Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Creación de una guía de apoyo para responsables y encargados de tratamiento basada en el Reglamento de Protección de Datos Europeo

Trabajo Fin de Grado

Grado en Ingeniería Informática

Autor: Jesús Ortiz Amaya

Tutor: Juan Vicente Oltra Gutiérrez

Curso 2017/2018

Resumen

Este trabajo trata de realizar un estudio técnico y legal sobre la normativa de protección de datos, que en el momento en el que se desarrolla el trabajo, está compuesta por el Reglamento General de Protección de Datos y los artículos que no han sido modificados por este reglamento de la Ley Orgánica de Protección de Datos de 1999. El objetivo de este trabajo es extraer las obligaciones que los responsables y los encargados de tratamiento de datos personales deben tener en cuenta para cumplir con lo exigido por la legislación. Como resultado, se desarrollará una aplicación que expondrá de forma sistemática y catalogada las obligaciones mencionadas anteriormente y que servirá como guía para comprobar si los responsables y encargados han aplicado las medidas y principios exigidos por ley.

Palabras clave: RGPD, LOPD, tratamiento, datos, protección, guía, responsable, encargado, privacidad.

Abstract

This work tries to realize a study on data protection regulation, which in the time that the work is developed, is composed by the General Data Protection Regulation and by those articles of the Organic Law on Data Protection of 1999 that haven't been modified by this regulation. The objective of this work is to extract the obligations that the person in charge and the personal manager of data processing must have in mind to satisfy the law. As a result, an application will be developed. This application will expose the previous obligations in a systematic and cataloged way. Furthermore, this application will serve as a guide to verify if the person in charge and the manager, have applied the measures and values demanded by law.

Keywords: GDPR, LODP, processing, data, guide, person in charge, manager, privacy.

Tabla de contenidos

1. Introducción 9
1.1 Motivación 9
1.2 Objeto y objetivos 10
1.3 Metodología 10
1.4 Estructura 11
2. Estado del arte 12
2.1 Regulación sobre los tratamientos de datos 13
2.1.1 Base legal del tratamiento 14
2.1.2 Relación responsable – encargado 14
2.1.3 Notificación de ficheros 16
2.1.4 Transparencia e información a los interesados 17
2.1.5 Prestación del consentimiento 19
2.1.6 Regulación de datos sobre personas fallecidas 20
2.1.7 Datos especialmente protegidos 20
2.1.8 Derechos de los interesados 22
2.1.9 Cesión de datos a terceros 23
2.1.10 Transferencias internacionales 24
2.1.11 Análisis de riesgo 26
2.1.12 Protección de datos desde el diseño y por defecto 28
2.1.13 Medidas de seguridad 29
2.1.14 Notificación de violaciones de seguridad 29
2.1.15 Evaluación de impacto sobre la protección de datos 31
2.1.16 Delegado de protección de datos 33
2.1.17 Regulación sobre el consentimiento en las *cookies* 34
2.1.18 Regulación sobre la contratación de *cloud computing* 37
2.1.19 Regulación sobre la reutilización de la información del sector público. 39
2.1 Crítica al estado del arte 40
2.2 Propuesta 40
3. Análisis del problema 41
3.1 Requisitos técnicos sobre los tratamientos de datos 41

3.1.1 Base legal del tratamiento 42
3.1.2 Contratación de un encargado de tratamiento 43
3.1.3 Relación responsable – encargado 44
3.1.4 Notificación de ficheros 44
3.1.5 Transparencia e información a los interesados 44
3.1.6 Prestación del consentimiento 45
3.1.7 Tratamiento de datos de menores de edad 46
3.1.8 Regulación de datos sobre personas fallecidas 47
3.1.9 Datos especialmente protegidos 47
3.1.10 Calidad y proporcionalidad 47
3.1.11 Derechos de los interesados 48
3.1.12 Cesión de datos a terceros 50
3.1.13 Transferencias internacionales 51
3.1.14 Análisis de riesgo 51
3.1.15 Registro de actividades de tratamiento 53
3.1.16 Protección de datos desde el diseño y por defecto 54
3.1.17 Medidas de seguridad 54
3.1.18 Notificación de violaciones de seguridad 56
3.1.19 Evaluación de impacto sobre la protección de datos 57
3.1.20 Delegado de protección de datos 58
3.1.21 Deber de confidencialidad 59
3.2 Identificación y análisis de soluciones posibles 59
3.3 Solución propuesta 60
4. Diseño de la solución 62
5. Conclusiones 65
6. Relación del trabajo desarrollado con los estudios cursados 67
7. Referencias 68
8. Anexos 70
8.1 Etapas de una evaluación de impacto sobre la protección de datos 70
8.2 Sistema de capas para mostrar la información relativa a las *cookies* 71
8.3 Sanciones del anteproyecto de la Ley Orgánica de Protección de Datos 72
8.4 Tipología de contrato responsable – encargado 78
8.5 Ejemplos para recabar el consentimiento cumpliendo con las exigencias del RGPD 86
9 Glosario 88

1. Introducción

El 25 de mayo de 2018 entró en vigor el nuevo Reglamento General de Protección de Datos (R (UE) 2016/679 del Consejo, de 27 de abril de 2016), sustituyendo a todas las disposiciones de la Ley Orgánica de Protección de Datos de 1999 (LOPD 15/1999, 13 de diciembre de 1999) con las que entra en contradicción. Con la nueva legislación, todas las organizaciones que tratan datos de carácter personal están obligadas a adoptar las medidas necesarias para cumplir con el nuevo reglamento, lo que implica que el responsable de los tratamientos debe modificar algunos aspectos que cumplían con la antigua ley orgánica y ya no están vigentes, y añadir nuevas obligaciones que deben ser analizadas y aplicadas dependiendo de las circunstancias de cada organización. Además, los responsables deben de tener en cuenta los dos principios más característicos e importantes del nuevo reglamento: la responsabilidad proactiva y el enfoque de riesgo.

