POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

Código:	02.1
Versión:	0
Fecha de la versión:	23/05/19
Creado por:	Responsable de Seguridad
Aprobado por:	Responsable de Fichero
Nivel de confidencialidad:	Público

Historial de cambios

Fecha	Versión	Creado por	Descripción del cambio
0103/18	0	Resp. Seguridad	Descripción básica del documento

1. Propósito, alcance y usuarios

ASOCIACION DE FAMILIARES DE ENFERMOS DE ALZHEIMER Y OTRAS DEMENCIAS DE LLERENA Y COMARCA, en lo sucesivo, la "Empresa", se esfuerza por cumplir con las leyes y reglamentos aplicables relacionadas con la protección de datos personales en los países donde opera. Esta política establece los principios básicos por los cuales la Empresa trata los datos personales de consumidores, clientes, proveedores, socios comerciales, empleados y otras personas, e indica las responsabilidades de sus departamentos comerciales y empleados mientras trata los datos personales.

Esta política se aplica a la Empresa y sus subsidiarias controladas de forma directa o indirecta que realizan negocios dentro del Área Económica Europea (AEE) o procesan los datos personales de los interesados dentro del AEE.

Los usuarios de este documento son todos los empleados, permanentes o temporales, y todos los contratistas que trabajan en nombre de la Compañía.

2. Documentos de referencia

- El RGPD UE 2016/679 (Reglamento (EU) 2016/679 del Parlamento Europeo y del Consejo del 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)
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 1720/2007, de 21 de diciembre, Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (RLOPD).
- Política de protección de datos personales de los empleados
- Política de retención de datos
- Descripción del puesto de delegado de protección de datos
- Directrices para el inventario de datos y actividades de tratamiento
- Procedimiento de solicitud de acceso de los interesados
- Directrices para la evaluación de impacto de protección de datos
- Procedimiento de transferencia transfronteriza de datos personales
- Políticas de seguridad de la información
- Procedimiento de aviso de violación de seguridad

3. Definiciones

Las siguientes definiciones de términos utilizados en este documento provienen del Artículo 4 del Reglamento General de Protección de Datos de la Unión Europea:

Datos personales: toda información sobre una persona física identificada o identificable("**Interesado**") 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.

Datos personales sensibles: Datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. Debe incluirse entre tales datos personales los datos de carácter personal que revelen el origen racial o étnico, opiniones políticas, convicciones religiosas o filosóficas, afiliaciones sindicales, datos genéticos, datos biométricos, dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.

Responsable de los datos: La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

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

Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos 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.

Anonimización: Eliminar de forma irreversible la identificación de datos personales de modo que la persona no pueda ser identificada utilizando un tiempo, coste y tecnología razonables, ya sea por el responsable o por cualquier otra persona para identificar a ese individuo. Los principios de tratamiento de datos personales no se aplican a datos anónimos ya que ya no son datos personales.

Seudonimización: El tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable. La seudonimización reduce, pero no elimina completamente, la capacidad de asociar datos personales a un interesado. Como los datos seudonimizados aún se consideran datos personales, el tratamiento de estos datos debe de cumplir con los principios de tratamiento de datos personales.

Tratamiento transfronterizo de datos personales: El tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro; o el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro.

Autoridad de control: la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51;

Autoridad principal de control: La autoridad de control con la responsabilidad principal de tratar con una actividad de tratamiento de datos transfronterizos, por ejemplo cuando un interesado presenta una reclamación sobre el tratamiento de sus datos personales; es responsable, entre otros, de recibir los avisos de violación de seguridad de datos, ser notificado sobre la actividad de tratamiento de riesgo y tendrá plena autoridad en lo que respecta a sus deberes para garantizar el cumplimiento de las disposiciones del RGPD UE.

Cada **"autoridad de control local"** mantendrá en su propio territorio y supervisará cualquier tratamiento de datos local que afecte a los interesados o que sea realizado por un responsable o encargado de la UE, o no perteneciente a la UE, cuando el tratamiento se dirige a interesados que residan en su territorio. Sus tareas y poderes incluyen llevar a cabo investigaciones y aplicar medidas administrativas y multas, promover la conciencia pública sobre los riesgos, reglas, seguridad y derechos en relación con el tratamiento de datos personales, así como obtener acceso a las instalaciones del responsable y el encargado, incluido cualquier equipo y medio de tratamiento de datos.

