POLITICA GENERAL DE PRIVACIDAD

SINERBA.

ÍNDICE

1. INTRODUCCIÓN 1
2. DEFINICIONES 1
3. ÁMBITO SUBJETIVO DE APLICACIÓN 2
3.1. Alcance 2
3.2. Responsable del tratamiento 2
3.3. Encargado del tratamiento 3
3.4. Autoridad de Control 3
3.5. Delegado de Protección de Datos 3
4. ÁMBITO OBJETIVO DE APLICACIÓN 4
5. NORMATIVA APLICABLE 4
6. PRINCIPIOS GENERALES 5
6.1. Licitud del tratamiento 5
6.2. Lealtad del tratamiento 5
6.3. Transparencia del tratamiento 5
7. DEBER DE INFORMACIÓN Y DE LEGITIMACIÓN DEL TRATAMIENTO 6
8. PROCEDIMIENTO DE GESTIÓN DE EJERCICIO DE DERECHOS 7
9. MEDIDAS DE SEGURIDAD DE LOS DATOS PERSONALES 8
10. REGISTRO DE ACTIVIDADES DEL TRATAMIENTO 9
11. EVALUACIÓN DE PROVEEDORES 9
12. EVALUACIONES DE IMPACTO 9
14. TRANSFERENCIAS INTERNACIONALES DE DATOS 11
15. INTELIGENCIA ARTIFICIAL 11
16. APROBACIÓN Y MODIFICACIÓN DE LA POLÍTICA 11
17. CONTROL DE CAMBIOS Y APROBACIÓN 11

1. INTRODUCCIÓN

La protección de las personas físicas en relación con el tratamiento de sus datos personales es un derecho fundamental. La rápida evolución tecnológica ha traído consigo un aumento en la magnitud de recogida e intercambio de datos personales en el sector privado. Por esta razón, la normativa vigente en materia de protección de datos personales se centra en regular el tratamiento de datos personales (independientemente del soporte, automatizado o no), los derechos de los interesados sobre ellos y obligaciones de quienes lo tratan.

Dicho esto, en base a lo dispuesto en el considerando 78 y el artículo 24 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**"), a fin de poder demostrar la conformidad con el RGPD, el responsable del tratamiento debe aportar políticas internas y aplicar medidas que cumplan con los principios de protección de datos desde el diseño y por defecto, todo ello en base a un criterio de proporcionalidad y cumpliendo con el principio de responsabilidad proactiva.

En consecuencia, el objeto de la presente Política General de Privacidad (en adelante la "**Política**") pretende fijar los estándares de cumplimiento de forma proactiva para dar cumplimiento -valga la redundancia- a la normativa vigente en materia de protección de datos personales y privacidad.

2. DEFINICIONES

A efectos de la presente Política, conviene tener en cuenta los siguientes conceptos:

Datos personales: es toda la información sobre una persona física identificada o identificable (el "**interesado**"), se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador como, por ejemplo, un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjunto de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Responsable del tratamiento: persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios de tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

Encargado del tratamiento: persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

Consentimiento del interesado: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

Violación de la seguridad de los datos personales: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. ÁMBITO SUBJETIVO DE APLICACIÓN

3.1. Alcance

La presente Política resulta de aplicación a las siguientes entidades del grupo Sinerba Holding (en adelante nos referiremos a las mismas como el "**Grupo**" o "**Sinerba Holding**"), esto es:

- BILBA CONSTRUCCIÓN E INFRAESTRUCTURAS, S.L.
- LEBA SERVICIOS Y OBRAS, S.L.
- TAILOR RETAIL MAKERS, S.L.
- SUBA PROYECTOS COMPARTIDOS, S.L.
- SABIA ENERGÍA, S.L.
- SINERBA HOLDING, S.L.

En consecuencia, la Política resultará de obligado cumplimiento para todas las personas que formen parte de las entidades del Grupo, bien a través de cualquier tipo de relación contractual, laboral o profesional, o bien que ostenten cargos directivos o sean miembros del órgano de administración. Igualmente podrá ser de obligado cumplimiento para terceros que guarden relación con el Grupo como, por ejemplo, prestadores de servicios que puedan acceder a datos personales titularidad de algunas de las entidades del Grupo.