Por una parte, la responsabilidad proactiva es el principio que describe la necesidad del responsable del tratamiento de datos de aplicar medidas técnicas y organizativas para poder garantizar y demostrar que el tratamiento o tratamientos que lleva a cabo son conformes respecto al Reglamento General de Protección de Datos. En términos prácticos, este principio requiere que se analice que datos personales tratan, con que finalidad y que tipo de operaciones de tratamiento de datos llevan a cabo.

Por otra parte, el enfoque de riesgo señala que las medidas dirigidas a cumplir con el nuevo reglamento deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas. De acuerdo con este enfoque, algunas medidas del Reglamento General de Protección de Datos solo serán de aplicación cuando exista un alto riesgo para los derechos y libertades, mientras que otras deberán modularse en función del nivel y tipo de riesgo que los tratamientos presenten.

Con todo esto presente, las empresas se enfrentan a un nuevo desafío, donde tienen que adaptarse a una nueva metodología para tratar los datos personales y cuya infracción, en caso de no tomar las medidas pertinentes, puede suponer una multa administrativa que puede llegar hasta los 20.000.000 de euros.

1.1 Motivación

La elección de este Trabajo de Fin de Grado sobre otros se debe principalmente a su temática: la protección de datos. En segundo de carrera comencé a estudiar este tema y desde entonces despertó mi interés sobre como las organizaciones tratan los datos personales, que datos pueden tratar y cuáles no, cómo protege la ley los datos más sensibles o qué derechos se pueden ejercer sobre las organizaciones, sobre todo cuando la mayor parte de las empresas emplean una gran parte de sus recursos en investigar nuevas formas de obtener estadísticas y predicciones a través del tratamiento de datos personales, como por ejemplo, con el uso de la tecnología Big

Data. Desde un punto de vista personal, este trabajo supone un buen punto de partida para introducirme en la legislación de protección de datos. Desde un punto de vista profesional, este trabajo es una aproximación a las profesiones de consultoría y auditoría informática y también supone una oportunidad de poder estudiar las medidas de seguridad que aplican las empresas para la protección de los datos, a qué amenazas están expuestas y de qué dependen. Las otras opciones de trabajos que me planteaba también trataban la protección de datos, pero no desde un punto legislativo y técnico, sino que se basaban en el diseño de operaciones para el tratamiento de datos.

1.2 Objeto y objetivos

El objeto del presente Trabajo de Fin de Grado es la obtención del título de Ingeniería Informática expedido por la Universidad Politécnica de Valencia.

Los objetivos del presente trabajo se pueden dividir en dos.

- El primer objetivo es la realización de un estudio técnico del nuevo Reglamento General de Protección de Datos, para lo que se expondrán de forma sistemática, las principales cuestiones que deben tener en cuenta las organizaciones ya sean estas grandes, medianas, pequeñas, públicas o privadas.

- El segundo objetivo es la creación de una aplicación que sirva de guía, para ayudar a los responsables y encargados de tratamientos de datos de carácter personal, a adaptarse a las nuevas obligaciones que deberán tener en cuenta de cara a la aplicación del Reglamento General de Protección de Datos. Otra función de la aplicación será poder usarla a modo de lista de verificación, para que los responsables y encargados puedan determinar si se han dado los pasos necesarios para estar en condiciones de hacer una correcta aplicación del nuevo reglamento. Se pretende que la aplicación sirva de introducción a la normativa de protección de datos, utilizando un lenguaje sencillo e independiente del conocimiento en la materia que nos ocupa, la protección de datos.

1.3 Metodología

Para alcanzar los objetivos propuestos, este trabajo se divide en tres partes. La primera parte supone reunir los documentos de fuentes oficiales más significativos, que traten el Reglamento General de Protección de Datos, ya sea de forma general o porque traten aspectos específicos de él, y los puntos que siguen vigentes de la Ley Orgánica de Protección de Datos de 1999. Una vez reunidos, se clasifican en dos categorías según traen aspectos legales o aspectos técnicos. La segunda parte se basa en realizar un estudio de los aspectos técnicos de donde se extraen las obligaciones que deben tener en cuenta los responsables y los encargados de

tratamiento. Estas obligaciones son la base de la aplicación, y según ellas se construye la guía. El último paso es desarrollar la aplicación, diseñar y programar las funcionalidades. Con los aspectos legales se dará una visión de los aspectos fundamentales sobre la situación en la que se encuentra la normativa de protección de datos.