"Principal establecimiento con respecto a un responsable" con establecimientos en más de un estado miembro, es decir el lugar de su administración central en la Unión, a menos que las decisiones sobre los fines y los medios del tratamiento de datos personales se tomen en otro establecimiento del responsable del tratamiento en la Unión y este último tenga el poder para que se implementen tales decisiones, en cuyo caso el establecimiento que haya tomado tales decisiones se debe considerar como el establecimiento principal.

"Principal establecimiento con respecto a un encargado" con establecimientos en más de un estado miembro, es decir el lugar de su administración central en la Unión o, si el encargado careciese de una administración central en la Unión, el lugar en el que se lleven a cabo las principales actividades de tratamiento en el contexto de la las actividades de un establecimiento del encargado tienen lugar en la medida en que el encargado está sujeto a obligaciones específicas en virtud del presente Reglamento.

Grupo empresarial: Cualquier holding junto con su subsidiaria.

4. Principios básicos sobre el tratamiento de datos personales

Los principios de protección de datos describen las responsabilidades básicas de las organizaciones que tratan datos personales. El artículo 5 (2) del RGPD estipula que *"el responsable del tratamiento será responsable del cumplimiento de los principios y será capaz de demostrarlo"* de:

4.1. Legalidad, imparcialidad y transparencia

Los datos personales deben ser tratados de forma legal, imparcial y transparente en relación al interesado.

4.2. Limitación de la finalidad

Los datos personales deben ser recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.

4.3. Minimización de los datos

Los datos personales deben de ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. La Empresa debe aplicar anonimización o seudonimización a los datos personales si es posible para reducir el riesgo concerniente a los interesados.

4.4. Exactitud

Los datos personales deben ser exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

4.5. Limitación del plazo de conservación

Los datos personados no deben ser conservados más de lo necesario para los fines para los cuales los datos personales son tratados.

4.6. Integridad y confidencialidad

Teniendo en cuenta el estado de la tecnología y otras medidas de seguridad disponibles, el coste de implementación y la probabilidad y gravedad de los riesgos de los datos personales, la Empresa debe aplicar medidas técnicas u organizativas apropiadas para tratar los datos personales, de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental.

4.7. Responsabilidad proactiva

Los responsables del tratamiento serán responsables del cumplimiento de los principios descritos anteriormente y serán capaces de demostrarlo.

5. Desarrollo de protección de datos en actividades empresariales

Para poder demostrar el cumplimiento con los principios de protección de datos, una organización tiene que desarrollar la protección de datos en sus actividades empresarial.

5.1. Aviso a los interesados

(Ver directrices de tratamiento lícito.)

5.2. Elección y consentimiento del interesado

(Ver directrices de tratamiento lícito.)

5.3. Recogida

La empresa debe esforzarse por recoger la menor cantidad posible de datos personales. Si los datos personales se recogen de un tercero, el Responsable de Seguridad debe de asegurar que los datos personales son recogidos legalmente.

5.4. Uso, retención, y eliminación

La finalidad, los métodos, la limitación de almacenamiento y el período de retención de datos personales deben ser coherentes con la información contenida en el Aviso de privacidad. La Compañía debe mantener la precisión, integridad, confidencialidad y pertinencia de los datos personales en función de la finalidad del tratamiento. Se deben utilizar mecanismos de seguridad adecuados diseñados para proteger los datos personales para evitar el robo, uso indebido o abuso de los datos personales y evitar violaciones de seguridad de datos personales. Responsable de Seguridad es responsable del cumplimiento de los requisitos enumerados en esta sección.

5.5. Comunicación a terceros

Siempre que la Empresa utilice un proveedor externo o un socio empresarial para tratar datos personales en su nombre, el Responsable de Seguridad debe asegurar que este encargado proporcionará medidas de seguridad para salvaguardar los datos personales que sean adecuadas a los riesgos asociados. Para tal fin, debe usarse el Cuestionario de cumplimiento del RGPD del encargado.

La Empresa debe exigir de forma contractual al proveedor o al socio empresarial que proporcione el mismo nivel de protección de datos. El proveedor o socio empresarial sólo debe tratar los datos personales para cumplir sus obligaciones contractuales con la Empresa o siguiendo las indicaciones de la Empresa y no para otros fines. Cuando la Empresa trate datos personales junto con un tercero independiente, la Empresa debe especificar de manera explícita sus respectivas responsabilidades y las de un tercero en el pertinente contrato o cualquier otro documento legal vinculante, como el Acuerdo de tratamiento de datos del proveedor.