3.2. Responsable del tratamiento

Como responsable del tratamiento, las entidades del Grupo decidirán sobre el propósito, el contenido y el uso de los tratamientos de datos personales con respecto a sus empleados, clientes, usuarios y otros interesados. Por tanto, en la realización de estas actividades se debe cumplir las siguientes instrucciones:

- Asegurar que los datos sean adecuados y precisos, legítimamente obtenidos y tratados conforme al propósito para el cual fueron recogidos.
- Garantizar el cumplimiento de la confidencialidad relativo al tratamiento de datos personales.
- Informar al interesado de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.
- Poner a disposición de los interesados la documentación relativa al tratamiento de sus datos personales y el deber de informar.
- Facilitar y garantizar el ejercicio de derechos de los interesados.
- Aplicar medidas técnicas y organizativas para garantizar el principio de responsabilidad proactiva.

- Efectuar evaluaciones de impacto sobre privacidad en caso de ser necesario y mantener un registro de actividades del tratamiento.

- Notificar cualquier brecha de seguridad de datos personales a la Agencia Española de Protección de Datos.

- Garantizar que se respeten las normas en materia de protección de datos personales en sus relaciones con proveedores de servicios (encargados del tratamiento) que acceden a datos personales.

3.3. Encargado del tratamiento

Las sociedades del Grupo pueden formalizar acuerdos de prestación de servicios con otras sociedades del Grupo o con empresas externas, los cuales podrán tener acceso a datos personales ostentando estos últimos la condición de encargados del tratamiento. De la misma forma que podrá actuar como encargada del tratamiento en la prestación de servicios a otra entidad que actúa como responsable del tratamiento.

La relación relativa al encargado del tratamiento debe quedar regulado en un contrato por escrito, donde han de recogerse los siguientes puntos:

- Garantizar la confidencialidad de los tratamientos.

- Implementar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad de los datos, teniendo en cuenta los propósitos del tratamiento y riesgos.

- Autorización previa del responsable antes de subcontratar a otro encargado y garantizar que se cumplen con las mismas condiciones para el tratamiento de datos personales.

- Permitir y cooperar en todas las auditorías e inspecciones realizadas por el responsable.

- Asistir al responsable en la respuesta del ejercicio de derecho de los interesados y a garantizar el cumplimiento de las obligaciones relacionadas con las medidas de seguridad y las evaluaciones de impacto de privacidad.

- Eliminar o devolver los datos personales al responsable al finalizar los servicios y eliminar las copias existentes.

3.4. Autoridad de Control

La Autoridad de Control es la autoridad pública independiente establecida por un Estado miembro para el desarrollo de funciones que le atribuye la legislación vigente. En España, la Autoridad de Control es la Agencia Española de Protección de Datos ("**AEPD**").

El Grupo, dentro de sus relaciones con la AEPD, notificará las brechas de seguridad que puedan acontecerse, comunicará los datos al Delegado de Protección de Datos ("**DPD**") y los cambios que se realicen en cuanto a su figura, entre otras comunicaciones que puedan acontecerse en lo concerniente a consultas, etc.

3.5. Delegado de Protección de Datos

El RGPD y la LOPDPyGDD regulan la figura del DPD, cuyas funciones son las indicadas a continuación:

- Informar y asesorar al responsable del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que le incumben conforme a la normativa vigente en materia de protección de datos.

- Desempeño de una función preventiva y responsable, supervisando y coordinando la Política.

- Ejecutar y resolver en primera instancia los temas relacionados con la protección de datos.

- Supervisar el Registro de Actividades de Tratamiento.

- Asesoramiento y soporte en las evaluaciones de impacto.

- Comunicar las novedades legislativas en materia de protección de datos.

- Cualesquiera otras funciones que establezca la normativa aplicable o la presente Política.

El RGPD establece la obligación del responsable a garantizar la completa independencia del DPD, al mismo tiempo deberá proporcionar toda la información y medios que sean necesarios para el desempeño de su trabajo.

