Evaluación de cumplimiento normativo y riesgos de protección de datos

Reglamento General UE 679/2016 de Protección de Datos y Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de derechos digitales

FUNDACIÓ PRIVADA VIA-GUASP PER A LA TUTELA DEL MALALT MENTAL

18 de mayo de 2022

Tabla de contenidos

0 Introducción ... 3
0.1 Objetivo del informe ... 3
0.2 Alcance del informe ... 3
0.3 Codificación de las valoraciones y recomendaciones ... 3
0.4 Resumen ejecutivo y tabla de deficiencias y observaciones ... 4
1 Medidas de responsabilidad proactiva ... 5
1.1 Identificación de tratamientos como responsable y como encargado ... 5
1.2 Protección de datos en el diseño y por defecto ... 7
1.3 Publicación del registro de actividades de tratamiento ... 8
1.4 Evaluación de impacto y consulta previa ... 9
1.5 Tratamientos como encargado: contrato e instrucciones ... 13
1.6 Corresponsables del tratamiento ... 13
2 Principios de protección de datos ... 15
2.1 Licitud (legitimación) y transparencia (información a los interesados) ... 15
2.2 Minimización de datos, exactitud y limitación de plazo ... 22
2.3 Confidencialidad y deber de secreto ... 24
2.4 Derechos de acceso, rectificación, supresión y demás ... 25
3 Prestaciones de servicio recibidas ... 29
3.1 Firma de contratos con los encargados de tratamiento ... 29
4 Funciones y obligaciones del personal ... 32
4.1 Delegado de protección de datos ... 32
4.2 Delegación de las funciones de control de la seguridad de datos ... 35
4.3 Conocimiento del personal de las normas de seguridad que les afectan ... 35
5 Aplicación de las medidas de seguridad ... 37
5.1 Medidas relacionadas con la gestión de los soportes ... 37
5.2 Medidas relacionadas con el control de acceso a la información ... 38
5.3 Medidas relacionadas con copia respaldo y la disponibilidad de los sistemas ... 38
5.4 Medidas relacionadas con el uso de redes informáticas ... 39
5.5 Medidas relacionadas con el malware ... 39
5.6 Medidas relacionadas con la documentación (papel) ... 39
5.7 Gestión de incidencias de seguridad ... 40
6 Notificación de las violaciones de seguridad ... 41
6.1 Notificaciones a las autoridades y a los interesados ... 42
6.2 Notificaciones al responsable del tratamiento ... 42
7 Transferencia internacional de datos ... 43
7.1 Transferencias fuera del EEU conforme al RGPD ... 47

0 Introducción

0.1 Objetivo del informe

El objetivo del presente informe es recoger el resultado de la auditoría de cumplimiento de:

- **Reglamento General de Protección de Datos, en vigor a partir del 25 de mayo de 2018 (RGPD)**.
- **Nueva Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de derechos digitales (LOPDGDD), en vigor desde el 6 de diciembre de 2018.**

Cabe destacar que la Agencia Española de Protección de Datos tiene potestad sancionadora en materia de protección de datos.

0.2 Alcance del informe

El alcance del informe incluye los ficheros que contienen datos de carácter personal, los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal:

SOCIEDADES	FUNDACIÓ PRIVADA VIA-GUASP PER A LA TUTELA DEL MALALT MENTAL
WEB	https://via-guasp.com/

A continuación, se indica la fecha de realización de los chequeos, los centros de trabajo visitados y el personal involucrado.

FECHA	18 de mayo de 2022
CENTROS DE TRABAJO	Passeig de Maragall, 130 08027, Barcelona
PERSONAL INVOLUCRADO	FUNDACIÍ VÍA GUASP: Elena Gómez PRODAT: Mar Varea

Debe señalarse que el presente análisis se ha realizado en base a la toma de muestras. Por tanto, podrían existir deficiencias que no hayan sido detectadas y que por tanto no se incluyan en el mismo.

0.3 Codificación de las valoraciones y recomendaciones

Este informe incluye chequeos de auditoría relativos a cumplimiento normativo, que se señalan mediante el siguiente código de colores:

🔴	Incumplimiento
🟡	Cumplimiento parcial
🟢	Cumplimiento
🔵	Observaciones y recomendaciones

0.4 Resumen ejecutivo y tabla de deficiencias y observaciones

Tabla de deficiencias y observaciones

Apartado	Chequeo	Observación o incumplimiento	
2.1.2.1	Se cuenta con una legitimación válida para todos los tratamientos de datos personales de la organización	Se deberá revisar la página web en busca de fotografías en las que salgan personas que no prestaron su consentimiento para ello Se deberá revisar también para el caso de las fotografías colgadas en los tablones de la entrada del edificio. En caso de no poder identificar quién prestó y quién no su consentimiento, se deberá proceder a descolgar todas las fotografías	🟡
2.1.2.2	Se proporciona la información necesaria para cumplir los requisitos de información del RGPD	Se recuerda que se deberá sustituir el cartel de videovigilancia actual por el actualizado (RGPD)	🔴
2.2.2.4	Correcta aplicación de los plazos de conservación	Se deberá proceder a la destrucción de documentos muy antiguos, en especial los expedientes de pacientes que hace mucho que no han requerido de los servicios de la Fundación, así como los pacientes difuntos	🔴
2.3.2.2	El deber de secreto también afecta a personal externo, prestadores de servicios, estudiantes en prácticas, etc.	Se recuerda que tanto los estudiantes en prácticas como los voluntarios deberán firmar también el documento de protección de datos	🟡
3.1.2.1	Disponen de los contratos pertinentes para regular las prestaciones de servicio que conllevan un tratamiento de datos personales, adaptados al RGPD	Se recuerda a la Fundación, que se deberá enviar copia del contrato de encargado firmado por Víctor Martínez Cervera y Enrica Corominas	🔵
5.2	Medidas relacionadas con el control de acceso a la información	Se recuerda a la Fundación que se deberá proporcionar una contraseña a todos los nuevos empleados/estudiantes en prácticas/voluntarios, y éstos deberán modificarla una vez recibido el dispositivo Disconformidad: Se debe cambiar la contraseña del Wifi como mínimo, una vez al año. Actualmente, la contraseña del Wifi es la que vino por defecto, la de origen	🔴
5.4	Medidas relacionadas con el uso de redes informáticas	Se recomienda a la Fundación que activen la opción de realizar escaneos diarios a través del antivirus instalado en su equipo	🔵

1 Medidas de responsabilidad proactiva

1.1 Identificación de tratamientos como responsable y como encargado

El RGPD elimina la obligación de notificar los ficheros a la Agencia Española de Protección de Datos, pero introduce la obligación de realizar un registro de las actividades de tratamiento de datos personales, que debe recoger tanto las actividades que se realizan como responsable como aquellas que se realizan como encargados.

Artículo 30.1 del RGPD. Registro de las actividades de tratamiento

1. Cada responsable y, en su caso, su representante llevará un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:

a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;
b) los fines del tratamiento;
c) una descripción de las categorías de interesados y de las categorías de datos personales;
d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.

Además, el RGPD exige que el Registro de Actividades de Tratamiento incluya también las actividades realizadas en calidad de encargados.

Artículo 30.2 del RGPD. Registro de las actividades de tratamiento

2. Cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:

a) el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;
b) las categorías de tratamientos efectuados por cuenta de cada responsable;
c) en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30, apartado 1.

1.1.1 Situación actual

La siguiente tabla describe las actividades de tratamiento realizadas como RESPONSABLES.