5.6. Transferencia transfronteriza de datos personales

Antes de transferir datos personales fuera del Área Económica Europea (AEE) deben de emplearse garantías adecuadas incluida la firma de un acuerdo de transferencia de datos, tal como indica la Unión Europea y, si es necesario, debe obtenerse la autorización de la autoridad de protección de datos correspondiente. La entidad que recibe los datos personales debe cumplir con los principios de tratamiento de datos personales establecidos en el Procedimiento de transferencia de datos transfronterizos.

5.7. Derechos de acceso de los interesados

Al actuar como responsable de los datos, el Responsable de Seguridad es responsable de proporcionar a los interesados un mecanismo de acceso razonable que les permita acceder a sus datos personales, así como actualizar, rectificar, borrar o transmitir sus datos personales, cuando corresponda o sea requerido por la ley. El mecanismo de acceso se detallará más en el procedimiento de solicitud de acceso al interesado.

5.8. Portabilidad de datos

Los sujetos de los datos tienen derecho a recibir, previa solicitud, una copia de los datos que nos proporcionaron en un formato estructurado y a transmitir esos datos a otro responsable, de forma gratuita. El Responsable de Seguridad es responsable de garantizar que dichas solicitudes se procesen en un mes, que no sean excesivas y que no afecten a los derechos de los datos personales de otras personas.

5.9. Derecho al olvido

Previa solicitud, los interesados tienen derecho a obtener de la empresa el borrado de sus datos personales. Cuando la Empresa actúa como responsable, el Responsable de Seguridad debe tomar las medidas necesarias (incluidas medidas técnicas) para informar a terceros que usan o procesan esos datos para cumplir con la solicitud.

6. Directrices de tratamiento lícito

Los datos personales deben ser tratados sólo cuando sea autorizado de forma explícita por El Responsable de Seguridad.

La Empresa debe decidir si realizar la evaluación de impacto de protección de datos para cada actividad de tratamiento de datos de acuerdo con Directrices de evaluación de impacto de protección de datos.

6.1. Aviso a los interesados

En el momento de la recogida o antes de recoger datos personales para cualquier tipo de actividades de tratamiento, incluidas, entre otras, la venta de productos, servicios o actividades comerciales, el Responsable de Seguridad es responsable de informar adecuadamente a los interesados sobre los siguientes tipos de datos personales: los tipos de datos personales recogidos, los fines del tratamiento, los métodos de tratamiento, los derechos de los interesados con respecto a sus datos personales, el período de retención, las posibles transferencias de datos internacionales, si los datos serán compartidos con terceros y las medidas de seguridad de la Empresa para proteger los datos personales. Esta información es proporcionada a mediante un aviso de privacidad.

Si tu empresa tiene múltiples actividades de tratamiento de datos, necesitarás desarrollar avisos diferentes que variarán dependiendo de la actividad de tratamiento y de las categorías de datos personales recogidos; por ejemplo, un aviso puede escribirse para envío por correo electrónico y otro diferente para envío postal.

Cuando los datos personales son compartidos con un tercero, el Responsable de Seguridad debe asegurarse de que los interesados han sido notificados de ello mediante un aviso de privacidad.

Cuando los datos personales se transfieren a un tercer país de acuerdo con la política de transferencia transfronteriza de datos, el aviso de privacidad debe reflejar esto e indicar claramente dónde y a qué entidad se transfieren los datos personales.

Cuando se recogen datos personales confidenciales, el delegado de protección de datos debe asegurarse de que el Aviso de privacidad indique de forma explícita el propósito para el que se recopilan estos datos personales sensibles.

6.2. Obtención del consentimiento

Siempre que el tratamiento de datos personales se base en el consentimiento del interesado u otros motivos legales, el Responsable de Seguridad es responsable de conservar un registro de dicho consentimiento. el Responsable de Seguridad es responsable de facilitar a los interesados las opciones para proporcionar el consentimiento y debe informar y garantizar que su consentimiento (siempre que se utilice el consentimiento como base legal para el tratamiento) pueda retirarse en cualquier momento.