4. ÁMBITO OBJETIVO DE APLICACIÓN

La presente Política se aplica a todo tratamiento, total o parcial, realizado sobre datos personales o conjunto de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción, que utilizados por una o varias entidades del Grupo en calidad de responsables o corresponsables del tratamiento.

Asimismo, también resultará de aplicación respecto de cualquiera de las operaciones de tratamiento indicadas en el párrafo anterior en el que cualquier entidad del Grupo actúe como encargada del tratamiento respecto de otras entidades del Grupo o respecto de terceros.

5. NORMATIVA APLICABLE

Los textos normativos vigentes en materia de protección de datos son los indicados a continuación:

- 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**").

- Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 ("**Reglamento de Inteligencia Artificial**").

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales ("**LOPDPyGDD**").

- Ley 34/20022, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

- Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

Adicionalmente, se observarán las directrices, recomendaciones y otros actos que sean adoptados por el Comité Europeo de Protección de Datos ("**CEPD**") y el Supervisor Europeo de Protección de Datos ("**SEPD**").

Igualmente, se tendrán en cuenta las distintas circulares, informes jurídicos y resoluciones que emita la Agencia Europea de Protección de Datos ("**AEPD**") u otros organismos competentes como, por ejemplo, la Agencia Española de Supervisión de Inteligencia Artificial ("**AESIA**")

6. PRINCIPIOS GENERALES

El tratamiento de datos personales efectuado por las sociedades del Grupo deberá estar sujeto a los principios que se desarrollan a continuación:

6.1. Licitud del tratamiento

La normativa de protección de datos requiere que el tratamiento sea lícito, para ello, el Grupo se encargará de recabar el consentimiento del interesado u otra razón legítima contemplada en la legislación sobre protección de datos. El artículo 6 del RGPD recoge cinco razones lícitas para el tratamiento de datos personales, además del consentimiento: (i) ejecución de un contrato, (ii) cumplimiento de una misión en el ejercicio de los poderes públicos, (iii) cumplimiento de una obligación, (iv) interés legítimo.

6.2. Lealtad del tratamiento

El Grupo notificará a los interesados y al público en general que tratará los datos personales de manera lícita y transparente. Las operaciones del tratamiento no ser realizarán de forma secreta, debiendo los interesados ser conocedores de los riesgos potenciales.

6.3. Transparencia del tratamiento

El Grupo adoptará las medidas que sean apropiadas para mantener a los interesados informados acerca del uso de sus datos personales.

a) Principio de limitación de la finalidad

El Grupo realizará un tratamiento de datos personales con un fin perfectamente delimitado y que los fines adicionales solo sean compatibles con el fin original.

b) Principio de minimización de datos

El tratamiento de los datos personales que realice el Grupo debe limitarse a lo necesario para cumplir el fin legítimo. Este tratamiento solo puede llevarse a cabo cuando la finalidad de dicho tratamiento no se pueda cumplir razonablemente por otros medios. El tratamiento de los datos personales no podrá suponer en injerencia desproporcionada en los derechos e intereses y libertades.

c) Principio de exactitud de los datos

El Grupo garantizará la exactitud de todos los datos, de esta forma los datos inexactos deberán ser suprimidos o rectificados sin dilación. A veces, puede que sea necesario verificar los datos a fin de garantizar su exactitud.

d) Principio de limitación del plazo de conservación

El Grupo se encargará de suprimir o anonimizar los datos personales en el momento en que dejen de ser necesarios para los fines para los que fueron recabados.

e) Principio de integridad y confidencialidad

Los datos personales serán tratados por el Grupo con el propósito de garantizar 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 u organizativas apropiadas.

f) Principio de responsabilidad proactiva

El Grupo obliga a los responsables y encargados del tratamiento a adoptar medidas que fomenten, promuevan y garanticen la protección de los datos personales en sus actividades de tratamiento.

g) Protección de datos desde el diseño por defecto

El Grupo se encargará de aplicar medidas que salvaguarden el cumplimiento de los requisitos en materia de protección de datos personales. En este sentido, uno de los principales aspectos para implementar la protección de datos desde el diseño y por defecto es el siguiente:

- *Privacidad desde el diseño*: cuando el Grupo tenga previsto diseñar o elaborar un producto o servicio, deberá tenerse en cuenta desde su fase de elaboración todos los requisitos de información, consentimiento informado y demás obligaciones en materia de protección de datos.
- *Privacidad por defecto*: el Grupo debe procurar instaurar medidas que garanticen la protección de datos durante todo su ciclo de utilización, es decir, desde que son obtenidos hasta que dejan de tratarse, procurando el bloqueo y borrado de los mismos.