1.4 Estructura

El trabajo se compone de cuatro capítulos. El primero de ellos muestra un análisis del estado actual de la normativa de protección de datos, exponiendo las medidas que los responsables y, en ocasiones los encargados, deben aplicar para garantizar que los tratamientos son conformes con el Reglamento General de Protección de Datos.

En el segundo capítulo se expone el estudio técnico realizado sobre la normativa de protección de datos, mostrando las obligaciones que los responsables y los encargados deben de realizar para cumplir con lo exigido por el Reglamento General de Protección de Datos.

En el tercero, se explica el desarrollo de la aplicación, mostrando, por una parte, el diseño gráfico de la interfaz y por otra, la programación de las funcionalidades.

El último capítulo trata sobre las conclusiones obtenidas. Se muestran los objetivos alcanzados, las versiones futuras de la aplicación, las limitaciones encontradas y las conclusiones personales obtenidas.

Como añadido a los capítulos anteriores, en la parte final de la memoria, se pueden encontrar anexos en los que se incluyen recomendaciones de la Agencia Española de Protección de Datos sobre las evaluaciones de impacto y las *cookies*, una tipología de contrato para los encargados de tratamiento y ejemplos para recabar el consentimiento cumpliendo con lo exigido por el Reglamento General de Protección de Datos. También se puede encontrar un glosario que incluye las palabras específicas de la memoria.

2. Estado del arte

Con la entrada en vigor del Reglamento General de Protección de Datos, en adelante RGPD, el 25 de mayo de 2018, quedan derogadas las disposiciones de la Ley Orgánica de Protección de Datos, en adelante LOPD, de 1999, excepto aquellas que no son abarcadas por el reglamento. Además, se añaden nuevos principios y obligaciones que antes no habían sido contempladas por la LOPD de 1999.

El encargado de aplicar el nuevo reglamento es el responsable de tratamiento, que a efectos de este documento se entenderá como la entidad, persona o órgano administrativo que decide sobre la finalidad, el contenido y el uso del tratamiento de datos personales. Por otra parte, es importante diferenciar entre el responsable de tratamiento y el encargado de tratamiento. Se entenderá como encargado del tratamiento a la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. De aquí en adelante se le referenciará como interesado del tratamiento de datos o interesado. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios con respecto a los cuales existe una probabilidad razonable de que puedan ser utilizados por el responsable del tratamiento o por cualquier otra persona para la identificación directa o indirecta de dicha persona física.

Para determinar si existe una probabilidad razonable de que se utilicen unos medios determinados para la identificación de una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por tanto, los principios de protección de datos personales no deben aplicarse a la información anónima, es decir, a la información que no guarda relación con una persona física identificada o identificable, ni a los datos personales convertidos en anónimos de forma que el interesado al que se refieren ya no resulte identificable.

El RPGD especifica que las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de *cookies* u otros identificadores, como etiquetas de radiofrecuencia. Un ejemplo de estos identificadores en línea serían las direcciones IP, los nombres de usuario para registrarse en páginas web o los metadatos derivados de comunicaciones electrónicas. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser usados para elaborar perfiles de las personas físicas e identificarlas.

Asimismo, el RGPD define una lista de datos considerados especialmente protegidos, en los que se incluyen: la ideología, la afiliación sindical, la religión, el origen racial, la

vida sexual, las infracciones penales y administrativas, los datos relativos a la salud, los datos genéticos y los datos biométricos.

Cualquier actividad en la que estén presentes datos de carácter personal constituirá un tratamiento de datos, ya se realice de manera manual o automatizada, total o parcialmente.

2.1 Regulación sobre los tratamientos de datos

El RGPD en su artículo 5, establece los principios que todo tratamiento de datos debe basarse. Los principios se muestran a continuación:

• Licitud, lealtad y transparencia: los datos personales deben ser tratados de manera lícita, leal y transparente en relación con el interesado.

•Limitación de la finalidad**:** los datos personales deben ser recogidos con fines determinados, explícitos y legítimos, y no deben ser tratados de manera incompatible con dichos fines. No se considerará incompatible con los fines iniciales el tratamiento posterior de los datos con fines de archivo de interés público, fines de investigación científica e histórica o fines estadísticos.

• Minimización de datos: los datos personales deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

• Exactitud: los datos personales deben ser exactos y si fuera necesario actualizados, adoptándose medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos a los fines para los que se tratan.

• Limitación del plazo de conservación: los datos personales deben ser mantenidos de forma que se permita la identificación de los interesados no más tiempo del necesario para los fines del tratamiento. Podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo de interés público, fines de investigación científica e histórica o fines estadísticos, sin perjuicio de la aplicación de las correspondientes medidas técnicas y organizativas apropiadas que impone el RGPD.

• Integridad y seguridad: los datos personales deben ser tratados de manera que se garantice su adecuada seguridad, incluyendo la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, aplicando las medidas técnicas y de organización apropiadas.

• Responsabilidad proactiva: el responsable del tratamiento debe de cumplir todos los principios anteriores y ser capaz de demostrar dicho cumplimiento.

El RGPD establece un catálogo de medidas que el responsable y, en ocasiones los encargados, deben aplicar para garantizar que los tratamientos son conformes a al nuevo reglamento. El catálogo de medidas se compone de los siguientes puntos.