ACTIVIDAD DE TRATAMIENTO DE DATOS	FINALIDAD	CATEGORÍAS DE INTERESADOS Y TIPOS DE DATOS	DESTINATARIOS Y TRANSFERENCIAS	NIVEL DE RIESGO
COMUNICACIÓN Y PUBLICIDAD	Publicidad y prospección comercial; Comercio electrónico	Clientes y usuarios; Proveedores; Asociados o miembros; Pacientes / Información comercial	Organizaciones o personas directamente relacionadas con el responsable	BAJO
CONTABILIDAD	Gestión de clientes, contable, fiscal y administrativa	Empleados; Clientes y usuarios; Proveedores / Detalles del empleo; Económicos, financieros y de seguros	Organizaciones o personas directamente relacionadas con el responsable; Organismos de la seguridad social; Administración tributaria; Bancos, cajas de ahorros y cajas rurales	BAJO
CONTABILIDAD TUTELADOS	Gestión de clientes, contable, fiscal y administrativa	Clientes y usuarios; Pacientes / Económicos, financieros y de seguros	Organizaciones o personas directamente relacionadas con el responsable; Administración tributaria; Bancos, cajas de ahorros y cajas rurales	BAJO
DONANTES	Gestión de clientes, contable, fiscal y administrativa	Clientes y usuarios / Económicos, financieros y de seguros	Organizaciones o personas directamente relacionadas con el responsable	BAJO
EXPEDIENTE TUTELADOS O PRE-TUTELADOS	Gestión de asistencia social; Educación; Gestión y control sanitario	Clientes y usuarios; Pacientes / Características personales; Circunstancias sociales; Académicos y profesionales; Detalles del empleo	Organizaciones o personas directamente relacionadas con el responsable; Organismos de la seguridad social; Asociaciones y organizaciones sin ánimo de lucro	ALTO
NÓMINAS, PERSONAL Y RRHH	Recursos humanos; Gestión de nóminas	Empleados / Características personales; Circunstancias sociales; Académicos y profesionales; Detalles del empleo	Organizaciones o personas directamente relacionadas con el responsable; Organismos de la seguridad social; Administración tributaria; Bancos, cajas de ahorros y cajas rurales; Entidades aseguradoras	BAJO
PATRONATO	Prestación de servicios de solvencia patrimonial y crédito	Asociados o miembros; Personas de contacto / Académicos y profesionales; Detalles del empleo	Organizaciones o personas directamente relacionadas con el responsable; Asociaciones y organizaciones sin ánimo de lucro	BAJO
VIDEOVIGILANCIA	Seguridad y control de acceso a edificios; Videovigilancia	Empleados; Clientes y usuarios; Proveedores; Asociados o miembros; Pacientes / Características personales; Imagen	Fuerzas y cuerpos de seguridad	MEDIO
REGISTRO DE JORNADA	Recursos humanos; Gestión de nóminas	Empleados / Detalles del empleo; Transacciones de bienes y servicios	Organismos de la seguridad social; El propio interesado o sus representantes legales; Inspección de Trabajo	BAJO

La siguiente tabla describe las actividades de tratamiento realizadas como ENCARGADOS

ACTIVIDAD DE TRATAMIENTO DE DATOS	FINALIDAD	QUIÉN ES EL RESPONSABLE DEL TRATAMIENTO	TRANSFERENCIAS INTERNACIONALES
-	-	-	-

1.1.2 Valoración del cumplimiento normativo

Num	Chequeo	Resultado	Nivel
1	Disponer de un Registro de Actividades de Tratamiento (como responsable)	La Fundación cuenta con un registro de actividades de tratamiento, éste se mantiene al día	●
2	El Registro de Actividades de Tratamiento incluye las actividades realizadas como encargado, identificando para cada una la identidad del responsable	No aplica	●
3	La relación de actividades de tratamiento es completa	Cumplimiento	●
4	Se dispone de toda la información exigida por el RGPD, para todos y cada uno de los tratamientos, incluyendo el plazo de conservación y la descripción de las medidas de seguridad	Se cumple con lo establecido en el art. 30 RGPD	●

1.2 Protección de datos en el diseño y por defecto

Artículo 24 del RGPD. Responsabilidad del responsable del tratamiento

1.Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

Artículo 25 del RGPD. Protección de datos desde el diseño y por defecto

1.Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

1.2.1 Situación actual

Durante el proceso de revisión del cual es objeto la presente auditoría, se ha procedido a evaluar nuevamente el riesgo de las actividades de tratamiento existentes.

Siguiendo las recomendaciones de la Agencia Española de Protección de Datos, se ha procedido a clasificar las actividades de tratamiento en base a su nivel de riesgo inherente. Dicha clasificación se utiliza como ayuda para establecer las medidas técnicas y organizativas pertinentes, así como para establecer el tipo de análisis de riesgos necesario.

1.2.2 Valoración del cumplimiento normativo

Num	Chequeo	Resultado	Nivel
1	En términos generales, se han establecido medidas técnicas y organizativas adecuadas al nivel de riesgo	Se han tomado medidas acordes al nivel de riesgo de cada actividad	●
2	Se involucra la protección de datos en el desarrollo de nuevos tratamientos	La Fundación comunica a PRODAT todas las actividades nuevas que implican un tratamiento de datos	●
3	Aplicación de la protección de datos por defecto: si el interesado o afectado configura un servicio o introduce sus datos, las "preferencias de privacidad" tienen por defecto una configuración restrictiva, especialmente los datos no son visibles para otros sin mediar acción del interesado.	Cumplimiento	●
4	Frecuencia de las revisiones y auditorías de protección de datos adecuadas al riesgo	Se realizan revisiones y auditorías periódicamente	●

1.3 Publicación del registro de actividades de tratamiento

Artículo 31 de la LOPD. Registro de las actividades de tratamiento.

2. Los sujetos enumerados en el artículo 77.1 de esta ley orgánica harán público un inventario de sus actividades de tratamiento accesible por medios electrónicos en el que constará la información establecida en el artículo 30 del Reglamento (UE) 2016/679 y su base legal.

1.3.1 Situación actual

Las categorías de responsables o encargados del tratamiento sujetas a la obligación de publicidad de art. 31 son las siguientes:

a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.
b) Los órganos jurisdiccionales.
c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.
d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.
e) Las autoridades administrativas independientes.
f) El Banco de España.

g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.
h) Las fundaciones del sector público.
i) Las Universidades Públicas.
j) Los consorcios.
k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

1.3.2 Valoración del cumplimiento normativo

Num	Chequeo	Resultado	Nivel
1	La entidad se encuentra dentro de las categorías de responsables o encargados del tratamiento sujetas a la obligación de publicación del registro de actividades de tratamiento, y se ha realizado dicha publicación, que además está actualizada.	No aplica	

1.4 Evaluación de impacto y consulta previa

Artículo 35 del RGPD. Evaluación de impacto relativa a la protección de datos

1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

> *a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;*
> *b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o*
> *c) observación sistemática a gran escala de una zona de acceso público.*

4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.

5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.

6. Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.

7. La evaluación deberá incluir como mínimo:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;
b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;
c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y
d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

8. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.

9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.

11. En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento.

Artículo 36 del RGPD. Consulta previa

1. El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo.

2. Cuando la autoridad de control considere que el tratamiento previsto a que se refiere el apartado 1 podría infringir el presente Reglamento, en particular cuando el responsable no haya identificado o mitigado suficientemente el riesgo, la autoridad de control deberá, en un plazo de ocho semanas desde la solicitud de la consulta, asesorar por escrito al responsable, y en su caso al encargado, y podrá utilizar cualquiera de sus poderes mencionados en el artículo 58. Dicho plazo podrá prorrogarse seis semanas, en función de la complejidad del tratamiento previsto. La autoridad de control informará al responsable y, en su caso, al encargado de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, indicando los motivos de la dilación. Estos plazos podrán suspenderse hasta que la autoridad de control haya obtenido la información solicitada a los fines de la consulta.

3. Cuando consulte a la autoridad de control con arreglo al apartado 1, el responsable del tratamiento le facilitará la información siguiente:

a) en su caso, las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento, en particular en caso de tratamiento dentro de un grupo empresarial;
b) los fines y medios del tratamiento previsto;
c) las medidas y garantías establecidas para proteger los derechos y libertades de los interesados de conformidad con el presente Reglamento;
d) en su caso, los datos de contacto del delegado de protección de datos;
e) la evaluación de impacto relativa a la protección de datos establecida en el artículo 35, y
f) cualquier otra información que solicite la autoridad de control.

4. Los Estados miembros garantizarán que se consulte a la autoridad de control durante la elaboración de toda propuesta de medida legislativa que haya de adoptar un Parlamento nacional, o de una medida reglamentaria basada en dicha medida legislativa, que se refiera al tratamiento.

5. No obstante lo dispuesto en el apartado 1, el Derecho de los Estados miembros podrá obligar a los responsables del tratamiento a consultar a la autoridad de control y a recabar su autorización previa en relación con el tratamiento por un responsable en el ejercicio de una misión realizada en interés público, en particular el tratamiento en relación con la protección social y la salud pública.

Artículo 28 de la LOPDGDD. Obligaciones generales del responsable y encargado del tratamiento.

1. Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV del citado reglamento.

2. Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:

a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.
b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.
c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.
d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.
e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.
f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.
g) Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.
h) Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.

