Grupo ENERGO-PRO

POLÍTICA DE PROTECCIÓN DE DATOS DE EMPLEADOS (INTERNOS)

2021

POLÍTICA DE PROTECCIÓN DE DATOS DE EMPLEADOS (INTERNOS)

1. Introducción

Nuestro negocio es la generación hidroeléctrica. Operamos plantas en Europa Central y Oriental, el mar Negro y el Cáucaso. A su vez, participamos del negocio de distribución y comercialización de potencia, operando redes de distribución a gran escala en Bulgaria y Georgia con más de 2.3 millones de usuarios de red.

Nuestra compañía fue establecida en 1994 en la ciudad Checa de Svitavy, participando en la modernización y rehabilitación del sector hidroeléctrico en Europa Central y Oriental durante el periodo de transición económica. La capacidad total instalada de nuestras centrales es de 1243 MW, mientras que la generación anual de energía es mayor a los 3.8 TWh.

Una parte del grupo multinacional ENERGO-PRO, con casa matriz en Praga, es el fabricante esloveno de turbinas hidroeléctricas Litostroj Power d.o.o., con proyectos comisionados en más de 60 países alrededor del mundo. Su subsidiaria, Litostroj Engineering a.s., registrada en la República Checa (previamente conocida como ČKD Blansko Engineering, a.s.), concentra sus esfuerzos en la investigación, diseño y trabajos de ingeniería. El Grupo Litostroj también suministra equipo para centrales hidroeléctricas, incluyendo turbinas reversibles para almacenamiento por bombeo (Pumped-Storage), y centrales de bombeo.

2. What this is about

Esta es la política de protección de datos del Grupo ENERGO-PRO[1] ("**nosotros**", "**nuestro**"). Debe ser seguida por todos los empleados, contratistas, trabajadores temporales, agentes y consultores ("**personal**" o "**usted**") que trabajen para o con ENERGO-PRO. Llevamos a cabo los datos personales de nuestros empleados.

Esta política establece cómo buscamos proteger los datos personales y asegurarnos de que el personal comprenda las reglas que rigen el uso de los datos personales a los que tienen acceso en el curso de su trabajo. En particular, esta política requiere personal para asegurar que el Oficial de Protección de Datos (DPO) deba ser consultado antes de que cualquier proceso significativo de procesamiento de datos se inicie para asegurarse de que las medidas de cumplimiento pertinentes se aborden.

Esta política proporciona información y orientación de uso general en todas las áreas comerciales. ¿Porque es esto importante?

Si no manejamos los datos personales de manera responsable y legal, esto puede tener un impacto negativo en la confianza de las personas en nuestro negocio. Además, nuestra información comercial sensible es confidencial y debe protegerse adecuadamente; de lo contrario, esto puede significar que perdamos nuestra ventaja competitiva, suframos daños a la reputación o nos expongamos a responsabilidades legales.

Es importante destacar que, si no cumplimos con las leyes de protección de datos, también podemos enfrentarnos a multas regulatorias masivas (de hasta 20 millones de euros o el 4% de la facturación anual global, lo que sea mayor).

3. Definiciones

Es importante que comprenda los siguientes términos:

"**Leyes de protección de datos**" hace referencia a las leyes que rigen la privacidad, el uso y la protección de los datos personales, incluido el RGPD y cualquier ley local que se aplique en el país donde trabaja o para las personas cuya información utiliza.

[1] El Grupo incluye DK Holding Investments, s.r.o., el único y directo accionista de ENERGO-PRO a.s., así como todas sus directas e indirectas subsidiarias.

"**RGPD**" hace referencia al Reglamento General de Protección de Datos (GDPR), que se ha aplicado en toda la Unión Europea ("UE") desde el 25 de mayo de 2018, y afecta a organizaciones establecidas en la UE y también a aquellas fuera de la UE que utilizan datos personales de personas en la UE en cierta forma.