2.1.1 Base legal del tratamiento

El tratamiento de los datos personales debe apoyarse en una base legal que lo legitime, por tanto, es necesario que los datos se traten de acuerdo con las condiciones recogidas en el RGPD. En este sentido, el artículo 6 del RGPD recoge los supuestos en los que se considera que el tratamiento de datos personales es lícito. Los supuestos no mantienen entre sí ninguna relación de prioridad o prelación:

• Que se cuente con el consentimiento del interesado para los fines específicos del tratamiento.

• Que el tratamiento sea 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.

• Que el tratamiento sea necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.

• Que el tratamiento sea necesario para proteger intereses vitales del interesado o de otra persona física.

• Que el tratamiento sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

• Que el tratamiento sea 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.

El interés legítimo se puede utilizar como base de licitud de un tratamiento siempre que no prevalezcan los intereses o los derechos y libertades de los interesados y teniendo en cuenta las expectativas razonables de las personas afectadas por el tratamiento, basadas en la relación que tienen con el responsable del tratamiento.

En los casos en que la base jurídica de los tratamientos sea el consentimiento, éste deberá tener las características previstas por el RGPD. Más adelante, en la sección 2.1.5, se presentan y analizan estas características y la forma en la que debe ser recabado el consentimiento.

2.1.2 Relación responsable – encargado

El responsable debe elegir un encargado que ofrezca las garantías suficientes respecto a la implantación y al mantenimiento de las medidas técnicas y organizativas apropiadas, de acuerdo con lo establecido en el RGPD y que garantice la protección de los derechos de las personas afectadas.

La relación entre el responsable y el encargado debe quedar establecida en un contrato o en un acto jurídico similar que los vincule. Si se trata de un contrato debe de contener los requisitos establecidos en el RGPD. Si por el contrario es un acto jurídico, puede basarse en clausulas tipo por la comisión europea o por la autoridad de control competente.

La Agencia Española de Protección de Datos, en adelante AEPD, estipula en la guía de directrices para la elaboración de contratos entre responsables y encargados el contenido mínimo de un acuerdo o acto con un encargado de tratamiento. El acuerdo debe contener los siguientes puntos:

• Instrucciones del responsable de tratamiento: es necesario identificar de forma clara y concreta cuales son los tratamientos de datos a realizar por el encargado de tratamiento, atendiendo al servicio prestado y a la forma de prestarlo. Es necesario determinar de forma clara las comunicaciones a terceros que el responsable encomienda al encargado o que se derivan de su servicio prestado.

• El deber de confidencialidad: hay que establecer de forma clara que el encargado garantiza que las personas autorizadas en tratar los datos personales se han comprometido de forma expresa a respetar la confidencialidad o están sujetas a una obligación de confidencialidad estatutaria. Debe quedar documentado y a disposición del responsable.

• Medidas de seguridad: se debe de establecer la obligación del encargado de adoptar las medidas de seguridad necesarias con conformidad al RGPD. El responsable y el encargado deben de establecer las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado, que deben de incluir la seudonimización y el cifrado de datos personales, la capacidad de garantizar la confidencialidad, la integridad, la disponibilidad y la resiliencia permanente de los sistemas y servicios de tratamiento, la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, y un proceso de evaluación y valoración de la eficiencia de las medidas técnicas y organizativas.

• El régimen de subcontratación: el RGPD exige la autorización previa y por escrito antes de que el encargado realice una subcontratación. El subencargado, es decir, el encargado subcontratado, está sujeto a las mismas condiciones que el encargado.

• Los derechos de los interesados: hay que establecer la forma en la que el encargado asiste al responsable en el cumplimiento de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados. Los derechos contemplados son el derecho de acceso, el derecho de rectificación, el derecho de supresión, el derecho de limitación, el derecho de portabilidad, el derecho de oposición y a no ser objeto de decisiones individualizadas automatizadas. El acuerdo debe establecer si es el encargado a quien corresponde atender y dar respuestas a las solicitudes o bien comunicar al responsable que se ha ejercido un derecho. En el primer supuesto, se debe establecer la forma y plazo para atender o en su caso, dar respuesta a la solicitud. En el segundo supuesto, se debe establecer la forma y plazo para comunicar la solicitud al responsable.

• La colaboración en el cumplimiento de las obligaciones del responsable: se debe establecer la forma por la cual el encargado ayuda al responsable a garantizar el cumplimiento de las obligaciones relativas a la aplicación de las medidas de seguridad que correspondan, la notificación de violaciones de datos a las autoridades de protección de datos, la comunicación de violaciones de datos a los interesados, la realización de las evaluaciones de impacto sobre la protección de datos y, en su caso, la realización de consultas previas.

• El destino de los datos al finalizar la prestación: se debe establecer si al final de la prestación de los servicios de tratamiento se debe proceder a la supresión o a la devolución de los datos y de cualquier copia existente. Debe quedar de forma clara cuál de las dos opciones es la elegida y los plazos en que debe cumplirse.

• La colaboración con el responsable para demostrar el cumplimiento: es necesario poner a disposición del responsable toda la documentación necesaria para demostrar el cumplimiento de las directrices establecidas, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, realizadas por el responsable o por otro auditor que responda por el responsable.