1.4.1 Situación actual

Lista de tratamientos para los que el RGPD establece explícitamente la obligación de hacer una EIPD (artículo 35.3 del RGPD)	
a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;	NO
b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10,	NO
c) observación sistemática a gran escala de una zona de acceso público.	NO
Criterio: la EIPD es obligatoria si el tratamiento cumple cualquiera de los requisitos a, b o c	

Decisión de necesidad de EVAL IMPACTO PROTECC DATOS (art. 35.2) según el WP29 probablemente suponen un alto riesgo:	
Evaluación y scoring, incluyendo perfilado y predicción	NO
Decisiones automatizadas con efectos legales o similares	NO
Tratamientos usados para observar, monitorizar o controlar sistemáticamente sujetos	NO
Tratamiento de datos sensibles (según artículos 9 y 10 RGPD)	SÍ
Tratamiento de datos a gran escala	NO
Conjuntos de datos que han matcheado o combinados	NO
Tratamiento de datos relativos a colectivos vulnerables (ej: empleados; niños; con enfermedad mental; solicitantes de asilo; personas mayores)	SÍ
Criterio del WP29: la evaluación de impacto deberá hacerse cuando el tratamiento cumpla al menos 2 de los requisitos	

Lista de tratamientos que requieren EVAL IMPACTO según la Agencia Española de Protección de Datos (ver https://www.aepd.es/media/criterios/listas-dpia-es-35-4.pdf)	
1. Tratamientos que impliquen perfilado o valoración de sujetos, incluida la recogida de datos del sujeto en múltiples ámbitos de su vida (desempeño en el trabajo, personalidad y comportamiento), que cubran varios aspectos de su personalidad o sobre sobre sus hábitos.	NO
2.Tratamientos que impliquen la toma de decisiones automatizadas o que contribuyan en gran medida a la toma de tales decisiones, incluyendo cualquier tipo de decisión que impida a un interesado el ejercicio de un derecho o el acceso a un bien o un servicio o formar parte de un contrato.	NO
3.Tratamientos que impliquen la observación, monitorización, supervisión, geolocalización o control del interesado de forma sistemática y exhaustiva, incluida la recogida de datos y metadatos a través de redes, aplicaciones o en zonas de acceso público, así como el procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, TV interactiva, aplicaciones móviles, etc.	NO
4.Tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos.	SÍ
5.Tratamientosque impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física.	NO
6.Tratamientosque impliquen el uso de datos genéticos para cualquier fin.	NO
7.Tratamientos que impliquen el uso de datos a gran escala. Para determinar si un tratamiento se puede considerar a gran escala se considerarán los criterios establecidos en la guía WP243 “Directrices sobre los delegados de protección de datos (DPD)” del Grupo de Trabajo del Artículo 29.	NO
8.Tratamientos que impliquen la asociación, combinación o enlace de registros de bases de datos de dos o más tratamientos con finalidades diferentes o por responsables distintos.	NO
9.Tratamientos de datos de sujetos vulnerables o en riesgo de exclusión social, incluyendo datos de menores de 14 años, mayores con algún grado de discapacidad, discapacitados, personas que acceden a servicios sociales y víctimas de violencia de género, así como sus descendientes y personas que estén bajo su guardia y custodia.	SÍ
10.Tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo para los derechos y libertades de las personas.	NO
11.Tratamientos de datos que impidan a los interesados ejercer sus derechos, utilizar un servicio o ejecutar un contrato, como por ejemplo tratamientos en los que los datos han sido recopilados por un responsable distinto al que los va a tratar y aplica alguna de las excepciones sobre la información que debe proporcionarse a los interesados según el artículo 14.5 (b,c,d) del RGPD	NO

Puesto que FUNDACIÓ VÍA-GUASP venía realizando actividades que suponían un tratamiento de datos de categoría sensible con anterioridad a la implementación de la actual normativa de protección de datos, en la que se establece la obligación de realizar una EIPD

en ciertos supuestos, precisamente con el objetivo de determinar el impacto que puede suponer poner en marcha dichas actividades, previa a su realización, no resulta preceptiva la evaluación de impacto en el presente supuesto.

1.4.2 Valoración del cumplimiento normativo

Num	Chequeo	Resultado	Nivel
1	Se ha analizado la obligación o conveniencia de realizar evaluaciones de impacto	Cumplimiento	●

1.5 Tratamientos como encargado: contrato e instrucciones

Artículo 28 del RGPD. Encargado del tratamiento

(…) 3. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable (…)

1.5.1 Situación actual

No existen tratamientos realizados como encargados.

1.5.2 Valoración del cumplimiento normativo

Num	Chequeo	Resultado	Nivel
1	En los tratamientos realizados como encargados, se dispone de un contrato de encargado conforme a la legislación vigente, recogiendo la obligación de seguir las instrucciones documentadas del responsable	No aplica	●

1.6 Corresponsables del tratamiento

Artículo 26 del RGPD. Corresponsables del tratamiento

1. *Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que se les aplique a ellos. Dicho acuerdo podrá designar un punto de contacto para los interesados.*

2. *El acuerdo indicado en el apartado 1 reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los interesados. Se pondrán a disposición del interesado los aspectos esenciales del acuerdo.*

> 3. *Independientemente de los términos del acuerdo a que se refiere el apartado 1, los interesados podrán ejercer los derechos que les reconoce el presente Reglamento frente a, y en contra de, cada uno de los responsables.*

1.6.1 Situación actual

No existen tratamientos realizados como corresponsables.

1.6.2 Valoración del cumplimiento normativo

Num	Chequeo	Resultado	Nivel
1	En caso de existir tratamientos como corresponsables, se ha firmado el acuerdo exigido en el art. 26	No aplica	

2 Principios de protección de datos

2.1 Licitud (legitimación) y transparencia (información a los interesados)

El RGPD establece una serie de supuestos bajo los que un tratamiento será legal: consentimiento, ejecución de un contrato, obligaciones legales, etc. Fuera de estos supuestos el tratamiento de datos no está permitido. Los artículos 9 y 10 del RGPD establecen condiciones adicionales para proceder al tratamiento de los datos de categorías especiales, así como para los datos de infracciones penales.

El RGPD establece requisitos reforzados para el consentimiento, que deberá ser mediante una declaración o clara acción afirmativa del interesado. Desaparece por tanto el consentimiento tácito.

El RGPD también establece los requisitos en materia de información, a proporcionar a los interesados, tanto si los datos los proporcionan directamente o bien se obtienen de alguna otra fuente.

Artículo 6 del RGPD. Licitud del tratamiento

1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

2. Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX.

3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por:

a) el Derecho de la Unión, o
b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento.

La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor

del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

4. Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:

a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;
b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;
c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;
d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;
e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.

Artículo 7 del RGPD. Condiciones para el consentimiento

1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.

2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.

3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.

4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

Artículo 8 del RGPD. Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información

1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.

Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.

2. El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.

3. El apartado 1 no afectará a las disposiciones generales del Derecho contractual de los Estados miembros, como las normas relativas a la validez, formación o efectos de los contratos en relación con un niño.

Artículo 7 de la LOPDGDD. Consentimiento de los menores de edad.

1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.

Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

2. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.

Artículo 9 del RGPD. Tratamiento de categorías especiales de datos personales

1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de 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.

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;
b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;
c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;
d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;
e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;
f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;
g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;
h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;
i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,
j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación

científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.

4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.

Artículo 10 del RGPD. Tratamiento de datos personales relativos a condenas e infracciones penales

El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas.

Artículo 13 del RGPD. Información que deberá facilitarse cuando los datos personales se obtengan del interesado

1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
b) los datos de contacto del delegado de protección de datos, en su caso;
c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;
e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;
d) el derecho a presentar una reclamación ante una autoridad de control;
e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito

necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;
f) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.

Artículo 14 del RGPD. Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado

1. Cuando los datos personales no se hayan obtenidos del interesado, el responsable del tratamiento le facilitará la siguiente información:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
b) los datos de contacto del delegado de protección de datos, en su caso;
c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;
d) las categorías de datos personales de que se trate;
e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
f) en su caso, la intención del responsable de transferir datos personales a un destinatario en un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de ellas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente respecto del interesado:

a) el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo;
b) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable del tratamiento o de un tercero;
c) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
d) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada;
e) el derecho a presentar una reclamación ante una autoridad de control;
f) la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;
g) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. El responsable del tratamiento facilitará la información indicada en los apartados 1 y 2:

a) dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos;
b) si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado, o
c) si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los

datos personales sean comunicados por primera vez.

4. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de los datos personales para un fin que no sea aquel para el que se obtuvieron, proporcionará al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y cualquier otra información pertinente indicada en el apartado 2.

5. Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que:

a) el interesado ya disponga de la información;
b) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información;
c) la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, o
d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria.

Artículo 11 de la LOPDGDD. Transparencia e información al afectado.

1. Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

2. La información básica a la que se refiere el apartado anterior deberá contener, al menos:
a) La identidad del responsable del tratamiento y de su representante, en su caso.
b) La finalidad del tratamiento
c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.
Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679.

3. Cuando los datos personales no hubieran sido obtenidos del afectado, el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 del Reglamento (UE) 2016/679 facilitando a aquel la información básica señalada en el apartado anterior, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.
En estos supuestos, la información básica incluirá también:
a) Las categorías de datos objeto de tratamiento.
b) Las fuentes de las que procedieran los datos.

2.1.1 Situación actual

Atendiendo a las actividades de tratamiento la tabla a continuación resume la existencia de una base legal legitimadora del tratamiento, así como el cumplimiento del deber de informar.

Tratamiento / Colectivo de interesados	Datos de categorías especiales conforme art. 9 RGPD	Base legal del tratamiento de datos (legitimación)	Documento donde consta contenido derecho de información
COMUNICACIÓN Y PUBLICIDAD	NO	ART 6.1.A (CONSENTIMIENTO)	POLÍTICA DE PRIVACIDAD

CONTABILIDAD	NO	ART 6.1.C (OBLIGACIÓN LEGAL DEL RESPONSABLE)	NORMATIVA MERCANTIL APLICABLE
CONTABILIDAD TUTELEADOS	NO	ART 6.1.B (CONTRATO O PRECONTRATO)	CONTRATO O PRECONTRATO
DONANTES	NO	ART 6.1.A (CONSENTIMIENTO) Y 6.1.C (OBLIGACIÓN LEGAL DEL RESPONSABLE)	POLÍTICA DE PRIVACIDAD NORMATIVA APLICABLE
EXPEDIENTE TUTELADOS O PRE-TUTELADOS	SÍ	ART 6.1.B (CONTRATO O PRECONTRATO)	CONTRATO O PRECONTRATO
NÓMINAS, PERSONAL Y RRHH	NO	ART 6.1.B (CONTRATO O PRECONTRATO) Y 6.1.C (OBLIGACIÓN LEGAL DEL RESPONSABLE)	CONTRATO O PRECONTRATO NORMATIVA APLICABLE
PATRONATO	NO	ART 6.1.B (CONTRATO O PRECONTRATO) Y 6.1.C (OBLIGACIÓN LEGAL DEL RESPONSABLE)	CONTRATO O PRECONTRATO NORMATIVA APLICABLE
VIDEOVIGILANCIA	NO	ART 6.1.E (MISIÓN DE INTERÉS PÚBLICO)	CARTEL DE VIDEOVIGILANCIA
REGISTRO DE JORNADA	NO	ART 6.1.B (CONTRATO O PRECONTRATO) Y 6.1.C (OBLIGACIÓN LEGAL DEL RESPONSABLE)	CONTRATO O PRECONTRATO NORMATIVA LABORAL APLICABLE

En relación a los procedimientos automatizados de consentimiento, que deben contar con mecanismos similares de revocación, nos encontramos los siguientes:

Consentimiento otorgado por medios automatizados	¿Cuenta con sistema similar (simple) de revocación?
CONSENTIMIENTO COOKIES	No aplica

2.1.2 Valoración del cumplimiento normativo

Num	Chequeo	Resultado	Nivel
1	Se cuenta con una legitimación válida para todos los tratamientos de datos personales de la organización	Se deberá revisar la página web en busca de fotografías en las que salgan personas que no prestaron su consentimiento para ello Se deberá revisar también para el caso de las fotografías colgadas en los tablones de la entrada del edificio. En caso de no poder identificar quién prestó y quién no su consentimiento, se deberá proceder a descolgar todas las fotografías	🟡
2	Se proporciona la información necesaria para cumplir los requisitos de información del RGPD	Se recuerda que se deberá sustituir el cartel de videovigilancia actual por el actualizado (RGPD)	🔴
3	Los formularios web incluyen la información necesaria y aceptación de la política de privacidad	Cumplimiento	🟢

Num	Chequeo	Resultado	Nivel
4	Es tan fácil dar el consentimiento como revocarlo	Cumplimiento	●

2.2 Minimización de datos, exactitud y limitación de plazo

Artículo 5 del RGPD. Principios relativos al tratamiento

1.Los datos personales serán:

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) 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 («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas (…) a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

En relación a la determinación de los plazos de conservación, se tendrá en consideración la siguiente tabla:

Abogados: 5 años mínimo, expedientes, para posibles responsabilidades profesionales (Código Civil art. 1964.2 red. Ley 42/2015)
Auditores de cuentas: 5 años, papeles auditor (RD 1/2011 art. 24 y RD 1517/2011, art. 58)
Centros reconocimientos conductores: 10 años, informes, dictámenes profesionales y documentos (RD 170/2010 art. 15.5)
Contabilidad y fiscalidad: 4 años, documentos y registros de trascendencia tributaria (Ley General Tributaria arts. 66 a 70)
Control acceso casinos y salas de bingo: 6 meses, ficheros para controlar el acceso (Inst. 2/1996 AEPD)
Control acceso edificios: 30 días, ficheros para controlar el acceso (Inst. 1/1996 AEPD)
Detectives: 3 años, informes y grabaciones (Ley 5/2014 art. 49.4)
Establecimientos hoteleros: 3 años, libro-registro y partes de entrada (OM INT/1922/2003)
Establecimientos metales preciosos: 5 años, libros-registro (RD 197/1988 art. 99)
Historia clínica Canarias: 20 años desde alta, consentimiento informado e información asistencial (D 178/2005 CA Canarias art. 29.3 D)
Historia clínica Canarias: 5 años, documentación accesoria proceso asistencial (D 178/2005 CA Canarias art. 29.2)
Historia clínica Canarias: Indefinidamente, informes clínicos de alta (D 178/2005 CA Canarias art. 29.4 D)
Historia clínica Cantabria: 15 años desde fallecimiento, documentación e historia clínica (Ley 7/2002 CA Cantabria art. 72)
Historia clínica Catalunya: 15 años desde alta, consentimiento informado e información asistencial (Ley 21/2000 CA Cataluña)
Historia clínica Galicia: Indefinidamente, consentimiento informado e información asistencial (Ley 3/2001 CA Galicia art. 20)
Historia clínica general: 5 años mínimo desde alta, documentación e historia clínica (Ley 41/2002 art. 17.1)

Historia clínica Navarra: 5 años mínimo desde intervención, documentación e historia clínica (Ley Foral 17/2010 Navarra art. 61)
Historia clínica País Vasco: 10 años desde fallecimiento, documentación clínica (D 38/2012 País Vasco art. 21.2-4)
Historia clínica País Vasco: 15 años desde fallecimiento, historia clínica (D 38/2012 País Vasco art. 21.2-4)
Historia clínica País Vasco: 30 años, datos relativos a medicina nuclear y radioterapia (D 38/2012 País Vasco art. 19.2)
Historia clínica País Vasco: 5 años mínimo desde alta, documentación clínica (D 38/2012 País Vasco art. 19.1)
Impagados deudas telefonía: 3 años, facturas impagadas (Código Civil art. 1967 y jurisprudencia)
Laboral y seguridad social: 4 años, documentos y registros de obligaciones laborales (RDL 5/2000 art. 4)
Mediadores: 4 meses, expedientes mediación (Ley 5/2012 art. 22.1)
Normativa mercantil: 6 años, libros correspondencia y justificantes (Código Comercio art. 30)
Operadores comunicaciones electrónicas: 1 año, datos de tráfico de las comunicaciones (Ley 25/2007 art. 5)
Prevención de riesgos laborales: 5 años, documentos y registros de obligaciones en materia de PRL (RDL 5/2000 art. 4)
Sujetos obligados Ley PBC: 10 años, documentación acreditativa cumplimiento obligaciones PBC (Ley 10/2010 art. 25)
Tacógrafo digital (centros técnicos): 3 años, intervenciones técnicas realizadas (RD 425/2005)
Tacógrafo digital (centros técnicos): 5 años, certificados de intransferibilidad (RD 425/2005 apart. 10 DA 1)
Tacógrafo digital: 1 año, transferencias y copias de datos almacenados en la memoria (RD 425/2005 apart. 3 DA 1)
Videovigilancia (escolar): 10 días, imágenes captadas (Informe AEPD 475/2014)
Videovigilancia (FFCCS): 30 días, imágenes/audio captados (LO 4/1997 art. 8 y RD 596/1999 Arts. 18 y 19)
Videovigilancia: 1 mes, imágenes captadas (LOPDGDD)
Sistemas de denuncias internas: 3 meses (LOPDGDD)

2.2.1 Situación actual

El registro de actividades de tratamiento recoge los plazos a aplicar en base a la legislación vigente y los plazos aplicados.