"**Datos personales**" significa cualquier información relacionada con una persona física identificada o identificable (es decir, una que pueda ser identificada, directa o indirectamente, en particular por referencia a un identificador o uno o más factores específicos de los aspectos físicos, fisiológicos, genéticos, mentales, de identidad económica, cultural o social de dicha persona). Los identificadores incluyen cosas como el nombre, número ID, datos de ubicación y los identificadores en línea.

Ejemplos de los tipos de personas sobre las que recopilamos datos personales: empleados actuales y anteriores, agencias, personal contratado y otro personal, clientes, proveedores y contactos de marketing.

Ejemplos de los tipos de datos personales que recopilamos: datos de contacto de las personas, antecedentes educativos, detalles financieros y salariales, detalles de certificados y diplomas, educación y habilidades, estado civil, nacionalidad, cargo, datos de salud, datos biométricos y CV.

Los datos totalmente anonimizados (es decir, los datos a partir de los cuales no se puede identificar a una persona) y la información sobre personas fallecidas generalmente no se consideran datos personales.

"**Datos personales de categoría especial**" significa datos personales que revelan el origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, o afiliación sindical, y el procesamiento de datos genéticos, datos biométricos con el fin de identificar de forma única a una persona física, datos relacionados con la salud o datos relacionados con la vida sexual u orientación sexual de una persona física.

Los datos de categorías especiales (a veces denominados por su antiguo nombre de "datos personales sensibles") requieren una protección especial debido a la posibilidad de que causen perjuicios a la persona con la que se relacionan y, por lo tanto, deben controlarse estrictamente de acuerdo con esta política.

Los datos de salud son probablemente los datos más típicos que encontrará en esta categoría (que cubren tanto la salud física como mental) y cubren cualquier información que revele información sobre su estado de salud.

"**Procesamiento de datos**" significa cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por medios automatizados o no, como recopilación, registro, organización, estructuración, almacenamiento, adaptación o alteración, recuperación, consulta, uso, divulgación por transmisión, difusión o puesta a disposición de otra manera, alineación o combinación, restricción, borrado o destrucción. Prácticamente todo lo que haces con datos personales es procesamiento de datos.

"**Violaciones de datos**" significa una violación de la seguridad que conduce a la destrucción, pérdida, alteración, divulgación no autorizada o acceso a datos personales transmitidos, almacenados o procesados de otra manera, de manera accidental o ilegal.

4. Alcance

Esta política se aplica a todo el personal. Usted debe estar familiarizado con esta política y cumplir con sus términos.

Ocasionalmente, podemos complementar o enmendar esta política con políticas y/o pautas adicionales, le informaremos de los cambios materiales cuando apliquen.

5. ¿Quién es responsable de esta política?

El DPO tiene la responsabilidad general de esta política. Él o ella es responsable de garantizar que todo el personal cumpla con esta política.

Sin embargo, lograr el cumplimiento correcto de la protección de datos redunda en el interés de todos y es responsabilidad de todo el personal. Si detecta un problema de protección de datos (o un problema potencial), infórmelo y resuélvalo rápidamente y siempre solicite asistencia cuando lo necesite.

6. Nuestros procedimientos

Legalidad, justicia y procesamiento transparente

Debemos procesar los datos personales de manera legal, justa y transparente de acuerdo con los derechos de las personas. Esto generalmente significa que no debemos procesar datos personales a menos que:

- el procesamiento sea:

  a) necesario para ejecutar un contrato que tenemos con un individuo (incluido un contrato de trabajo) o para cumplir con las obligaciones legales que tenemos; o
  b) de otro modo necesario para nuestros intereses legítimos y no está anulado por los derechos de protección de datos de la persona; o
- la persona cuyos datos estamos procesando ha dado su consentimiento para ello.

El consentimiento debe ser libre, específico, informado e inequívoco, y otorgado mediante una declaración o una acción afirmativa clara, que demuestre que el individuo está de acuerdo con el procesamiento de sus datos personales. Usted deberá mantener registros de los consentimientos. Si alguien retira su consentimiento para que procesemos su información, tendremos que dejar de procesarla.

