

Política de protección de datos personales

1. Finalidad	1
2. Ámbito de aplicación.....	1
3. Principios Generales del Tratamiento de Datos Personales	1
4. Principios básicos relativos al tratamiento de datos personales.....	2
5. Medidas de Seguridad.....	3
6. Transferencias Internacionales de Datos.....	4
7. Delegado de Protección de Datos (DPO).....	4
8. Implementación y Control.....	4
9. Evaluación y Actualización.....	4
10. Contacto	5

La implementación de una Política de Privacidad de Datos Personales en Grupo Tecopy responde al compromiso de la organización con la protección de los derechos fundamentales en el tratamiento de la información personal, alineándose con las exigencias de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) y el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD). Esta *Política* garantiza que el tratamiento de los datos de clientes, empleados y colaboradores se realice de manera responsable, transparente y segura, consolidando un entorno de confianza y asegurando que la privacidad sea una prioridad en todos los procesos operativos.

1. Finalidad

Esta Política de Protección de Datos Personales tiene como objetivo establecer los principios y directrices que guían el tratamiento de los datos personales dentro del perímetro del Grupo, garantizando el respeto a los derechos de las personas físicas, como el derecho a la intimidad y el derecho al honor, en conformidad con la normativa aplicable en materia de protección de datos, incluyendo el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos (LOPD).

2. Ámbito de aplicación

Esta *Política* es aplicable a todas las entidades, departamentos y personas trabajadoras de las empresas que integran a Grupo Tecopy: Tecopy, SAU, Centro de Observación y Teledetección Espacial, SAU, Enclave Formación, SLU, Grupo Tecopy Cartera Empresarial, S.L, así como a las empresas subcontratadas y otros terceros que, en su relación con dichas organizaciones, tengan acceso a datos personales. Asimismo, es de aplicación a cualquier tratamiento de datos personales realizado por las empresas del Grupo, independientemente de su soporte o del lugar donde se encuentren almacenados, siempre que estén bajo el control del Grupo.

3. Principios Generales del Tratamiento de Datos Personales

Las entidades que conforman el Grupo se comprometen a cumplir rigurosamente con la normativa de protección de datos vigente en su jurisdicción, aplicable según el tipo de tratamiento de datos personales que realicen y en concordancia con las disposiciones o acuerdos vinculantes adoptados dentro del marco del Grupo. Del mismo modo, estas entidades fomentarán que los principios establecidos en esta Política sean considerados: (I) en el diseño e implementación de cualquier proceso que conlleve el tratamiento de datos personales; (II) en los productos y servicios que ofrezcan; (III) en todos los contratos y compromisos formalizados con personas físicas; y (IV) en la puesta en marcha de sistemas y plataformas que faciliten a los profesionales del Grupo o a terceros el acceso, recopilación o tratamiento de datos personales.

4. Principios básicos relativos al tratamiento de datos personales

a) Principio de Licitud, Lealtad y Transparencia

El tratamiento de datos personales debe cumplir con los principios de legitimidad, licitud y lealtad, según la legislación vigente. Esto significa que los datos personales deben ser recogidos con fines específicos y legítimos, y en los casos en los que sea necesario, se debe obtener el consentimiento previo de las personas interesadas.

Además, los fines del tratamiento de los datos deben ser claros y establecidos en el momento de su recogida. En particular, no se recabarán ni tratarán datos sensibles, como aquellos relacionados con el origen racial, ideología política, creencias religiosas, orientación sexual, afiliación sindical, salud, o datos genéticos o biométricos, salvo que la legislación lo permita o lo exija. En estos casos, el tratamiento de dichos datos estará sujeto a las normas correspondientes.

b) Principio de Limitación de la Finalidad

Los datos personales solo pueden ser recogidos con fines determinados, explícitos y legítimos, y no deben ser tratados posteriormente de manera incompatible con dichos fines. Esto significa que la organización debe especificar el propósito del tratamiento desde el principio y no utilizar los datos para otros fines sin obtener un nuevo consentimiento.

c) Principio de Minimización de Datos

El tratamiento de los datos personales debe limitarse a los datos que sean estrictamente necesarios en relación con los fines para los que son tratados. Es decir, solo deben recabarse y tratarse los datos que sean adecuados, pertinentes y limitados a lo necesario.

d) Principio de Exactitud

Los datos personales deben ser exactos y, cuando sea necesario, estar actualizados. Es responsabilidad del responsable del tratamiento tomar medidas razonables para garantizar que los datos que sean inexactos, respecto a los fines para los que se tratan, se supriman o rectifiquen sin demora.

e) Principio de Limitación del Plazo de Conservación

Los datos personales deben mantenerse en un formato que permita la identificación de los interesados durante un plazo no superior al necesario para los fines del tratamiento. Esto significa que los datos no pueden conservarse indefinidamente, salvo que exista una justificación legal para ello.

f) Principio de Integridad y Confidencialidad

Los datos personales deben ser tratados de manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas y organizativas apropiadas.

g) Principio de Responsabilidad Proactiva (Accountability)

El responsable del tratamiento debe ser capaz de demostrar que cumple con los principios anteriores. Este principio exige que las organizaciones tomen un enfoque proactivo para asegurar el cumplimiento, implementando las medidas necesarias (como auditorías, registros de actividades de tratamiento, etc.) y siendo capaces de probar ese cumplimiento si es necesario.