No obstante, la Fundación deberá velar por el cumplimiento de dichos plazos de destrucción de la documentación.

2.2.2 Valoración del cumplimiento normativo

Num	Chequeo	Resultado	Nivel
1	Minimización en la recogida de datos: los datos recogidos son adecuados, pertinentes y no excesivos en base a su finalidad	Se da cumplimiento al principio de minimización en la recogida de datos	

Num	Chequeo	Resultado	Nivel
2	Minimización en el tratamiento: los datos únicamente serán accesibles para aquellas personas implicadas en su tratamiento, no siendo accesibles para las demás, siguiendo el principio de "necesidad de saber" (need to know)	Los datos únicamente son accesibles por el personal implicado en su tratamiento	
3	Se han valorado plazos para las actividades del "registro de actividades de tratamiento"	En el registro de actividades de tratamiento se han fijado los plazos de conservación pertinentes	
4	Correcta aplicación de los plazos de conservación	Se deberá proceder a la destrucción de documentos muy antiguos, en especial los expedientes de pacientes que hace mucho que no han requerido de los servicios de la Fundación, así como los pacientes difuntos	
5	Fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, medidas técnicas y organizativas como la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines	No aplica	

2.3 Confidencialidad y deber de secreto

Artículo 5 del RGPD. Principios relativos al tratamiento

1.Los datos personales serán:

f) tratados 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, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

2.El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

Artículo 5 de la LOPDGDD. Deber de confidencialidad.

1. Los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.
2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.
3. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

2.3.1 Situación actual

Chequeos deber de secreto:

Colectivo	*OK / NO OK*
Empleados	OK
Estudiantes en prácticas	NO OK

2.3.2 Valoración del cumplimiento normativo

Num	Chequeo	Resultado	Nivel
1	Se ha elaborado un documento para informar al personal sobre el deber de secreto en relación a los datos personales a los que puedan tener acceso	Todos los empleados han firmado el documento relativo a la protección de datos	●
2	El deber de secreto también afecta a personal externo, prestadores de servicios, estudiantes en prácticas, etc.	Se recuerda que tanto los estudiantes en prácticas como los voluntarios deberán firmar también el documento de protección de datos	●

2.4 Derechos de acceso, rectificación, supresión y demás

Artículo 15 del RGPD. Derecho de acceso del interesado

1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:

a) los fines del tratamiento;
b) las categorías de datos personales de que se trate;
c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;
d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;
e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;
f) el derecho a presentar una reclamación ante una autoridad de control;
g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;
h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

2. Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia.

3. El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El

responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.

4. El derecho a obtener copia mencionado en el apartado 3 no afectará negativamente a los derechos y libertades de otros.

Artículo 16 del RGPD. Derecho de rectificación

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

Artículo 17 del RGPD. Derecho de supresión («el derecho al olvido»)

1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;
b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;
c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;
d) los datos personales hayan sido tratados ilícitamente;
e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;
f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:

a) para ejercer el derecho a la libertad de expresión e información;
b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;
c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;
d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o
e) para la formulación, el ejercicio o la defensa de reclamaciones.

Artículo 18 del RGPD. Derecho a la limitación del tratamiento

1. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;
b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;
c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;
d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

2. Cuando el tratamiento de datos personales se haya limitado en virtud del apartado 1, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.

3. Todo interesado que haya obtenido la limitación del tratamiento con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación.

Artículo 19 del RGPD. Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento

El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16, al artículo 17, apartado 1, y al artículo 18 a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.

Artículo 20 del RGPD. Derecho a la portabilidad de los datos

1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:

a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y
b) el tratamiento se efectúe por medios automatizados.

2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

4. El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros.

Artículo 21 del RGPD. Derecho de oposición

1. El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

2. Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado

tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.

3. Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.

4. A más tardar en el momento de la primera comunicación con el interesado, el derecho indicado en los apartados 1 y 2 será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.

5. En el contexto de la utilización de servicios de la sociedad de la información, y no obstante lo dispuesto en la Directiva 2002/58/CE, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.

6. Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.

Artículo 22 del RGPD. Decisiones individuales automatizadas, incluida la elaboración de perfiles

1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

2. El apartado 1 no se aplicará si la decisión:

a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;
b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o
c) se basa en el consentimiento explícito del interesado.

3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.
Sección 5

2.4.1 Situación actual

La entidad cuenta con un procedimiento escrito para la atención de derechos.

2.4.2 Valoración del cumplimiento normativo

Num	Chequeo	Resultado	Nivel
1	La entidad cuenta con un procedimiento escrito para atender las solicitudes	Cumplimiento	●
2	La entidad ha formado a los empleados involucrados en la atención a clientes sobre cómo atender estos derechos	Los empleados son conscientes de las obligaciones en materia de protección de datos	●

3 Prestaciones de servicio recibidas

3.1 Firma de contratos con los encargados de tratamiento

El RGPD establece la figura del Encargado del tratamiento, que accede a los ficheros responsabilidad de un tercero con motivo de prestarle un servicio. Se establece la obligación de confeccionar un contrato regulando entre otros extremos las condiciones de seguridad a aplicar en el acceso a los datos por parte del Encargado / Prestador.

Artículo 28 del RGPD. Encargado del tratamiento

1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.

2. El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.

3. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

> *a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;*
> *b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;*
> *c) tomará todas las medidas necesarias de conformidad con el artículo 32;*
> *d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;*
> *e) asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;*
> *f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;*
> *g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;*
> *h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.*

En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

4. Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el

contrato u otro acto jurídico entre el responsable y el encargado a que se refiere el apartado 3, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.

5. La adhesión del encargado del tratamiento a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a que se refieren los apartados 1 y 4 del presente artículo.

6. Sin perjuicio de que el responsable y el encargado del tratamiento celebren un contrato individual, el contrato u otro acto jurídico a que se refieren los apartados 3 y 4 del presente artículo podrá basarse, total o parcialmente, en las cláusulas contractuales tipo a que se refieren los apartados 7 y 8 del presente artículo, inclusive cuando formen parte de una certificación concedida al responsable o encargado de conformidad con los artículos 42 y 43.

7. La Comisión podrá fijar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.

8. Una autoridad de control podrá adoptar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el mecanismo de coherencia a que se refiere el artículo 63.

9. El contrato u otro acto jurídico a que se refieren los apartados 3 y 4 constará por escrito, inclusive en formato electrónico.

10. Sin perjuicio de lo dispuesto en los artículos 82, 83 y 84, si un encargado del tratamiento infringe el presente Reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento.

Artículo 29 del RGPD. Tratamiento bajo la autoridad del responsable o del encargado del tratamiento

El encargado del tratamiento y cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo podrán tratar dichos datos siguiendo instrucciones del responsable, a no ser que estén obligados a ello en virtud del Derecho de la Unión o de los Estados miembros.

Disposición transitoria quinta LOPDGDD. Contratos de encargado del tratamiento

Los contratos de encargado del tratamiento suscritos con anterioridad al 25 de mayo de 2018 al amparo de lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal mantendrán su vigencia hasta la fecha de vencimiento señalada en los mismos y en caso de haberse pactado de forma indefinida, hasta el 25 de mayo de 2022.

Durante dichos plazos cualquiera de las partes podrá exigir a la otra la modificación del contrato a fin de que el mismo resulte conforme a lo dispuesto en el artículo 28 del Reglamento (UE) 2016/679 y en el Capítulo II del Título V de esta ley orgánica.

3.1.1 Situación actual

La siguiente tabla resume la existencia de encargados de tratamiento y si se cuenta con un contrato adaptado al RGPD.