Siempre que sea posible, debemos tratar de asegurarnos de que el procesamiento esté permitido por una de las razones alternativas descritas en el primer punto anterior (particularmente para la información relacionada con el empleo). En la mayoría de los casos, esta disposición se aplicará a las actividades de procesamiento de datos comerciales de rutina.

Datos personales de categoría especial

En la mayoría de los casos en los que procesamos datos personales de categorías especiales, necesitaremos el consentimiento explícito del interesado para hacerlo, a menos que se apliquen circunstancias excepcionales o la ley nos exija hacerlo (por ejemplo, para cumplir con las obligaciones legales para garantizar la salud y la seguridad en el trabajo, o si alguien está gravemente herido y no puede dar su consentimiento).

Cualquier consentimiento deberá identificar claramente cuáles son los datos relevantes, por qué se están procesando y a quién se divulgarán. Idealmente, la persona deberá responder con una declaración en palabras y (si es posible) que esté firmada y fechada. Usamos un formulario de consentimiento para fines de salud específicos. (Ver Apéndice 1.)

Procesamiento para fines específicos

Usted no puede simplemente recopilar datos personales por "razones por determinar". Debe asegurarse de que los datos personales se recopilen solo para fines específicos, los cuales se le informan a la persona. Usted no puede decidir, más tarde, usar esos datos para algo completamente diferente (en la mayoría de los casos, tendría que regresar con la persona y pedir permiso para usar los datos para ese propósito diferente).

Minimización de datos y precisión

Nos aseguraremos de que cualquier dato personal que procesemos sea exacto, adecuado, relevante y no excesivo dado el propósito para el que fue obtenido.

Usted deberá realizar comprobaciones periódicas para asegurarse de que los datos personales que tenemos sigan siendo precisos y actualizarlos según sea necesario. Las personas pueden solicitar que corrijamos los datos personales inexactos relacionados con ellos. Si cree que la información es inexacta, debe registrar el hecho de que la exactitud de la información está en disputa e informar al DPO. Es posible que la información que sea incorrecta, engañosa, inexacta o desactualizada deba actualizarse o posiblemente destruirse; si no está seguro de esto, hable con el DPO.

Al crear formularios o procesos para recopilar datos personales, deberá asegurarse de que estos recopilen los datos mínimos requeridos, y nada más; cualquier dato que no sea necesario para el propósito para el que se está recopilando o ha sido recopilado no debe recopilarse en el primer lugar. No procesaremos los datos personales obtenidos para un propósito para ningún propósito no relacionado a menos que la persona en cuestión haya aceptado esto o de otra manera lo esperaría razonablemente.

7. Seguridad de datos

Debemos mantener los datos personales seguros contra la destrucción, pérdida, alteración, divulgación o acceso no autorizados, accidentales o ilegales. Esto significa que cumplan con nuestras directrices y políticas de seguridad.

Tenemos la obligación de implementar las medidas técnicas y organizativas adecuadas para garantizar que los datos permanezcan seguros. Dependiendo de la situación, puede ser apropiado, por ejemplo, para:

- Limitar el acceso a los datos, únicamente a las personas específicas autorizadas que necesiten conocerlos (controles de acceso);
- Utilizar datos no identificables (por ejemplo, anonimizados o codificados);
- Escritorios y armarios seguros con cerradura. Los escritorios y armarios deben mantenerse cerrados con llave si contienen datos personales (e información confidencial);
- Deshacerse de los datos personales de forma segura. Los documentos en papel deben triturarse. Los disquetes, CD-ROM y USB deben destruirse físicamente cuando ya no sean necesarios; o
- Utilizar el equipo de forma segura. Asegúrese de que terceros, como los visitantes, no puedan ver datos personales en los monitores de la empresa. Cierre la sesión de las PC cuando las deje desatendidas.