Los requisitos del RGPD se aplican a encargados localizados dentro del espacio de la Unión Europea, y a los tratamientos de datos personales dentro de este espacio. En el caso de establecer un acuerdo con un encargado que no está localizado en la Unión o que el tratamiento se efectúa fuera de la Unión, la comunicación de datos se rige por la regulación establecida en el reglamento para las transferencias internacionales.

2.1.3 Notificación de ficheros

Con el RGPD desaparece la obligación de notificar la inscripción de ficheros, tanto de responsables públicos o como privados, en el registro de ficheros de la AEPD, o al registro de la autoridad autonómica competente. Esta medida puede tener un carácter provisional, ya que el anteproyecto de la Ley Orgánica de Protección de Datos (Anteproyecto LOPD, s/f), que en el momento en el que se está desarrollando el trabajo no ha sido aprobado por el Congreso de los Diputados de España, puede volver a añadir la obligación de notificación de ficheros. Hay que tener en cuenta que un Estado miembro puede añadir nuevas obligaciones al RGPD, pero no puede eliminarlas.

Sin embargo, los responsables y encargados deben mantener un registro de actividades de tratamiento por escrito, incluso en formato electrónico. El registro debe de estar a disposición de la autoridad de control, por lo que debe estar permanentemente actualizado y en un formato claro y legible que facilite su comprensión por parte de terceros. El registro de actividades de tratamiento se debe entender como un documento vivo, que requiere revisión continua y actualización cada vez que se produzca un cambio relevante en alguna actividad de tratamiento registrada.

El registro de actividades de tratamiento debe contener una descripción de los tratamientos de datos que se realizan con la siguiente información:

• Nombre y datos de contactos del responsable.

• Finalidades del tratamiento.

• Nombre y datos de contacto del delegado de protección de datos (si lo hubiere).

• Categorías de datos personales.

• Categorías de los interesados.

• Descripción de las medidas técnicas y organizativas de seguridad.

• Categorías de destinatarios de comunicaciones, incluidos terceros países u organizaciones internacionales.

• En el caso de haber transferencias internacionales como las indicadas en el artículo 49, apartado 1, párrafo segundo[1], la documentación de garantías adecuadas.

• Cuando sea posible, plazos previstos para la supresión de las diferentes categorías de datos.

La implementación de este registro obliga a inventariar todos los tratamientos que se están realizando. Los tratamientos se deben incluir en el registro de actividades en el momento previo antes de su puesta en marcha.

El registro puede organizarse sobre la base de las informaciones de los ficheros notificados al registro general de protección de datos de la AEPD, si bien no es un registro de ficheros sino de tratamientos. Para configurar este registro de tratamientos, se puede partir de operaciones de tratamiento concretas a una finalidad básica común de todas ellas, así como de los ficheros que ya se encuentren inscritos.

2.1.4 Transparencia e información a los interesados

El RGPD regula el derecho a la información en sus artículos 13 y 14, distinguiendo entre la información que se debe facilitar al titular de los datos dependiendo si los datos personales se han obtenido del mismo o no. Hasta la aplicación del RGPD, la información que debía facilitarse era la siguiente:

[1] 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.

• La existencia de un fichero o tratamiento de datos personales.

• La finalidad para la cual se recaban los datos personales.

• Quiénes son los destinatarios de la recogida de los datos personales.

• Donde pueden ejercitar los derechos los interesados.

• La identidad de quién recaba los datos personales.

Sin embargo, con el RGPD esta lista de información se amplía, de tal forma que se debe incluir los siguientes puntos:

• Los datos de contacto del delegado de protección de datos (si lo hubiere).

• La base jurídica o legitimación del tratamiento.

• El plazo o criterios de conservación de la información.

• La existencia de decisiones automatizadas o elaboración de perfiles.

• La previsión de transferencias de datos a terceros países.

• El derecho a presentar una reclamación ante las autoridades de control competentes.

Y, en el caso de que los datos no se obtengan del propio interesado:

• El origen de los datos.

• Las categorías de los datos.

Además, en el caso de que los datos no se obtengan del propio interesado por proceder de alguna cesión legítima, el responsable informará a las personas interesadas dentro de un plazo razonable, pero, en cualquier caso:

• Antes de un mes desde que se obtuvieron los datos personales.

• Antes o en la primera comunicación con el interesado.

• Antes de que los datos, en su caso, se hayan comunicado a otros destinatarios.

Esta obligación de informar se debe cumplir sin necesidad de requerimiento alguno, y el responsable debe poder acreditar con posterioridad que ha sido satisfecha. La información se debe proporcionar de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.

El RGPD también regula una serie de supuestos en los que no es necesario cumplir con este derecho de información:

• Cuando el interesado ya disponga de la información.

• En el caso de que los datos no procedan del interesado, cuando la comunicación resulte imposible o suponga un esfuerzo desproporcionado, cuando el registro o la comunicación esté expresamente establecido por el derecho de la Unión o de los

Estados miembros, o cuando los datos deban seguir teniendo carácter confidencial por un deber legal de secreto.