Encargado	*Prestación*	*Firmado conforme LOPD99 / Firmado conforme RGPD / No firmado*
TODOENLACES, S.L.	Alojamiento y gestión de la página web	Firmado conforme RGPD
BUSQUET ECONOMISTES AUDITORS, S.L.U.	Asesoramiento laboral y fiscal	Firmado conforme RGPD
VÍCTOR MARTÍNEZ CERVERA	Mantenimiento informático	No firmado
ENRICA COROMINAS	Asesoramiento en defesa jurídica	No firmado
SAGE SPAIN, S.L.	Mantenimiento y gestión de la plataforma SAGE	Firmado conforme RGPD

3.1.2 Valoración del cumplimiento normativo

Num	Chequeo	Resultado	Nivel
1	Disponen de los contratos pertinentes para regular las prestaciones de servicio que conllevan un tratamiento de datos personales, adaptados al RGPD	Se recuerda a la Fundación, que se deberá enviar copia del contrato de encargado firmado por Víctor Martínez Cervera y Enrica Corominas	●

4 Funciones y obligaciones del personal

4.1 Delegado de protección de datos

Artículo 37 del RGPD. Designación del delegado de protección de datos

1. El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:

a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;
b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o
c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

2. Un grupo empresarial podrá nombrar un único delegado de protección de datos siempre que sea fácilmente accesible desde cada establecimiento.

3. Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño.

4. En casos distintos de los contemplados en el apartado 1, el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen a categorías de responsables o encargados podrán designar un delegado de protección de datos o deberán designarlo si así lo exige el Derecho de la Unión o de los Estados miembros. El delegado de protección de datos podrá actuar por cuenta de estas asociaciones y otros organismos que representen a responsables o encargados.

5. El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39.

6. El delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

7. El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control.

Artículo 34 LOPDGDD. Designación de un delegado de protección de datos

1. Los responsables y encargados del tratamiento deberán designar un delegado de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate de las siguientes entidades:

a) Los colegios profesionales y sus consejos generales.
b) Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.
c) Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.
d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.
e) Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.
f) Los establecimientos financieros de crédito.
g) Las entidades aseguradoras y reaseguradoras.
h) Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.
i) Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.

j) Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.
k) Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo
tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.
l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.
Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.
m) Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.
n) Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.
ñ) Las empresas de seguridad privada.
o) Las federaciones deportivas cuando traten datos de menores de edad.

3. Los responsables y encargados del tratamiento comunicarán en el plazo de diez días a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, las designaciones, nombramientos y ceses de los delegados de protección de datos tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria.

Artículo 38 del RGPD. Posición del delegado de protección de datos

1. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.

2. El responsable y el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de las funciones mencionadas en el artículo 39, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.

3. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.

4. Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento.

5. El delegado de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros.

6. El delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses.

Artículo 39 del RGPD. Funciones del delegado de protección de datos

1. El delegado de protección de datos tendrá como mínimo las siguientes funciones:

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;
b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las

políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;
c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;
d) cooperar con la autoridad de control;
e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

2. El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

4.1.1 Situación actual

Valoración de la obligación de designar un DPD

Con arreglo al punto 37.1.a del RGPD ("el tratamiento lo lleve a cabo una autoridad u organismo público")	NO APLICA
Con arreglo al punto 37.1.b del RGPD ("las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala")	NO APLICA
Con arreglo al punto 37.1.c del RGPD ("*gran escala de categorías especiales de datos personales con arreglo al artículo 9*")	NO APLICA
Con arreglo al art 34 de la nueva LOPDGDD	NO APLICA

Otros aspectos

Dpd designado voluntariamente?	No

4.1.2 Valoración del cumplimiento normativo

Num	Chequeo	Resultado	Nivel
1	Se ha designado al delegado de protección de datos y se ha comunicado a las autoridades de protección de datos. Se ha verificado en el registro de delegados de la autoridad de control que no hay información obsoleta o incorrecta	No aplica	
2	En los tratamientos realizados como "encargado", se ha identificado al delegado de protección de datos designado por el responsable	No aplica	

4.2 Delegación de las funciones de control de la seguridad de datos

Artículo 29 del RGPD. Tratamiento bajo la autoridad del responsable o del encargado del tratamiento

… cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo podrá tratar dichos datos siguiendo las instrucciones del responsable …

4.2.1 Situación actual

Función	Persona/s designada/s
Responsable de seguridad	Montserrat Villagrasa Corominas

4.2.2 Valoración del cumplimiento normativo

Num	Chequeo	Resultado	Nivel
1	Constancia escrita de la delegación de las funciones de control realizadas por los responsables de seguridad y administradores de sistemas	Se ha designado formalmente la figura del responsable de seguridad	●

4.3 Conocimiento del personal de las normas de seguridad que les afectan

Artículo 29 del RGPD. Tratamiento bajo la autoridad del responsable o del encargado del tratamiento

El encargado del tratamiento y cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo podrán tratar dichos datos siguiendo instrucciones del responsable (…)

Artículo 32.4 del RGPD. Seguridad del tratamiento

El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable (…)

4.3.1 Situación actual

Se ha hecho formación del RGPD presencial	NO
Se ha hecho formación del RGPD online	NO
Información manual bienvenida / nuevos empleados	SÍ
Información accesible permanentemente	SÍ

Todos los empleados son conscientes de la normativa de protección de datos. Asimismo, todos los empleados han firmado el documento relativo a la protección de datos.

4.3.2 Valoración del cumplimiento normativo

Num	Chequeo	Resultado	Nivel
1	Se han adoptado medidas para que el personal conozca de forma comprensible las normas de seguridad que les afectan	Cumplimiento	●

5 Aplicación de las medidas de seguridad

Artículo 32 del RGPD. Seguridad del tratamiento

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de 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. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.

5.1 Medidas relacionadas con la gestión de los soportes

MEDIDA DE SEGURIDAD	NIVEL DE RIESGO	VALORACIÓN EFICACIA MEDIDAS
Identificación e inventario de soportes	RIESGO BAJO	Conforme
Etiquetado que dificulte la identificación de los soportes y documentos de nivel alto al personal no autorizado	RIESGO BAJO	Conforme
Autorización de la salida de soportes fuera de la organización	RIESGO ALTO	**Conforme con recordatorio:** Toda información perteneciente a la Fundación deberá ser devuelta en la mayor brevedad posible por el trabajador autorizado a sacar documentos fuera del lugar de trabajo
Registro de Entrada/Salida de soportes automatizados con datos sensibles	RIESGO MEDIO	**Conforme con recordatorio:** Remisión al punto anterior
Cifrado en la distribución de soportes automatizados	RIESGO BAJO	Conforme
Prohibición de grabar datos de nivel alto en dispositivos portátiles y utilización en dichos casos excepcionales de cifrado	RIESGO BAJO	Conforme
Desecho de los soportes y documentos mediante destrucción o procesos que garanticen que la información no es recuperable a posteriori	RIESGO BAJO	Conforme

MEDIDA DE SEGURIDAD	NIVEL DE RIESGO	VALORACIÓN EFICACIA MEDIDAS
Sistema de monitorización automatizada de los dispositivos conectados en red y dispositivos móviles	RIESGO BAJO	Conforme
Dispositivos móviles inteligentes con bloqueo y cifrado	RIESGO BAJO	Conforme
Controles que garanticen el control de la información tratada y almacenada en dispositivos BYOD (“bring your own device”)	RIESGO BAJO	No aplica

5.2 Medidas relacionadas con el control de acceso a la información

MEDIDA DE SEGURIDAD	NIVEL DE RIESGO	VALORACIÓN EFICACIA MEDIDAS
Acceso limitado a los recursos necesarios para cada usuario	RIESGO BAJO	Conforme
Identificación y autenticación individual mediante contraseñas o equivalente	RIESGO BAJO	Conforme
Procedimiento confidencial de asignación de contraseñas	RIESGO BAJO	**Conforme con recordatorio:** Se recuerda a la Fundación que se deberá proporcionar una contraseña a todos los nuevos empleados/estudiantes en prácticas/voluntarios, y éstos deberán modificarla una vez recibido el dispositivo
Renovación de contraseñas al menos anual	RIESGO ALTO	**Disconforme:** Se debe cambiar la contraseña del Wifi como mínimo, una vez al año
Almacenamiento ininteligible de las contraseñas vigentes	RIESGO BAJO	Conforme
Mecanismo para limitar intentar reiteradamente el acceso no autorizado	RIESGO BAJO	Conforme
Control de acceso físico sistemas automatizados nivel medio / alto (sala servidores etc.)	RIESGO BAJO	**Conforme con aclaración:** el servidor se encuentra dentro de un rack que ésta, a su vez, se ubica en una sala de acceso restringido, de la cual solamente existe una copia de la llave
Registro de reintentos de autenticación	RIESGO BAJO	Conforme
Registro de accesos a sistemas automatizados con datos sensibles	RIESGO MEDIO	Conforme
Sistemas de detección de intrusiones (IDS)	RIESGO BAJO	Conforme