7. DEBER DE INFORMACIÓN Y DE LEGITIMACIÓN DEL TRATAMIENTO

Antes de tratar cualquier tipo de dato personal, las sociedades del Grupo deberán informar a los interesados de una forma simple, clara y fácil de entender, sobre todos aquellos aspectos relativos al tratamiento de sus datos personales.

De la misma forma, cuando los datos personales son obtenidos a través de terceros, también será necesario informar a los interesados.

En este sentido, para garantizar el deber de información el Grupo procederá a proporcionar a los interesados en primer lugar una primera capa de información y facilitará el acceso a una información más detallada respecto al tratamiento de los datos personales a través de una segunda capa.

En cuanto a la legitimación del tratamiento el Grupo procurará tener en cuenta las siguientes condiciones:

- *Consentimiento*: el Grupo debe procurar que el consentimiento de los interesados sea prestado por medio de un acto afirmativo, voluntario, claro e inequívoco. Y cuando la naturaleza de los datos así lo requieran, se procurará que el consentimiento sea expreso.
- *Otros medios de legitimación*: el Grupo podrá tratar los datos personales de los interesados conforme a los siguientes medios de legitimación: ejecución de un contrato, cumplimiento de una obligación legal, interés público o para fines de interés legítimo, siempre y cuando en este último caso no primen los derechos e intereses del interesado.

8. PROCEDIMIENTO DE GESTIÓN DE EJERCICIO DE DERECHOS

El Grupo tiene la obligación de informar a los interesados respecto del ejercicio de sus derechos, siendo estos los indicados a continuación:

- *Derecho de acceso*: los interesados tienen derecho a acceder a los datos personales que están siendo tratados.
- *Derecho de rectificación*: los interesados pueden rectificar cualquier dato personal que sea inexacto o incompleto, a fin de garantizar su exactitud y tratamiento adecuado.
- *Derecho de supresión*: los interesados tienen derecho a eliminar sus datos personales.
- *Derecho de oposición*: los interesados tienen derecho a oponerse al tratamiento de sus datos personales, en cualquier momento y sin justificar el motivo.
- *Derecho de limitación*: los interesados tienen derecho a la limitación del tratamiento de los datos personales que le conciernen.
- *Derecho a la portabilidad*: los interesados tienen derecho a recibir sus datos personales en un formato estructurado, de uso común y legible.
- *Derecho a un tratamiento automatizado*: los interesados tienen derecho a no estar sujetos a una decisión basada en un procedimiento automatizado, inclusive realización de perfiles. Esto incluirá aquellas actividades en las que el Grupo pueda evaluar a los clientes, predecir comportamientos, desempeño o preferencias, comparando su perfil con el de usuarios o clientes similares.

El ejercicio de derechos no conlleva contraprestación alguna para el interesado, solo en aquellos supuestos en los que las solicitudes sean infundadas excesivas o repetitivas. De esta forma el Grupo podrá cobrar el canon correspondiente a los costes generados dentro del ejercicio de derechos o negarse a la actuación de dicho derecho, siempre y cuando justifique tales evidencias.

El ejercicio de derechos puede dividirse en cuatro fases:

1. *SOLICITUD*

El interesado o el representante podrá solicitar el ejercicio de sus derechos por los siguientes canales:

Dirección correo electrónico:	protecciondedatos@sinerba.es
Dirección correo postal:	Avenida Los Vegas, 50, Cruz de Humilladero. CP:29006 (Málaga)

Conforme a la normativa aplicable, el contenido mínimo de las solicitudes debe ser:

- Nombre, apellidos, documento acreditativo de su identidad (copia DNI o NIE).
- Acreditación de que el representante actúe en nombre del interesado.
- Contenido de la solicitud (acceso, rectificación, supresión, etc.).
- Dirección de notificaciones, fecha y firma.