Cuando la recogida de datos personales se relaciona con un niño menor de 16 años, el Responsable de Seguridad debe asegurarse que el consentimiento paterno se entrega antes de la recogida utilizando la solicitud de consentimiento paterno (el artículo 8 del RGPD establece que "el responsable del tratamiento hará todo lo posible para verificar los casos en el que el titular de la patria potestad dé o autorice el consentimiento del niño, teniendo en cuenta la tecnología disponible".)

Cuando existan solicitudes para corregir, modificar o destruir los registros de datos personales, el Responsable de Seguridad debe asegurarse de que estas solicitudes se tramiten dentro de un marco de tiempo razonable. El Responsable de Seguridad también debe registrar las solicitudes y mantener un registro de éstas.

Los datos personales solo se deben tratar para el propósito para el que se recogieron inicialmente. En el caso de que la Empresa quiera tratar los datos personales recogidos para otro fin, la Empresa debe buscar el consentimiento de sus interesados en un escrito claro y conciso. Cualquier solicitud de este tipo debe incluir la finalidad inicial para la que se recogieron los datos, y también el (los) nuevo (s) fin (es) adicional (es). La solicitud también debe incluir el motivo del cambio en la (las) finalidad (es). El Responsable de Seguridad es responsable de cumplir con las reglas de este párrafo.

Ahora y en el futuro, el Responsable de Seguridad debe garantizar que los métodos de recogida cumplan con las leyes pertinentes, las buenas prácticas y los estándares de la industria.

El Responsable de Seguridad es responsable de crear y conservar un registro de los avisos de privacidad.

El consentimiento para la comunicación de los datos de carácter personal a un tercero será nulo cuando la información que se facilite al interesado no le permita conocer la finalidad a que se destinarán los datos cuya comunicación se autoriza, o el tipo de actividad de aquel a quien se pretenden comunicar.

Un caso especial de comunicación es el acceso por cuenta de terceros vinculados al negocio. No se considerará comunicación de datos el acceso de un tercero a la información cuando dicho acceso sea necesario para la prestación de un servicio a la empresa.

La realización de tratamientos por cuenta de terceros tiene que estar regulada en un contrato que deberá constar por escrito, o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad que el encargado del tratamiento está obligado a implementar e indicaciones de cualquier otra índole sobre el tratamiento de los datos.

Como ya se ha visto, una pieza fundamental, tanto en el tratamiento como en la comunicación de datos de carácter personal es el consentimiento del afectado. Según la normativa vigente, el tratamiento de los datos de carácter personal, así como su cesión, requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.

No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

Es decir, no se necesitará recabar el consentimiento de los clientes para tratar sus datos personales al objeto de prestar representación jurídica o cualquier otro servicio, o para dar traslado de esos datos a la Administración Pública, siempre y cuando no se usen con ningún otro fin. Tampoco se necesitará el consentimiento del cliente cuando terceros deban acceder a esa información en el marco de una prestación de servicios a la empresa. Eso sí, deberá delimitar el alcance y responsabilidades en el correspondiente contrato de servicios.

En los casos en los que se debe comunicar a un tercero esos datos, como, por ejemplo, a una empresa de fuerza de ventas, sí debe recabarse el consentimiento del cliente. Dicho consentimiento debe ser:

- Libre, lo que supone que deberá haber sido obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por el Código Civil.
- Específico, es decir, referido a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del tratamiento
- Informado, es decir que el afectado conozca, con anterioridad a la operación para la que se le solicita consentimiento, las finalidades para las que se le pide autorización.
- Inequívoco, lo que implica que no resulta admisible deducir el consentimiento de los meros actos realizados por el afectado (consentimiento presunto), siendo preciso que exista expresamente una acción u omisión que implique la existencia del consentimiento.

De lo que se ha indicado no se desprende que el consentimiento deba ser expreso en todo caso, razón por la cual en aquellos supuestos en que el legislador ha pretendido que el consentimiento deba revestir ese carácter, lo ha indicado expresamente. Así sucede en el caso de tratamiento de datos

especialmente protegidos, indicando el artículo 7.2 la necesidad de consentimiento expreso y escrito para el tratamiento de los datos de ideología, religión, creencias y afiliación sindical, y el artículo 7.3 la necesidad de consentimiento expreso aunque no necesariamente escrito para el tratamiento de los datos relacionados con la salud, el origen racial y la vida sexual.