5.3 Medidas relacionadas con copia respaldo y la disponibilidad de los sistemas

MEDIDA DE SEGURIDAD	NIVEL DE RIESGO	VALORACIÓN EFICACIA MEDIDAS
Existencia de procedimientos de copia de respaldo y de recuperación de datos con frecuencia diaria	RIESGO BAJO	Conforme
RPO (volumen de datos que se pueden perder en caso de incidente, depende de la frecuencia de las copias) aceptable para la dirección	RIESGO MEDIO	Conforme
Consistencia de los procedimientos de backup y recuperación	RIESGO BAJO	Conforme

MEDIDA DE SEGURIDAD	NIVEL DE RIESGO	VALORACIÓN EFICACIA MEDIDAS
Se ha establecido quién es responsable de hacer la copia de los datos almacenados en la nube	RIESGO BAJO	Conforme
Capacidad de restaurar la disponibilidad de los datos de manera rápida, tras incidente	RIESGO BAJO	Conforme
Verificación periódica de los procedimientos de copia de respaldo.	RIESGO BAJO	Conforme
Copia de respaldo en un lugar diferente y con separación lógica	RIESGO BAJO	Conforme
Cifrado de la copia de seguridad externa	RIESGO BAJO	Conforme
Existencia de varias copias o de un histórico de copias adecuado	REISGO BAJO	Conforme
Alertas sobre errores en los procesos de backup	REISGO BAJO	Conforme

5.4 Medidas relacionadas con el uso de redes informáticas

MEDIDA DE SEGURIDAD	NIVEL DE RIESGO	VALORACIÓN EFICACIA MEDIDAS
Cortafuegos	RIESGO BAJO	Conforme
Protección proactiva contra ataques informáticos: escaneo de vulnerabilidades, servicios de hacking, etc.	RIESGO MEDIO	**Conforme con recordatorio:** Se recomienda a la Fundación que activen la opción de realizar escaneos diarios a través del antivirus instalado en su equipo
Cifrado para la transmisión de datos de nivel alto (Internet o redes wifi)	RIESGO BAJO	Conforme
Controles que garanticen las conexiones habilitadas para teletrabajo	RIESGO BAJO	**Conforme con aclaración:** A través de VPN (Net extender)

5.5 Medidas relacionadas con el malware

MEDIDA DE SEGURIDAD	NIVEL DE RIESGO	VALORACIÓN EFICACIA MEDIDAS
Antivirus actualizado en todos los equipos	RIESGO BAJO	Conforme
Sistema operativo actualizado en los dispositivos	RIESGO BAJO	Conforme

5.6 Medidas relacionadas con la documentación (papel)

MEDIDA DE SEGURIDAD	NIVEL DE RIESGO	VALORACIÓN EFICACIA MEDIDAS
Dispositivos de almacenamiento con acceso restringido y mecanismo tipo llave equivalente	RIESGO BAJO	Conforme
Ubicación de los dispositivos de almacenamiento de documentos de nivel alto en salas con acceso restringido	RIESGO BAJO	Conforme
Registro de accesos a los documentos de nivel alto	RIESGO BAJO	**Conforme con explicación:** Para acceder a la sala donde se guarda el servidor, así como para abrir los armarios bajo llave, se debe solicitar copia de ésta
Aplicación de criterios de archivo de los documentos que garanticen la localización, acceso conservación de los documentos	RIESGO BAJO	Conforme

MEDIDA DE SEGURIDAD	NIVEL DE RIESGO	VALORACIÓN EFICACIA MEDIDAS
Custodia de la documentación durante su tramitación por parte del personal a su cargo	RIESGO BAJO	Conforme
Generación de copias de documentos con datos de nivel alto solo por personal autorizado	RIESGO BAJO	Conforme
Traslado de los documentos: medidas de protección para impedir el robo, acceso o manipulación	RIESGO BAJO	Conforme

5.7 Gestión de incidencias de seguridad

MEDIDA DE SEGURIDAD	NIVEL DE RIESGO	VALORACIÓN EFICACIA MEDIDAS
Procedimiento documentado de actuación ante incidencias	RIESGO BAJO	Conforme
Registro de las incidencias	RIESGO BAJO	Conforme
Se ha reaccionado de manera diligente ante los incidentes	RIESGO BAJO	Conforme
Aplicación de medidas para impedir que los incidentes se repitan	RIESGO MEDIO	**Conforme con aclaración:** Se ha implementado un sistema de firewall externo, un sistema de protección endpoint y el hábito de revisar si se han realizado las actualizaciones periódicas necesarias

6 Notificación de las violaciones de seguridad

Artículo 33 del RGPD. Notificación de una violación de la seguridad de los datos personales a la autoridad de control

1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, como mínimo:

> *a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;*
> *b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;*
> *c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;*
> *d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.*

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo.

Artículo 34 del RGPD. Comunicación de una violación de la seguridad de los datos personales al interesado

1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

> *a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;*
> *b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;*
> *c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.*

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3.

6.1 Notificaciones a las autoridades y a los interesados

Num	Chequeo	Resultado	Nivel
1	La entidad cuenta con un protocolo relativo a la notificación de las violaciones de seguridad	Cumplimiento	●
2	En relación a los incidentes del último ejercicio, se han valorado los incidentes de manera diligente y en su caso se han realizado las notificaciones necesarias a las autoridades o a los interesados	Cumplimiento	●

6.2 Notificaciones al responsable del tratamiento

Num	Chequeo	Resultado	Nivel
1	La entidad cuenta con los datos de contacto de las personas a comunicar aquellas violaciones de seguridad relativas a datos tratados como encargados	No aplica	●
2	En relación a los incidentes del último ejercicio, que afectaran a datos de otros responsables, se han comunicado dichos incidentes a los responsables, sin dilación indebida	No aplica	●

7 Transferencia internacional de datos

Artículo 44 del RGPD. Principio general de las transferencias

Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado.

Artículo 45 del RGPD. Transferencias basadas en una decisión de adecuación

1. Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica.

2. Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos:

a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos;
b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y
c) los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

3. La Comisión, tras haber evaluado la adecuación del nivel de protección, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado a tenor de lo dispuesto en el apartado 2 del presente artículo. El acto de ejecución establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. El acto de ejecución especificará su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control a que se refiere el apartado 2, letra b), del presente artículo. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

4. La Comisión supervisará de manera continuada los acontecimientos en países terceros y organizaciones internacionales que puedan afectar a la efectiva aplicación de las decisiones adoptadas con arreglo al apartado 3 del presente artículo y de las decisiones adoptadas sobre la base del artículo 25, apartado 6, de la Directiva 95/46/CE.

5. Cuando la información disponible, en particular tras la revisión a que se refiere el apartado 3 del presente artículo, muestre que un tercer país, un territorio o un sector específico de ese tercer país, o una organización internacional ya no garantiza un nivel de protección adecuado a tenor del apartado 2 del presente artículo, la Comisión, mediante actos de ejecución, derogará, modificará o suspenderá, en la medida necesaria y sin efecto retroactivo, la decisión a que se refiere el apartado 3

del presente artículo. Dichos actos de ejecución se adoptarán de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.

Por razones imperiosas de urgencia debidamente justificadas, la Comisión adoptará actos de ejecución inmediatamente aplicables de conformidad con el procedimiento a que se refiere el artículo 93, apartado 3.

6. La Comisión entablará consultas con el tercer país u organización internacional con vistas a poner remedio a la situación que dé lugar a la decisión adoptada de conformidad con el apartado 5.

7. Toda decisión de conformidad con el apartado 5 del presente artículo se entenderá sin perjuicio de las transferencias de datos personales al tercer país, a un territorio o uno o varios sectores específicos de ese tercer país, o a la organización internacional de que se trate en virtud de los artículos 46 a 49.

8. La Comisión publicará en el Diario Oficial de la Unión Europea y en su página web una lista de terceros países, territorios y sectores específicos en un tercer país, y organizaciones internacionales respecto de los cuales haya decidido que se garantiza, o ya no, un nivel de protección adecuado.

9. Las decisiones adoptadas por la Comisión en virtud del artículo 25, apartado 6, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas por una decisión de la Comisión adoptada de conformidad con los apartados 3 o 5 del presente artículo.