2.1.5 Prestación del consentimiento

Como se ha menciona de la sección 2.1.1, los tratamientos cuya base legal sea la prestación del consentimiento, el responsable debe asegurarse que este sea inequívoco. El consentimiento inequívoco es aquel que se ha prestado mediante una manifestación del interesado o mediante una clara acción afirmativa. Los consentimientos conocidos como tácitos, basados en la inacción de los interesados, dejan de ser válidos a partir de la aprobación del RGPD, incluso para tratamientos iniciados con anterioridad. En estos casos, debe encontrase una base jurídica adecuada dentro de las que ofrece el RGPD. Si se produce un cambio de base jurídica, los interesados deben ser informados del cambio y deben poder ejercer los derechos asociados a la nueva base.

Dentro del marco del RGPD, el consentimiento se caracteriza por lo siguiente:

• Puede ser para uno o varios fines. En este caso:

◦ Sería posible agruparlas en virtud de su vinculación. Un ejemplo de ello es el consentimiento para la recepción de publicidad propia o de terceros.

◦ Sin embargo, lo anterior no es posible cuando los tratamientos implican conductas distintas.

• Debe ser prestado de forma libre, si bien en el ámbito de las Administraciones Públicas, siempre que actúen en el ejercicio de sus competencias, esta libertad puede no existir.

• Debe ser revocable.

• El responsable debe poder probar en todo momento que ha obtenido el consentimiento.

• Debe utilizar un lenguaje claro y sencillo.

Si se usa para obtenerlo una declaración escrita, debe quedar claramente diferenciada la parte referente a la protección de datos del resto de declaraciones.

Asimismo, en el supuesto de datos sensibles, en la adopción de decisiones automatizadas y en transferencias internacionales, el consentimiento, además de inequívoco, ha de ser explícito.

Por parte de la legitimación del tratamiento de datos personales mediante el consentimiento de menores, el RGPD determina que los Estados miembros pueden establecer por ley el consentimiento de los menores siempre que la edad no sea inferior a 13 años ni superior a 16. En España, esa edad está fijada en los 14 años.

2.1.6 Regulación de datos sobre personas fallecidas

El considerando 27 del RGPD afirma que: “el presente reglamento no se aplica a la protección de datos personales de personas fallecidas. Los Estados miembros son competentes para establecer normas relativas al tratamiento de los datos personales de estas”.

Esta exclusión del ámbito de aplicación viene ratificada en el considerando 158: “el presente reglamento también debe aplicarse al tratamiento de datos personales realizado con fines de archivo, teniendo presente que no debe ser de aplicación a personas fallecidas”. También viene ratificada en el considerando 160: “el presente reglamento debe aplicarse asimismo al tratamiento de datos personales que se realiza con fines de investigación histórica. Esto incluye asimismo la investigación histórica y la investigación para fines genealógicos, teniendo en cuenta que el presente reglamento no es de aplicación a personas fallecidas”.

Por lo que la regulación que se debe seguir para la protección de los datos de las personas fallecidas es la LOPD de 1999. En sí, la LOPD de 1999, no hace ningún tipo de referencia a la protección de los datos de los fallecidos, sin embargo, el reglamento de desarrollo del año 2007 (RDL 1720/2007, 21 de diciembre) sí contiene una previsión específica al respecto en su artículo 2.4: “este reglamento no será de aplicación a los datos referidos a personas fallecidas. No obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de este con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos”.

Siguiendo la regulación impuesta por la LOPD de 1999, esta no resulta de aplicación al tratamiento de los datos de los fallecidos. Por otra parte, la norma reglamentaria contempla la posibilidad de que las personas vinculadas al fallecido, por razones familiares o análogas, puedan comunicar la defunción y, en su caso, solicitar la cancelación de los datos.

2.1.7 Datos especialmente protegidos

La regla general contemplada en el RGPD según en su artículo 9 es la prohibición del tratamiento de categorías especiales. El RGPD incluye en el concepto de datos especialmente protegidos a las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, datos relativos al origen racial o étnico, datos relativos a la salud o a la vida, la orientación sexual, los datos genéticos y los datos biométricos. No obstante, se recogen excepciones a esta regla general:

• El tratamiento es necesario para el cumplimiento de obligaciones y para 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 de la persona afectada.

• 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.

• El tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos.

• 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.

• 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 de la persona afectada.

Como motivos de interés público amparado en habilitaciones legales que exceptúan la prohibición, el propio RGPD recoge expresamente los siguientes supuestos:

• 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.

• 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.

• El tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

Además, los tratamientos de estos datos deben de estar supeditado a las garantías adecuadas de protección de los derechos y libertades del interesado que se establecen en la legislación. El consentimiento del interesado no debe constituir en sí mismo un fundamento jurídico para que las autoridades competentes procedan al tratamiento de datos personales sensibles.

2.1.8 Derechos de los interesados

Con carácter general, los responsables deben facilitar a los interesados el ejercicio de sus derechos, y para lograrlo, tanto los procedimientos como las formas deben ser visibles, accesibles y sencillas.

La LOPD de 1999 incluía como derechos de los interesados el derecho de acceso, el de rectificación, el de oposición y el de cancelación. Sin embargo, el RGPD no solo añade nuevos derechos, sino que también modifica el derecho de acceso que había sido definido en la antigua ley orgánica.