Por tanto, el consentimiento podrá ser tácito, en el tratamiento de datos que no sean especialmente protegidos (artículo 7.2 y 7.3 de la Ley Orgánica 15/1999) si bien para que ese consentimiento tácito pueda ser considerado inequívoco será preciso otorgar al afectado un plazo prudencial para que pueda claramente tener conocimiento de que su omisión de oponerse al tratamiento o la cesión de datos implica un consentimiento al mismo, no existiendo al propio tiempo duda alguna de que el interesado ha tenido conocimiento de la existencia del tratamiento o cesión de datos y de la existencia de ese plazo para evitar que se proceda al mismo.

El tratamiento de datos sin consentimiento previo del afectado en aquellos supuestos no exceptuados legalmente, puede ser motivo de infracción grave.

7. Organización y responsabilidades

La responsabilidad de garantizar el tratamiento adecuado de los datos personales recae en todos los que trabajan para la Empresa o con ella y tienen acceso a los datos personales tratados por la Empresa.

Las áreas clave de responsabilidades para el tratamiento de datos personales recaen sobre los siguientes puestos de la organización:

La Dirección toma decisiones y aprueba las estrategias generales de la Empresa en temas de protección de datos personales.

El **delegado de protección de datos (DPD) o el Responsable de Seguridad,** es responsable de gestionar el programa de protección de datos personales y del desarrollo y promoción de políticas de protección integral de datos personales, como se define en la descripción de puesto de delegado de protección de datos;

El **Departamento/asesor de asuntos legales junto con el delegado de protección de datos,** supervisa y analiza los cambios en las leyes y reglamentos sobre datos personales, desarrolla el cumplimiento de los requisitos, y ayuda a los departamentos comerciales en alcanzar sus objetivos de datos personales.

El **responsable de mantenimiento,** es responsable de:

- Asegurar todos los sistemas, servicios y equipo utilizado para el almacenamiento de datos cumplan con estándares de seguridad aceptables.
- Llevar a cabo comprobaciones y escaneos regulares para asegurar que el hardware y el software funcionan correctamente.

El **Responsable Comercial**, es responsable de:

- Aprobar cualquier declaración de protección de datos incluida en comunicaciones tales como correos electrónicos y cartas.

- Abordar cualquier consulta de protección de datos de periodistas o medios de comunicación como periódicos.
- Cuando sea necesario, trabajar con el delegado de protección de datos para garantizar que las iniciativas de marketing cumplan con los principios de protección de datos.

El **responsable de recursos humanos** es responsable de:

- Mejorar el conocimiento de todos los empleados sobre la protección de datos personales del usuario.
- Organizar formaciones sobre conocimiento especializado y concienciación en materia de protección de datos personales para los empleados que trabajan con datos personales.
- La protección integral de datos personales de los empleados. Debe asegurar que los datos personales de los empleados se traten en base a fines y necesidades de negocio legítimas del empresario.

El **responsable de compras** es responsable de transmitir las responsabilidades de protección de datos personales a los proveedores, y mejorar los niveles de conocimiento de los proveedores en materia protección de datos personales, así como reducir los requisitos de datos personales a cualquier tercero que esté utilizando un proveedor. El departamento de compras debe asegurar que la Empresa se reserva el derecho a auditar a sus proveedores.

8. Directrices para establecer la autoridad de control principal

8.1. La necesidad de establecer la autoridad de control principal

El nombramiento de una autoridad de control principal es sólo pertinente si la Empresa lleva a cabo tratamiento transfronterizo de datos personales.

El tratamiento de datos transfronterizos se lleva a cabo si:

a) *el tratamiento de los datos personales se lleva a cabo por las filiales de la Empresa que tienen su sede en otros estados miembros;*

o

b) *el tratamiento de datos personales que tiene lugar en un establecimiento único de la Empresa en la Unión Europea, pero que afecta sustancialmente o puede afectar sustancialmente a los interesados en más de un estado miembro.*

Si la empresa solo tiene establecimientos en un Estado miembro y sus actividades de tratamiento afectan únicamente a los interesados en ese Estado miembro, no es necesario establecer una autoridad de control principal. La única autoridad competente será la autoridad de control en el país donde la Empresa está legalmente establecida.

8.2. El establecimiento principal y la autoridad de control principal

8.2.1. Establecimiento principal del responsable de los datos

La dirección de la Empresa necesita identificar su sede principal para que pueda determinarse la autoridad de control principal.

