SGPI05

POLITICA COMO ENCARGADOS DEL TRATAMIENTO

Elaborado: 23/09/2024

Revisado y aprobado: 23/09/2024

izertis

Índice

1. OBJETIVO Y ALCANCE

La presente política pretende dar cumplimiento a la Norma ISO/IEC 27701, al 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 en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales en lo relativo a establecer las medidas y controles que IZERTIS, S.A a la que se obliga cuando realiza servicios a clientes que implican el tratamiento de datos personales actuando en estos casos como ENCARGADO DEL TRATAMIENTO.

La presente Política deberá ser observada por IZERTIS, S.A, y todo el personal que maneje datos de carácter personal en el desarrollo de servicios a clientes.

Esta política alcanzará a todos los sistemas de tratamiento de la información que contengan IIP relacionado con la prestación de servicios a clientes.

2. PRINCIPIOS GENERALES DE PRIVACIDAD

IZERTIS deberá:

- Garantizar la **formación** necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales objeto del acuerdo.
- Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la **confidencialidad y a cumplir las medidas de seguridad** correspondientes, de las que hay que informarles convenientemente.
- **Poner a disposición** del responsable (cliente) **toda la información necesaria** para demostrar el cumplimiento de sus obligaciones.
- Deberá permitir que el cliente lleve a cabo las **auditorias** de privacidad y protección de datos si así lo solicita, colaborando con el equipo auditor y facilitando todas las evidencias y registros que le sean requeridos

3. CONDICIONES GENERALES

3.1. Acuerdo con el cliente (DPA)

Se deberá de firmar un acuerdo entre el Responsable del Tratamiento (cliente) e IZERTIS en calidad de Encargado del Tratamiento para dar cumplimiento al **Art. 28 del 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 (RGPD).**

En caso de contradicción entre lo indicado en esta Política y el DPA (Acuerdo de Protección de Datos como Encargado del Tratamiento) firmado prevalecerá lo acordado en el acuerdo.

Este acuerdo podrá establecerse en un Contrato de Encargado de Tratamiento, un Anexo de Protección de datos al Contrato Mercantil o una Adenda al Contrato primario.

3.2. Finalidades

IZERTIS se obliga a:

- Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto del encargo. En ningún caso podrá utilizar los datos con fines propios.
- Tratar los datos de acuerdo con las instrucciones indicadas por el cliente en calidad de RESPONSABLE DEL TRATAMIENTO

3.3. Uso de marketing y publicidad

IZERTIS se obliga a:

- No utilizar los datos personales facilitados en virtud del acuerdo de encargo con fines de marketing y publicidad si no puede evidenciar que se ha obtenido el consentimiento previo del interesado correspondiente.
- Proporcionar dicho consentimiento no podrá ser nunca una condición para la realización del servicio.

3.4. Instrucción infractora

Si IZERTIS considera que alguna de las instrucciones dadas por el cliente infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, deberá informar inmediatamente al Responsable del tratamiento (cliente) a través del correo electrónico facilitado por el mismo como contacto para el desarrollo del servicio contratado.

3.5. Obligaciones de IZERTIS

IZERTIS deberá permitir al cliente las comprobaciones o evidencias que solicite de cumplimiento de privacidad y protección de datos cuando las solicite, colaborando con el cliente y facilitando evidencias y registros requeridos.

3.6. Registro de actividades del tratamiento de datos personales

IZERTIS deberá mantener los registros necesarios para demostrar el cumplimiento con sus obligaciones, entre las que se encuentra llevar un registro de las actividades desarrolladas como encargado para dar cumplimiento al **Art. 30.2. del RGPD y que debe incluir:**

- Categorías de tratamiento realizadas
- Transferencias internacionales de datos
- Descripción general de las medidas técnicas y organizativas adoptadas

3.7. Devolución, transferencia o eliminación de datos personales

Una vez finalice el acuerdo de prestación de servicio, IZERTIS debe devolver al responsable (cliente) o trasmitir a otro encargado que designe el responsable los datos personales, y suprimir cualquier copia que esté en su poder. No obstante, podrá mantener bloqueados los datos para atender posibles responsabilidades administrativas o jurisdiccionales. Al finalizar el período de retención legal, la Empresa procederá a la eliminación segura de los datos personales conforme a lo indicado en el punto 3.7.1

Estas obligaciones sólo aplican para los datos alojados en infraestructuras gestionadas o propiedad de IZERTIS. Si los datos se encuentran en infraestructuras gestionadas y/o propiedad del cliente, IZERTIS no tendrá responsabilidad sobre la devolución, transferencia y/o eliminación de los datos salvo que estas acciones entren dentro del servicio contratado.

Siempre se deberá tener en cuenta en todos estos supuestos lo acordado en el acuerdo firmado que prevalecerá sobre lo indicado en esta Política.

3.7.1 Mecanismos eliminación de los datos personales

En los supuestos en que, se concluya el deber de **suprimir los datos personales**, se deberá proceder a la eliminación física de los mismos ya se encuentren éstos en soporte automatizado o no automatizados:

1. Si los datos están contenidos en **soporte no automatizado**, se deberá proceder a la destrucción física de los documentos. A tal efecto se recomienda:
    - La utilización de **proveedores de servicio de destrucción documental** que nos facilita certificado de destrucción.
    - La utilización de herramientas de destrucción física de papel, tales como, **destructoras de papel**.
2. Si los datos están contenidos en **soporte informático**, se procederá de igual forma a su **eliminación de la aplicación**, sin que sea suficiente el empleo de una marca lógica o el mantenimiento de otro fichero alternativo en el que se registren los derechos de supresión. La entidad dispone además de las siguientes herramientas:

- **Olvido** certificada por el CCN-CERT para la eliminación de información programada.
- **Metaclean** también certificada por el CCN-CERT para la eliminación de metadatos en los ficheros adjuntos a los correos electrónicos.