h) Derechos de los interesados

Los interesados cuyos datos personales sean tratados por Grupo Tecopy tienen los siguientes derechos:

- **Derecho de acceso:** Los interesados tienen derecho a saber si estamos tratando sus datos, qué datos estamos tratando y a recibir una copia de los mismos.
- **Derecho de rectificación:** Pueden solicitar la modificación de los datos inexactos o incompletos.
- **Derecho de supresión (derecho al olvido):** Los interesados pueden solicitar la eliminación de sus datos cuando ya no sean necesarios para los fines para los cuales fueron recogidos, entre otros supuestos.
- **Derecho a la limitación del tratamiento:** Podrán solicitar la limitación del tratamiento de sus datos personales en determinadas circunstancias.
- **Derecho a la portabilidad de los datos:** Los interesados podrán solicitar la transmisión de sus datos a otro responsable.
- **Derecho de oposición:** Los interesados pueden oponerse al tratamiento de sus datos en determinadas situaciones y solicitar que dejemos de tratar sus datos.

Para ejercer cualquiera de estos derechos, los interesados deberán dirigirse a Grupo Tecopy través de los medios facilitados en el apartado de contacto.

5. Medidas de Seguridad

Grupo Tecopy se compromete a implementar las medidas técnicas y organizativas necesarias para garantizar un nivel adecuado de seguridad en el tratamiento de los datos personales. Entre dichas medidas se encuentran:

- Control de acceso restringido a los sistemas de tratamiento.
- Uso de tecnologías de cifrado para proteger los datos sensibles.
- Auditorías internas periódicas para garantizar el cumplimiento con la normativa.
- Procedimientos para gestionar incidentes de seguridad, incluyendo la notificación a las autoridades de protección de datos cuando sea necesario.

6. Transferencias Internacionales de Datos

Cualquier transferencia internacional de datos realizada por el Grupo estará sujeta a las garantías adecuadas conforme a la normativa aplicable. Si los datos personales deben ser transferidos fuera del Espacio Económico Europeo (EEE), se deberá asegurar y garantizar de que se cumplan las condiciones necesarias, tales como la existencia de cláusulas contractuales estándar aprobadas por la Comisión Europea o decisiones de adecuación.

7. Delegado de Protección de Datos (DPO)

Grupo Tecopy ha designado un Delegado de Protección de Datos (DPO), responsable de velar por el cumplimiento de esta *Política* y de la normativa aplicable en materia de protección de datos. El DPO también es el punto de contacto para los interesados que deseen ejercer sus derechos o realizar consultas sobre el tratamiento de sus datos personales.

8. Implementación y Control

La implementación de esta *Política* se lleva a cabo bajo la supervisión del Departamento de RR.HH. que será responsable de su correcta aplicación. Asimismo, se realizarán controles internos periódicos para garantizar su efectividad y cumplimiento. En caso de detectarse incumplimientos, se adoptarán las medidas correctoras pertinentes.

9. Evaluación y Actualización

Esta *Política* será objeto de revisión y actualización de forma periódica, al menos una vez al año, o siempre que se produzcan cambios relevantes en la normativa aplicable, en las prácticas internas de la organización, o en cualquier otro aspecto que pueda afectar la protección de los datos personales. El propósito de esta revisión es asegurar que la *Política* se mantenga actualizada, pertinente y adaptada a las necesidades de Grupo Tecopy y a los derechos de las personas interesadas.

Para garantizar la transparencia y el cumplimiento de esta *Política*, cualquier modificación que se realice será comunicada de manera clara y oportuna a todos los interesados a través de los siguientes canales:

- **Correo Electrónico Corporativo:** Se enviará una notificación directa a las direcciones de correo electrónico de los interesados registrados en la base de datos de la organización.
- **Intranet Corporativa:** Las actualizaciones estarán disponibles en la sección correspondiente de la intranet, para que el personal interno de la organización pueda acceder y revisar las modificaciones de la *Política* en cualquier momento.
- **Página Web Oficial:** Se publicarán las actualizaciones en la página web de la organización en el apartado de privacidad y protección de datos, accesible para cualquier persona interesada.

- **Boletines Internos y Reuniones Informativas:** En el caso de modificaciones significativas, se incluirá un resumen en los boletines internos de la organización o se organizarán reuniones informativas, tanto presenciales como virtuales, para explicar los cambios y resolver cualquier duda.

Con estas medidas, el Grupo se compromete a mantener informados a todos los interesados sobre las prácticas y medidas de protección de datos personales implementadas, asegurando que la política vigente sea siempre de conocimiento público y de fácil acceso.

10. Contacto

Los interesados, incluidos clientes, personas trabajadoras, colaboradores o cualquier otra persona cuyos datos personales sean tratados por Grupo Tecopy, pueden contactar para realizar consultas, solicitudes o cualquier otra cuestión relacionada con la protección de datos personales. Esto incluye, entre otros, el ejercicio de sus derechos de acceso, rectificación, supresión, limitación del tratamiento, oposición y portabilidad de los datos, de acuerdo con la normativa de protección de datos aplicable.

Para ello, pueden dirigirse al equipo de protección de datos de Grupo Tecopy a través del siguiente correo electrónico: dpo@grupotecopy.es