A continuación, se muestra el resultado de la aplicación del RGPD sobre la lista de derechos de los interesados establecida por la LOPD de 1999:

• Derecho de acceso: el titular de los datos tiene derecho a solicitar y obtener información de sus datos de carácter personal sometidos a tratamiento, y del origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos. La LOPD de 1999 no obligaba a facilitar copias o documentos excepto en el caso de historial clínico, sin embargo, el RGPD sí que reconoce el derecho de obtener una copia de los datos personales objetos del tratamiento.

• Derecho de rectificación: el titular de los datos tiene derecho a que se actualicen sus datos si son inexactos o incompletos. El RGPD no aplica ninguna modificación a este derecho.

• Derecho de cancelación: el titular de los datos tiene derecho a que se borren o se supriman sus datos si son inexactos o se han tratado ilegalmente. Respecto a este derecho, el RGPD tampoco aplica ninguna modificación.

• Derecho de oposición: el titular de los datos tiene derecho a solicitar que no se traten sus datos. El RGPD tampoco aplica ninguna modificación a este derecho.

• Derecho al olvido: no está considerado un derecho autónomo o diferenciado de los derechos clásicos, sino la consecuencia de la aplicación del derecho de cancelación de los datos personales.

• Derecho de limitación del tratamiento: la limitación de tratamiento supone que, a petición del interesado, no se aplicarán a sus datos personales las operaciones de tratamiento que en cada caso corresponderían. Se puede solicitar la limitación cuando:

○ El interesado ha ejercido los derechos de rectificación u oposición y el responsable está en proceso de determinar si procede a atender a la solicitud.

○ El tratamiento es ilícito, lo que determinaría el borrado de los datos, pero el interesado se opone a ello.

○ Los datos ya no son necesarios para el tratamiento, que también determinaría su borrado, pero el interesado solicita la limitación porque los necesita para la formulación, el ejercicio o la defensa de reclamaciones.

• Derecho a la portabilidad: el derecho a la portabilidad de los datos es una forma avanzada del derecho de acceso por el cual la copia que se proporciona al interesado debe ofrecerse en un formato estructurado, de uso común y lectura mecánica. Este derecho sólo puede ejercerse:

- Cuando el tratamiento se efectúe por medios automatizados.
- Cuando el tratamiento se base en el consentimiento o en un contrato.
- Cuando el interesado lo solicita respecto a los datos que haya proporcionado al responsable y que le conciernan, incluidos los datos derivados de la propia actividad del interesado.

El RGPD contempla excepciones a los derechos de acceso, rectificación y cancelación en el caso de los ficheros de las Fuerzas y Cuerpos de Seguridad, que podrán denegarse en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

Otras excepciones afectan a los ficheros de la Hacienda Pública que podrán denegar el ejercicio de los derechos en el caso de que se obstaculicen las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el interesado esté siendo objeto de actuaciones inspectoras.

2.1.9 Cesión de datos a terceros

Según los artículos 11 y 21 de la LOPD antes de comunicar datos a un tercero, es necesario recabar el consentimiento previo del interesado. No obstante, no será necesario obtener el consentimiento del interesado para la cesión de los datos, en los siguientes casos:

• Cuando tenga por objeto la satisfacción de un interés legítimo del cesionario y lo autorice una norma con rango de Ley o una norma de Derecho, siempre que no prevalezca el interés a los derechos y libertades fundamentales de las personas cuyos datos van a ser cedidos o cuando la cesión de los datos sea necesaria para cumplir un deber que imponga una de dichas normas.

• Cuando esté autorizada por Ley.

• Cuando se trate de datos recogidos de fuentes accesibles al público.

• En caso de que exista una relación jurídica que implique la cesión y esta se limite a la finalidad que la justifique.

• Cuando el destinatario sea el Ministerio Fiscal, los Jueces y Tribunales, el Defensor del Pueblo o el Tribunal de Cuentas, o sus análogos autonómicos.

• En caso de urgencia relativa a la salud o para la realización de estudios epidemiológicos en los casos legalmente previstos.

Al mismo tiempo, para las cesiones de datos entre Administraciones Públicas, siguiendo la guía de protección de datos y administración local de la AEPD, no será necesario obtener el consentimiento del interesado en los siguientes casos:

• Cuando se realicen entre Administraciones Públicas con fines históricos, estadísticos o científicos.

• Si se trata de datos recogidos de fuentes accesibles al público excepto si se destinan a ficheros privados.

• Para el ejercicio de las mismas competencias o de competencias que versen sobre las mismas materias.

• Si se trata de los datos de carácter personal que una administración pública obtenga o elabore con destino a otra.

2.1.10 Transferencias internacionales

Cuando los datos personales se envían fuera del ámbito del Espacio Económico Europeo, que comprende todos los Estados miembros de la Unión Europea, más Noruega, Islandia y Liechtenstein, se produce una transferencia internacional de datos. El modelo de transferencias internacionales diseñado por el RGPD sigue los mismos criterios que el establecido por la Directiva 95/46 (Dir. 95/46/CE del Consejo Europeo, de 24 de octubre de 1995) y por las legislaciones nacionales de transposición.

Los datos solo podrán ser comunicados fuera del Espacio Económico Europeo:

• A países, territorios o sectores específicos y a organizaciones internacionales, sobre los que la Comisión Europea haya adoptado una decisión reconociendo que ofrecen un nivel de protección adecuado.