Si el solicitante no cumple los requisitos mínimos, la solicitud se rechazará y se le indicará al interesado la razón, requiriendo que subsane las deficiencias formales necesarias para procesar su ejercicio. Si la solicitud no es conforme a la normativa aplicable, se le informará al interesado de las circunstancias.

El DPD o responsable designado verificará el cumplimiento de los requisitos mínimos y la identidad del interesado. Si todo es correcto, se remitirá acuse de recibo.

2. *TRAMITACIÓN*

El DPD o el responsable designado analizará la solicitud para determinar si el ejercicio es procedente o no.

3. *RESPUESTA*

El DPD o responsable designado responderá a la solicitud conforme al plazo establecido en la normativa, pudiendo ser prorrogable por las razones aludidas en la norma. Se le facilitará toda la información que establezca el RGPD en un lenguaje claro, sencillo y conciso.

La prórroga del plazo de contestación y la negativa a la contestación del ejercicio debe comunicarse al interesado en los plazos previstos en la ley.

4. *REGISTRO*

Cada una de las solicitudes de ejercicio de derechos que hayan sido recibidas, se archivarán en los sistemas que posean las entidades del Grupo. Durante el plazo de conservación que prevea la normativa en materia de protección de datos.

9. MEDIDAS DE SEGURIDAD DE LOS DATOS PERSONALES

a) Medidas técnicas y organizativas

Los sistemas de seguridad tanto físicos como informáticos, contarán con mecanismos que protejan al Grupo de amenazas externas e internas. Los objetivos de los sistemas de seguridad serán los siguientes:

- ❖ Instaurar medidas de control necesarias al objeto de dar cumplimento a la normativa vigente en materia de protección de datos, así como en la prestación de servicios.

- ❖ Disponer de medidas que aseguren el acceso, integridad, confidencialidad, disponibilidad, autenticidad, trazabilidad de los datos y la prestación continuada de servicios.

- ❖ Proteger la infraestructura informática frente a amenazas.

b) Medidas jurídicas

Las medidas jurídicas previstas por el Grupo consistirán, generalmente, en:

- ❖ Instauración de políticas de privacidad, clausulados que informen respecto del tratamiento de sus datos personales a empleados, clientes, prestadores de servicio, etc.
- ❖ Contrato de encargado del tratamiento.
- ❖ Registro de actividades del tratamiento.

10. REGISTRO DE ACTIVIDADES DEL TRATAMIENTO

Las sociedades del Grupo disponen de un Registro de Actividades del Tratamiento de los datos que trata como responsable. Antes de introducir una nueva actividad de tratamiento se deberán realizar las siguientes actuaciones:

a) Analizar dicha actividad de tratamiento, con asesoramiento del DPD o responsable designado, al objeto de determinar si debe configurarse como una nueva actividad, si dispone de actualización de un tratamiento ya existente o si procede la supresión de la actividad.

b) Analizar si la nueva actividad se sostiene sobre una base de legitimación válida, así como si cumple con el resto de las obligaciones legales aplicables.

c) Determinar si la nueva actividad requiere o no de evaluación de impacto.

11. EVALUACIÓN DE PROVEEDORES

En la contratación de determinados prestadores de servicios, las distintas sociedades del grupo deberán evaluar las garantías que ofrecen en materia de privacidad, debiendo valorar según las circunstancias de cada caso si disponen de las siguientes medidas:

- ❖ Política de protección de datos.
- ❖ Existencia de DPD o responsable de la materia.
- ❖ Personal con formación en materia de privacidad.
- ❖ Clausulado de confidencialidad suscritas con los empleados.
- ❖ Procedimientos internos para la atención de reclamaciones efectuadas por los interesados.
- ❖ Subcontratación con terceros.
- ❖ Transferencias internacionales de datos.
- ❖ Historial de incidencias y brechas de seguridad.
- ❖ Historial de procedimientos e inspecciones ante la AEPD.

