el formulario para evaluar juntamente con Legal y demás áreas involucradas, si es necesario o no tramitar ante la Autoridad Peruana de Protección de Datos Personales (APDP), la creación de un nuevo Banco de Datos Personales o la modificación de uno ya existente.

<sup>1</sup> El tratamiento de Datos Personales realizado por EEP está sujeto a la supervisión, fiscalización, e imposición de sanciones, en caso de incumplimiento, por parte de la autoridad competente.

- b. El Administrador procederá con la descripción del Banco de Datos Personales, para lo cual deberá completar la Ficha de Seguridad<sup>2</sup> con la siguiente información:
- Información general y finalidad del Banco de Datos Personales.
  - Datos Personales objeto de tratamiento (precisando si se realiza la transferencia de dicha información).
  - Flujo del tratamiento de los Datos Personales.
  - Medidas de seguridad del Banco de Datos Personales.
  - Consentimiento y flujo transfronterizo (de ser aplicable).
- c. Tratándose de un Banco de Datos Personales que contengan Datos Sensibles, su creación sólo puede justificarse si su finalidad además de ser legítima es concreta y acorde con la actividad o fin para el cual es requerida.
- d. Los Bancos de Datos Personales deberán inscribirse ante la APDP y deberán contar con medidas de seguridad implementadas.
- e. El Administrador será el encargado de efectuar el seguimiento al cumplimiento de las medidas de seguridad implementadas para asegurar el adecuado tratamiento de los Datos Personales de los procesos su cargo.
- f. El DPM y el DPE prestará soporte a los Administradores en sus funciones para mantener el adecuado funcionamiento del Sistema de Gestión de Protección de Datos Personales.

## 5. Medidas de Seguridad:

Los Bancos de Datos Personales deben contar con medidas de seguridad (organizativas, técnica y legales) que permitan su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado, para lo cual se podrá considerar lo establecido en el Decreto Supremo N° 003-2013-JUS, así como la Directiva de Seguridad de la Información, aprobada por Resolución Directoral N° 019-2013-JUS/DGPDP.

## 6. Seguimiento:

Para asegurar el cumplimiento de la presente política y lo exigido por la Ley y la Política del Grupo ENGIE, el DPM, con soporte del DPE, liderará revisiones anuales donde verificará el adecuado tratamiento de los Datos Personales utilizados en cada proceso de EEP y el funcionamiento del Sistema de Gestión de Protección de Datos Personales.

### PROCEDIMIENTOS:

Para una mejor organización en el cumplimiento de roles durante la vigencia de la presente política, en el Anexo I se describen los pasos a seguir en los siguientes procedimientos:

“Inscripción o modificación de Banco de Datos Personales ante la APDP”.

“Atención de solicitud de Derechos ARCO”.

“Revocación del Consentimiento del Titular de Datos Personales”.

“Respuesta a Incidentes de Datos Personales”.