Debemos tener especial cuidado con las aplicaciones y los servicios basados en la nube. No coloque datos en una aplicación ni los cargue en la nube sin la autorización del DPO.

También debe asegurarse siempre de que los dispositivos que usa para acceder a los datos personales estén encriptados y asegurarse de que existan las protecciones adecuadas cuando comparta datos personales con otras personas.

La seguridad de datos es una prioridad, pero también un reto constante para nuestro negocio. Necesitamos asegurarnos de que estamos probando, analizando y evaluando regularmente la efectividad de las medidas de seguridad técnicas y organizativas que utilizamos para procesar datos personales.

Conservación de datos

Debemos conservar los datos personales durante no más de lo necesario. Lo que sea necesario dependerá de las circunstancias de cada caso, teniendo en cuenta las razones por las que se obtuvieron los datos personales, pero esto debe determinarse de manera coherente con Nuestra Guía de Conservación de Datos. (Ver Apéndice 2).

Al destruir o borrar datos personales, debe hacerlo de forma segura.

Si es posible anular la identificación de la información de modo que no se pueda individualizar a partir de ella, es posible que podamos conservarla durante más tiempo, por ejemplo, cuando sea útil para fines analíticos o estadísticos.

Sus datos personales

Usted debe tomar medidas razonables para garantizar que los datos personales que tenemos sobre usted sean exacta y actualizada como sea necesario, por ejemplo, si sus circunstancias personales cambian, por favor, informar al departamento de recursos humanos para que puedan actualizar sus registros.

8. Transferencia de datos internacionales

Existen restricciones sobre las transferencias internacionales de datos personales. Una transferencia internacional de datos puede ocurrir no solo cuando envía datos personales a un destinatario que se encuentra fuera de la EEA, sino también cuando se accede a datos personales o se ven desde fuera de la EEA.

No debe transferir datos personales fuera del EEA (que incluye la UE, Islandia, Liechtenstein y Noruega) sin antes consultar al DPO. En general, será necesario establecer contratos específicos o mecanismos de transferencia alternativos antes de que los datos personales puedan transferirse legalmente fuera de la EEA.

Debe tener especial cuidado cuando busque utilizar proveedores que tengan su sede fuera de la EEA o que utilicen subcontratistas fuera de la EEA para determinados aspectos de los servicios que prestan. Cuando utilice servicios basados en la nube, deberá verificar las ubicaciones donde se alojan los datos y asegurarse de que se cumplan los requisitos relacionados con las transferencias internacionales de datos.

9. Requerimientos de acceso de sujetos

Bajo el GDPR, los individuos tienen derecho (con ciertas excepciones) a solicitar acceso una copia de la información contenida sobre ellos. Esto puede incluir cualquier opinión que usted y otros empleados hayan agregado a sus registros. A veces, estos se conocen como "SAR" (que significa "solicitudes de acceso de sujetos").

Las personas también tienen derecho a solicitar la rectificación, el borrado, la restricción, la portabilidad de los datos, a oponerse al procesamiento y otros derechos en relación con la toma de decisiones automatizada y la elaboración de perfiles.

Estos derechos se denominan solicitudes de datos por sujetos (DSR). Si recibe un DSR, por favor atienda tal petición inmediatamente y realice seguimiento a la RPD mediante nuestro procedimiento DSR descrito en el Apéndice 3. Es posible que se le pida que nos ayude a cumplir con esas solicitudes, pero no hay que responder antes de contactar con la DPO, incluso para reconocer la solicitud.

No podemos cobrar una tarifa por responder a las DSR, aunque podemos cobrar nuestros costos administrativos si una solicitud es manifiestamente infundada o excesiva, especialmente si es repetitiva.

Ninguna de las DSR es absolutas - hay excepciones y restricciones a la información a la que tiene derecho una persona o lo que puede requerir una organización para hacer dar respuesta a una solicitud en virtud de las leyes de protección de datos.

¿Y si usted quiere realizar una DSR?