Artículo 46 del RGPD. Transferencias mediante garantías adecuadas

1. A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.

2. Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por:

> *a) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;*
> *b) normas corporativas vinculantes de conformidad con el artículo 47;*
> *c) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2;*
> *d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2;*
> *e) un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o*
> *f) un mecanismo de certificación aprobado con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.*

3. Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas contempladas en el apartado 1 podrán igualmente ser aportadas, en particular, mediante:

> *a) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o*
> *b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.*

4. La autoridad de control aplicará el mecanismo de coherencia a que se refiere el artículo 63 en los casos indicados en el apartado 3 del presente artículo.

5. Las autorizaciones otorgadas por un Estado miembro o una autoridad de control de conformidad con el artículo 26, apartado 2, de la Directiva 95/46/CE seguirán siendo válidas hasta que hayan sido modificadas, sustituidas o derogadas, en caso necesario, por dicha autoridad de control. Las decisiones adoptadas por la Comisión en virtud del artículo 26, apartado 4, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas, en caso necesario, por una decisión de la Comisión adoptada de conformidad con el apartado 2 del presente artículo.

Artículo 47 del RGPD. Normas corporativas vinculantes

1. La autoridad de control competente aprobará normas corporativas vinculantes de conformidad con el mecanismo de coherencia establecido en el artículo 63, siempre que estas:

a) sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus empleados;
b) confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales, y
c) cumplan los requisitos establecidos en el apartado 2.

2. Las normas corporativas vinculantes mencionadas en el apartado 1 especificarán, como mínimo, los siguientes elementos:

a) la estructura y los datos de contacto del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta y de cada uno de sus miembros;
b) las transferencias o conjuntos de transferencias de datos, incluidas las categorías de datos personales, el tipo de tratamientos y sus fines, el tipo de interesados afectados y el nombre del tercer o los terceros países en cuestión;
c) su carácter jurídicamente vinculante, tanto a nivel interno como externo;
d) la aplicación de los principios generales en materia de protección de datos, en particular la limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento, el tratamiento de categorías especiales de datos personales, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes;
e) los derechos de los interesados en relación con el tratamiento y los medios para ejercerlos, en particular el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles de conformidad con lo dispuesto en el artículo 22, el derecho a presentar una reclamación ante la autoridad de control competente y ante los tribunales competentes de los Estados miembros de conformidad con el artículo 79, y el derecho a obtener una reparación, y, cuando proceda, una indemnización por violación de las normas corporativas vinculantes;
f) la aceptación por parte del responsable o del encargado del tratamiento establecidos en el territorio de un Estado miembro de la responsabilidad por cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro de que se trate no establecido en la Unión; el responsable o el encargado solo será exonerado, total o parcialmente, de dicha responsabilidad si demuestra que el acto que originó los daños y perjuicios no es imputable a dicho miembro;
g) la forma en que se facilita a los interesados la información sobre las normas corporativas vinculantes, en particular en lo que respecta a las disposiciones contempladas en las letras d), e) y f) del presente apartado, además de los artículos 13 y 14;
h) las funciones de todo delegado de protección de datos designado de conformidad con el artículo 37, o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, así como de la supervisión de la formación y de la tramitación de las reclamaciones;
i) los procedimientos de reclamación;
j) los mecanismos establecidos dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos incluirán auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del interesado. Los resultados de dicha verificación deberían comunicarse a la persona o entidad a que se refiere la letra h) y al consejo de administración de la empresa que controla un grupo empresarial, o de la unión de empresas dedicadas a una actividad económica conjunta, y ponerse a disposición de la autoridad de control competente que lo solicite;
k) los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la autoridad de control;
l) el mecanismo de cooperación con la autoridad de control para garantizar el cumplimiento por parte de cualquier miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, en particular poniendo a disposición de la autoridad de control los resultados de las verificaciones de las medidas contempladas en la letra j);
m) los mecanismos para informar a la autoridad de control competente de cualquier requisito

jurídico de aplicación en un país tercero a un miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, que probablemente tengan un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes, y
n) la formación en protección de datos pertinente para el personal que tenga acceso permanente o habitual a datos personales.

3. La Comisión podrá especificar el formato y los procedimientos para el intercambio de información entre los responsables, los encargados y las autoridades de control en relación con las normas corporativas vinculantes a tenor de lo dispuesto en el presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

Artículo 48 del RGPD. Transferencias o comunicaciones no autorizadas por el Derecho de la Unión

Cualquier sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país que exijan que un responsable o encargado del tratamiento transfiera o comunique datos personales únicamente será reconocida o ejecutable en cualquier modo si se basa en un acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el país tercero requirente y la Unión o un Estado miembro, sin perjuicio de otros motivos para la transferencia al amparo del presente capítulo.

Artículo 49 del RGPD. Excepciones para situaciones específicas

1. En ausencia de una decisión de adecuación de conformidad con el artículo 45, apartado 3, o de garantías adecuadas de conformidad con el artículo 46, incluidas las normas corporativas vinculantes, una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional únicamente se realizará si se cumple alguna de las condiciones siguientes:

a) el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas;
b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado;
c) la transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica;
d) la transferencia sea necesaria por razones importantes de interés público;
e) la transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones;
f) la transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento;
g) la transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta.

Cuando una transferencia no pueda basarse en disposiciones de los artículos 45 o 46, incluidas las disposiciones sobre normas corporativas vinculantes, y no sea aplicable ninguna de las excepciones para situaciones específicas a que se refiere el párrafo primero del presente apartado, solo se podrá llevar a cabo si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofreció garantías apropiadas con respecto a la protección de datos personales. El responsable del tratamiento informará a la autoridad de control de la transferencia. Además de la información a que hacen referencia los artículos 13 y 14, el responsable del tratamiento informará al interesado de la transferencia y de los intereses legítimos imperiosos perseguidos.

2. Una transferencia efectuada de conformidad con el apartado 1, párrafo primero, letra g), no abarcará la totalidad de los datos personales ni categorías enteras de datos personales contenidos en el registro. Si la finalidad del registro es la consulta por parte de personas que tengan un interés legítimo, la transferencia solo se efectuará a solicitud de dichas personas o si estas han de ser las destinatarias.

3. En el apartado 1, el párrafo primero, letras a), b) y c), y el párrafo segundo no serán aplicables a

las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus poderes públicos.

4. El interés público contemplado en el apartado 1, párrafo primero, letra d), será reconocido por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.

5. En ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el Derecho de la Unión o de los Estados miembros podrá, por razones importantes de interés público, establecer expresamente límites a la transferencia de categorías específicas de datos a un tercer país u organización internacional. Los Estados miembros notificarán a la Comisión dichas disposiciones.

6. El responsable o el encargado del tratamiento documentarán en los registros indicados en el artículo 30 la evaluación y las garantías apropiadas a que se refiere el apartado 1, párrafo segundo, del presente artículo.

Artículo 50 del RGPD. Cooperación internacional en el ámbito de la protección de datos personales

En relación con los terceros países y las organizaciones internacionales, la Comisión y las autoridades de control tomarán medidas apropiadas para:

a) crear mecanismos de cooperación internacional que faciliten la aplicación eficaz de la legislación relativa a la protección de datos personales;
b) prestarse mutuamente asistencia a escala internacional en la aplicación de la legislación relativa a la protección de datos personales, en particular mediante la notificación, la remisión de reclamaciones, la asistencia en las investigaciones y el intercambio de información, a reserva de las garantías adecuadas para la protección de los datos personales y otros derechos y libertades fundamentales;
c) asociar a partes interesadas en la materia a los debates y actividades destinados a reforzar la cooperación internacional en la aplicación de la legislación relativa a la protección de datos personales;
d) promover el intercambio y la documentación de la legislación y las prácticas en materia de protección de datos personales, inclusive en materia de conflictos de jurisdicción con terceros países.

7.1 Transferencias fuera del EEU conforme al RGPD

7.1.1 Situación actual

Transferencias existentes:

Destinatario	Tipo (responsable a responsable / responsable a encargado / encargado a subencargado)	Tipo de garantías adecuadas	Otras situaciones
-	-	-	-

7.1.2 Valoración del cumplimiento normativo

Num	Chequeo	Resultado	Nivel
1	Falta de control por parte de la empresa en relación a las transferencias internacionales de datos	Cumplimiento	●
2	Establecimiento de garantías adecuadas para las transferencias	No aplica	●