12. EVALUACIONES DE IMPACTO

Cuando sea probable que un tipo de tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable deberá, antes de efectuar el tratamiento, realizar una evaluación de impacto. El RGPD exige la realización de dicha evaluación en los siguientes supuestos:

- ❖ Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar.
- ❖ Tratamiento a gran escala de las categorías de datos o de los datos personales relativos a condenas e infracciones penales.
- ❖ Observación sistemática a gran escala en zona de acceso al público.

De esta forma, el Grupo en aquellos casos en los que la actividad objeto de tratamiento requiera de una previa evaluación de impacto, procederá a realizar el siguiente procedimiento:

1. Descripción: se procederá a efectuar un análisis descriptivo del tratamiento previsto y objeto de evaluación.
2. Valoración: se realizará una valoración sobre la prevalencia y proporcionalidad del tratamiento
3. Análisis: se ponderará los riesgos que suponen el tratamiento y las medidas de seguridad establecidas para mitigar los mismos, en su caso.

13. NOTIFICACIÓN DE BRECHAS DE SEGURIDAD

En el supuesto de que alguna de las sociedades del Grupo detecte una incidencia que haya sido ocasionada por una posible brecha de seguridad, se establecerá el siguiente procedimiento:

DETECCIÓN	La persona que detecte la incidencia deberá comunicar a la mayor brevedad posible la situación al DPD o responsable designado y a las personas responsables. Si se trata de un proveedor, deberá notificarlo en la mayor brevedad conforme dispone la normativa y el contrato suscrito entre la sociedad y el encargado del tratamiento.
TRAMITACIÓN	Se evaluará la situación y el DPD o responsable designado elaborará un informe de actuaciones con lo siguiente: - Descripción de los hechos. - Consecuencias de la incidencia. - Número de personas afectadas. - Categoría de datos afectados. - Evaluación de los riesgos para las personas afectadas. - Medidas correctoras para la eliminación de la brecha. - Medidas preventivas para evitar futuras incidências.
COMUNICACIÓN	Se comunicará la brecha de seguridad en el plazo establecido por la norma a la AEPD y a los afectados, si procediera por obligación legal.

REGISTRO	Cuando se detecte una brecha de seguridad se hará constar en un registro.

14. TRANSFERENCIAS INTERNACIONALES DE DATOS

Existiría una transferencia internacional de datos cuando alguna de las entidades del Grupo, como responsable del tratamiento, transfiera datos personales a otro responsable o encargado del tratamiento establecido en territorio ajeno a la Unión Europea. Debiendo seguir el presente procedimiento:

1. **COMUNICACIÓN** al DPD o a la persona responsable en materia de privacidad.
2. **ANÁLISIS** se evaluará la comunicación y los requisitos para realizar la transferencia incluyendo las medidas seguras y predictivas y la existencia de garantías adecuadas.
3. **EJECUCIÓN** se dará las instrucciones oportunas para la realización de la transferencia cumpliendo en todo momento con la normativa vigente en materia de protección de datos.

15. INTELIGENCIA ARTIFICIAL

Teniendo en cuenta el creciente empleo de los sistemas de Inteligencia Artificial ("**IA**") en el sector privado y las obligaciones de cumplimiento previstas en el Reglamento de Inteligencia Artificial, la inclusión o empleo de datos personales a través de herramientas de IA deberán quedar sujetas a la normativa vigente en materia de protección de datos personales, garantizando el cumplimiento de los principios relativos al tratamiento de datos personales, así como la adopción de medidas y de procedimientos que sean necesarios.

16. APROBACIÓN Y MODIFICACIÓN DE LA POLÍTICA

Las modificaciones realizadas en la Política se harán a propuesta del DPD o del responsable designado, el cual se encargará de asesorar y dar soporte en la redacción de nuevos términos y modificados y aprobadas por el responsable del tratamiento, en este caso el Grupo.

17. CONTROL DE CAMBIOS Y APROBACIÓN

Versión	Fecha	Descripción	Autor	Estado	Aprobado
v.0	[*]	Versión inicial	[*]	[*]	[*]