Comuníquese con el DPO si desea corregir o solicitar información que tenemos sobre usted, o ejercer cualquiera de sus otros derechos descritos anteriormente.

10. Informar violaciones de datos

Todos los miembros del personal tienen la obligación de informar las fallas de cumplimiento de protección de datos, reales o potenciales. Esto nos permite:

- investigar la falla y tomar medidas correctivas si es necesario; e,
- Informar la infracción a las autoridades regulatorias o a la policía cuando sea aconsejable hacerlo.

No se demore en informar una violación de datos: el tiempo será fundamental para controlar la violación, además, tenemos la obligación de informar las violaciones de datos personales a los reguladores pertinentes (generalmente dentro de las 72 horas). Esto es muy importante.

La prevención es la forma más efectiva de defensa. Si ve algo que pueda representar un riesgo para la seguridad, infórmelo de inmediato a su superior jerárquico.

11. Capacitación

Todo el personal recibirá capacitación sobre esta política. Los nuevos miembros recibirán capacitación como parte del proceso de inducción. Se proporcionará más capacitación siempre que haya un cambio sustancial en la ley o en nuestra política y procedimiento.

La formación se proporciona en línea y cubrirá:

- la ley relativa a la protección de datos; y,
- nuestra protección de datos y políticas, así como los procedimientos relacionados.

La finalización de la formación es obligatoria.

El DPO supervisará continuamente las necesidades de formación, pero si cree que necesita más formación sobre cualquier aspecto de la ley pertinente o esta política o procedimientos, póngase en contacto con el DPO.

12. Vigilancia

Todos deben vigilar el cumplimiento de esta política. El DPO tiene la responsabilidad general de monitorear esta política con regularidad para asegurarse de que se cumpla.

13. Incumplimiento de esta política

Nos tomamos muy en serio el cumplimiento de esta política.

El incumplimiento lo pone en riesgo tanto a usted como a la empresa.

La importancia de esta política significa que el incumplimiento de cualquier requisito puede dar lugar a una acción disciplinaria según nuestros procedimientos, que puede resultar en el despido.

Si tiene alguna pregunta o inquietud sobre algo en esta política, no dude en comunicarse con el DPO.

APÉNDICE 1

FORMULARIO DE CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS PERSONALES DE CATEGORÍA ESPECIAL

DECLARACIÓN

El abajo firmante

_____

(Nombre, segundo nombre (s) y apellido)

Número de identificación personal (o equivalente): _____, en mi calidad de:

0 Empleado de la empresa

_____

0 Cónyuge, pareja que vive en familia, hijos mayores de 18 años del empleado de la empresa

_____

0 Representante autorizado de

_____

0 Otro / por favor describa /:

_____

DECLARO:

qué

Estoy de acuerdo

que ENERGO-PRO procese y almacene mis datos personales (incluidos mis datos de salud) proporcionados por mí en los documentos:

[0 Solicitud de apoyo financiero [cualquier fondo de salud aplicable];]
[0 Documentación médica descrita en la solicitud;]
[0 Otro / por favor describa /:]

_____

según los requisitos de:

• Reglamento (UE) 2016/679 del Consejo y Parlamento Europeo, del 27 de abril de 2016, sobre la protección de las personas en lo que respecta al tratamiento de datos personales y sobre la libre circulación de dichos datos (Reglamento (UE) 2016/679); y
• Las leyes y reglamentos nacionales de protección de datos,

Los cuales he proporcionado en relación con el propósito de [propósito, como apoyo financiero para el tratamiento de una enfermedad que no es pagado por el estado y / o bajo ningún plan de seguro médico obligatorio.]