Sin perjuicio de cualquier otro método de destrucción que pudiera valorarse, a continuación, se recogen los principales métodos de borrado identificados y clasificados en función de la capacidad efectiva para la eliminación lógica de los datos personales, así como sus ventajas e inconvenientes.

Se utilizará el más indicado tras estudiar el caso concreto conservando todas las evidencias de las decisiones adoptadas.

Métodos que no destruyen la información de forma segura Comandos de borrado Destrucción de la información mediante la utilización de comandos de borrado del sistema operativo	Formateo	Formateo de un dispositivo
	Anonimización	Su eficacia dependerá de la técnica de anonimización empleada en cada caso, que deberá garantizar de forma irreversible su identificación.
Métodos de destrucción de la información de forma segura	Destrucción	Podrá realizarse a través de diversos procedimientos mecánicos, en función de la naturaleza del soporte, en particular: ▪ Desintegración, pulverización, fusión e incineración. ▪ Trituración.
	Sobre-escritura	Escritura de un patrón de datos sobre los datos contenidos en los dispositivos de almacenamiento. Deberá asegurarse la sobre-escritura de la totalidad de la superficie de almacenamiento para asegurar la completa destrucción de los datos a través de la herramienta “Olvido”.

3.7.2 Mecanismos de devolución/transferencia de los datos personales

En los supuestos en que, se concluya el deber de **devolución de los datos personales** al cliente o transferencia a otro ENCARGADO DEL TRATAMIENTO se seguirán las instrucciones indicadas por el cliente que podrán estar incluidas en el acuerdo firmado. En todo caso siempre teniendo en cuenta que deben utilizarse mecanismos que ofrezcan técnicas de cifrado robustas que aseguren el no acceso a los datos no autorizado.

- La transferencia se realizará de **manera segura y conforme a las instrucciones documentadas del responsable** (cliente).
- Los datos personales serán transferidos en un formato **estructurado, interoperable y de fácil lectura mecánica** (ej., CSV, XML, JSON), con el objetivo de facilitar la integración por parte del nuevo encargado o del cliente (responsable del tratamiento).

- Se implementarán mecanismos de seguridad durante la transferencia, tales como el **cifrado de los datos** y la utilización de **canales seguros de transmisión** (ej., VPN, SFTP, o cualquier otra tecnología que garantice la confidencialidad e integridad de los datos).

3.8. Controles de transmisión de datos personales

Cuando para la prestación del servicio sea necesaria la **transmisión de datos personales** se deberá incluir medidas y controles que permitan garantizar que los datos llegan a su destino previsto. Estas medidas deberán incluir:

- Técnicas de cifrado seguras
- Controles de acceso robustos que permitan garantizar que sólo las personas autorizadas tienen acceso a los sistemas de transmisión
- Conservación de registros

Si la infraestructura a utilizar es responsabilidad del CLIENTE se deberán tener en cuenta las medidas de seguridad indicadas por el mismo.

3.9. Notificación de solicitudes de comunicación de datos personales

Cuando IZERTIS reciba cualquier solicitud de **comunicación de datos personales** objeto del acuerdo legalmente vinculante (ej. Desde la Agencia Tributaria, Fuerzas y Cuerpos de Seguridad, Autoridades Judiciales), deberá comunicarlo al cliente sin dilación indebida a través de correo electrónico dirigido al contacto indicado por el este para el servicio prestado o específico para estos fines.

Esta notificación incluirá la siguiente información:

- **Entidad solicitante:** Identificación de la autoridad, organismo o entidad que ha solicitado los datos.
- **Base legal**: Justificación o fundamentación legal de la solicitud, si se proporciona, para la solicitud de los datos.
- **Datos y categorías de interesados:** Descripción de los datos personales solicitados
- **Finalidad**: Motivo expuesto por la entidad solicitante para la solicitud de los datos.

- **Plazo de respuesta:** Plazo legal o administrativo establecido para responder a la solicitud.
- **Acciones previstas:** Medidas que IZERTIS tiene intención de tomar en respuesta a la solicitud, según los términos del acuerdo con el responsable del tratamiento (cliente).

3.10. Comunicación de datos personales legalmente vinculantes

IZERTIS deberá:

- Rechazar cualquier solicitud de comunicación de datos personales objeto del acuerdo que no sea legalmente vinculante
- Consultar previamente con el cliente antes de realizar cualquier comunicación de datos personales
- No aceptar cualquier solicitud de acuerdo para comunicación de datos personales que previamente deba ser autorizada por el cliente.

4. EN CASO DE CONTRADICCIÓN

En caso de que se produzcan contradicciones entre lo indicado en las cláusulas del acuerdo firmado como ENCARGADOS DEL TRATAMIENTO y esta política siempre prevalecerá lo acordado en el acuerdo firmado entre las partes.

5. CONTROL DE VERSIONES

Todo usuario de este fichero que encuentre un error u oportunidad de mejora deberá comunicarlo al responsable de este para su evaluación y, en su caso, modificación.

La versión en vigor del fichero es la que se encuentra en el repositorio corporativo.

VERSIÓN	FECHA	MODIFICACIONES
1	23/09/2024	Documento inicial

izertis

Passion for Technology