Si la Empresa se encuentra en un estado miembro de la EU y toma decisiones relacionadas con actividades de tratamiento transfronterizas en el lugar de su sede principal, existirá una sola autoridad de control principal para las actividades de tratamiento de datos llevadas a cabo por la Empresa.

Si la empresa tiene múltiples establecimientos que actúan de manera independiente y que toman decisiones sobre los fines y medios de tratamiento de tratamiento de datos personales, la dirección de la Empresa necesita reconocer que existe más de una autoridad de control principal.

8.2.2. Establecimiento principal del encargado de los datos

Cuando la Empresa actúa como un encargado de datos, entonces el principal establecimiento será el lugar de la administración central. En caso de que el lugar de la administración central no se localice en la UE, el establecimiento principal se establecerá donde se lleven a cabo las principales actividades en la UE.

8.2.3. Establecimiento principal de responsables y encargados para empresas fuera de la UE

Si la Empresa no tiene un establecimiento principal en la UE, y tiene filial (es) en la UE, entonces la autoridad de control competente es la autoridad de control local.

Si la Empresa no tiene un establecimiento principal en la UE ni tampoco filiales, debe de nombrar un representante en la EU, y la autoridad local competente será la autoridad de control local donde se localiza el representante.

9. Respuesta a violaciones de seguridad de datos.

Cuando la Empresa se percata de una violación de seguridad de datos personales tanto presunta como real, el Responsable de Seguridad debe realizar una investigación interna y tomar las medidas correctivas adecuadas a tiempo, de acuerdo con la política de violación de seguridad de datos. Cuando exista un riesgo para los derechos y las libertades de los interesados, la Compañía debe notificar a las autoridades de protección de datos relevantes sin dilación indebida y, cuando sea posible, dentro de las 72 horas.

10. Auditoria y responsabilidad proactiva

El Responsable de Seguridad es responsable de auditar si todos los departamentos implementan esta política de seguridad de datos personales, lo que podrá hacer mediante la contratación de auditores externos.

Cualquier empleado que viole esta política estará sujeto a medidas disciplinarias y el empleado también puede estar sujeto a responsabilidades civiles o penales si su conducta viola leyes o reglamentos.

11. Conflictos de legislación

Esta política está destinada a cumplir con las leyes y reglamentos en el lugar de establecimiento y de los países en los que opera ASOCIACION DE FAMILIARES DE ENFERMOS DE ALZHEIMER Y OTRAS DEMENCIAS DE LLERENA Y COMARCA. En caso de conflicto entre esta política y las leyes y reglamentos aplicables, prevalecerá esta última.

12. Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación	Persona responsable de su almacenamiento	Controles para la protección de registros	Tiempo de retención
solicitud de consentimiento del interesado	Carpeta RGPD	Delegado de protección de datos o Responsable de Seguridad	Sólo personal autorizado puede acceder a las solicitudes	10 años
Solicitud de retirada del consentimiento del interesado	Carpeta RGPD	Delegado de protección de datos o Responsable de Seguridad	Sólo personal autorizado puede acceder a las solicitudes	10 años
Solicitud de consentimiento paterno	Carpeta RGPD	Delegado de protección de datos o Responsable de Seguridad	Sólo personal autorizado puede acceder a las solicitudes	10 años
Solicitud de retirada del consentimiento paterno	Carpeta RGPD	Delegado de protección de datos o Responsable de Seguridad	Sólo personal autorizado puede acceder a las solicitudes	10 años

Nombre del registro	Ubicación	Persona responsable de su almacenamiento	Controles para la protección de registros	Tiempo de retención
Acuerdos de tratamiento de datos del proveedor	Carpeta RGPD	Delegado de protección de datos o Responsable de Seguridad	Sólo personal autorizado puede acceder la carpeta	5 años después de que el acuerdo haya expirado
Registro de avisos de privacidad	Carpeta RGPD	Delegado de protección de datos o Responsable de Seguridad	Sólo personal autorizado puede acceder la carpeta	Permanente

13. Validez y gestión de documentos

Este documento es válido a partir de 23/05/19.

El propietario de este documento es el Responsable de Seguridad, que debe revisar y, si fuera necesario, actualizar el documento al menos una vez al año.

El Responsable de Seguridad

EVA MARIA ZAMBRANO PACHÓN