Estoy familiarizado con:

- el propósito y los medios para procesar mis datos personales (incluidos mis datos de salud);
- el carácter voluntario del suministro de datos personales;
- el derecho a acceder y corregir o eliminar los datos recopilados y el derecho a restringir el procesamiento de datos personales;
- el derecho a oponerse al procesamiento, así como el derecho a solicitar la transferencia de mis datos personales a un tercero - controlador de datos personales;
- el derecho a apelar ante la Autoridad Nacional de Protección de Datos [insertar enlace al sitio web] en relación con el procesamiento de mis datos personales;
- la política de protección de datos de las empresas del grupo ENERGO-PRO;
- los datos de contacto del delegado de protección de datos: [insertar la dirección de correo electrónico del DPD]; y
- el hecho de que ENERGO-PRO pueda necesitar transferir mis datos personales (incluidos mis datos de salud) en todo el mundo y pueda utilizar a terceros para procesar mis datos personales en nombre de ENERGO-PRO.

_____

(Estoy informado y estoy de acuerdo con el procesamiento como se describe arriba)

Doy mi consentimiento como resultado de mi libre albedrío y se me informa que tengo derecho en cualquier momento a negarme a dar, en parte o en su totalidad, mi consentimiento y a retirar un consentimiento ya otorgado. El retiro de mi consentimiento no afecta la legalidad del procesamiento basado en un consentimiento previo al retiro.

[Se me informa que en caso de denegación (total / parcial) es posible no continuar con la consideración de la solicitud mencionada anteriormente.]

Fecha: _____ Declarante: _____

(firma)

Lugar: _____

* para completar manualmente

APENDICE 2

DIRECTRICES DE RETENCIÓN DE DATOS

Sus datos personales se almacenan solo durante un período que es necesario para lograr los fines propuestos.

En cuanto al desempeño de las relaciones laborales, solo se tratarán los datos personales requeridos por la ley y se mantendrán en los términos que establezca la legislación laboral y de seguridad social.

En ausencia de requisitos legales sobre la retención de datos, los datos pueden almacenarse por un período de hasta 5 años.

APENDICE 3

SOLICITUD DE DATOS DE SUJETOS

Si desea enviar una solicitud para acceder, rectificar, borrar, restringir u oponerse al procesamiento de los Datos personales que nos ha proporcionado previamente, o si desea enviar una solicitud para recibir una copia electrónica de sus Datos personales con el fin de transmitirlo a otra empresa (en la medida en que la ley aplicable le otorgue este derecho a la portabilidad de datos), puede comunicarse con nosotros por correo electrónico ([inserte la dirección de correo electrónico del DPO]). Responderemos a su solicitud de acuerdo con la ley aplicable.

Cualquiera que sea la solicitud que realice, debe contener una descripción detallada y precisa de los datos en cuestión. Cuando existan dudas razonables con respecto a su identidad, es posible que se le solicite que proporcione una copia de un documento para ayudarnos a verificar su identidad. Puede ser cualquier documento adecuado, tal como su DNI o pasaporte. Si proporciona cualquier otro documento, los datos personales como su nombre y su dirección deben ser claros para poder identificarlo, mientras que cualquier otro dato como una foto o cualquier característica personal puede estar tachado.

Nuestro uso de la información contenida en su documento de identificación está estrictamente limitado: los datos solo se usarán para verificar su identidad y no se almacenarán por más tiempo del necesario para este propósito.

Dependiendo de la naturaleza de su solicitud, deje en claro qué datos personales le gustaría que se modifiquen, si desea que se eliminen sus datos personales de nuestra base de datos o, de lo contrario, háganos saber qué limitaciones le gustaría poner en nuestro uso de sus datos personales. Para su protección, solo podemos implementar solicitudes con respecto a los Datos personales asociados con su cuenta, su dirección de correo electrónico u otra información de cuenta u otra información específica que le concierne y que usted utiliza para enviarnos esta solicitud, es posible que necesitemos verificar su identidad antes de implementar la misma.

Tenga en cuenta que es posible que necesitemos conservar cierta información para fines de mantenimiento de registros. También puede haber información residual que permanecerá dentro de nuestras bases de datos u otros registros y que no se eliminará.

Cumpliremos con su (s) solicitud (es) tan pronto como sea razonablemente posible.