• Cuando se hayan ofrecido garantías adecuadas sobre la protección que los datos recibirán en su destino.

• Cuando se aplique alguna de las excepciones que permiten transferir los datos sin garantías de protección adecuada, por razones de necesidad vinculadas al propio interés del titular de los datos o a intereses generales.

Se consideran países que proporcionan un nivel de protección adecuado, los Estados miembros de la Unión Europea, Islandia, Liechtenstein, Noruega o un Estado declarado por la comisión de las Comunidades Europeas como capaz de garantizar un nivel de protección adecuado, estando incluidos, hasta la fecha, Suiza, Argentina, las entidades estadounidenses adheridas a los principios de Puerto Seguro, Guernsey, Isla de Man y las entidades canadienses sujetas al ámbito de aplicación de la ley canadiense de protección de datos.

Se debe obtener la autorización previa del director de la AEPD cuando se tenga previsto realizar transferencias internacionales de datos a países que no proporcionan un nivel de protección adecuado y la transferencia no se ampare en alguna de las excepciones definidas en el artículo 49 del RGPD. Las excepciones se muestran a continuación:

• El interesado ha dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él debido a la ausencia de una decisión de adecuación y de garantías adecuadas.

• La transferencia es 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.

• La transferencia es necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica.

• La transferencia es necesaria por razones importantes de interés público.

• La transferencia es necesaria para la formulación, el ejercicio o la defensa de reclamaciones.

• La transferencia es necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado está física o jurídicamente incapacitado para dar su consentimiento.

• La transferencia se realiza desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tiene por objeto facilitar información al público y está 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 las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta.

Si la transferencia cumple alguna de las anteriores excepciones no es necesario obtener la autorización previa del director de la AEPD, no obstante, es obligatorio informar tanto a la AEPD como a los interesados.

Por otra parte, si el responsable o el encargado realiza transferencias internacionales, deben tener en cuenta los siguientes puntos que se definen en el RGPD:

• Las decisiones de adecuación que la Comisión Europea adoptó antes de la aplicación del RGPD siguen siendo válidas, y podrán seguir realizándose transferencias basadas en ellas, hasta que la Comisión Europea no las sustituya o derogue.

• Las decisiones de la Comisión Europea que establecieron sobre las cláusulas tipo para los contratos en los que se establecían garantías para las transferencias internacionales, siguen siendo válidas hasta que la Comisión Europea las sustituya o derogue.

• Las autorizaciones de transferencias que las autoridades nacionales de protección de datos otorgaron sobre la base de garantías contractuales siguen siendo válidas hasta que las autoridades no las revoquen.

• Las garantías sobre la protección que recibirán los datos en el destino las debe ofrecer el exportador, que puede ser tanto un responsable como un encargado de tratamiento.

• Se amplía la lista de posibles instrumentos para ofrecer garantías, incluyéndose, las normas corporativas vinculantes para responsables y encargados, los códigos de conducta y esquemas de certificación, así como las cláusulas contractuales modelo que puedan aprobar las autoridades de protección de datos.

• En los casos de normas corporativas vinculantes, cláusulas contractuales estándar, códigos de conducta y esquemas de certificación, la transferencia no requerirá la autorización de las autoridades de supervisión.

• Se añade una excepción al listado que en su momento estableció la Directiva 95/46. Se trata de la posibilidad de que el responsable pueda transferir los datos a un país sin el nivel adecuado de protección, cuando esa transferencia sea necesaria para satisfacer intereses legítimos imperiosos del responsable y la transferencia no es repetitiva y afecta sólo a un número limitado de interesados. En todo caso, la transferencia solo será posible si no prevalecen los derechos, libertades e intereses de las personas afectadas y deberá comunicarse a la autoridad de protección de datos.

2.1.11 Análisis de riesgo

El RGPD introduce el análisis de riesgo con la finalidad de que los responsables lleven a cabo una valoración del riesgo sobre los tratamientos que realizan. Este análisis de riesgo variará en función de:

• Los tipos de tratamiento.

• La naturaleza de los datos.

• El número de interesados.

• La cantidad y variedad de tratamientos que realice una misma organización.

Por otra parte, el RGPD no solo tiene en cuenta que el análisis de riesgo debe abarcar a las amenazas que se ciernen sobre la organización, sino también al riesgo existente en aplicar actividades de tratamiento sobre los datos personales de los interesados.

La AEPD en su guía práctica de análisis de riesgo en los tratamientos de datos personales sujetos al RGPD, detalla una hoja de ruta a seguir para realizar un correcto análisis de riesgo:

El primer paso es implantar la protección de datos desde el diseño y por defecto. Significa que el análisis de riesgo se debe de tener en cuenta desde el mismo

momento en el que se están definiendo las actividades de tratamiento. El responsable debe establecer procedimientos de control y seguridad que garanticen los principios de protección de datos.

El segundo paso es la definición y el diseño de las actividades de tratamiento. La definición de una actividad de tratamiento es un paso que requiere tener claro cuáles son las finalidades del tratamiento de datos personales. Corresponde a cada organización, de acuerdo con el principio de responsabilidad proactiva, decidir el nivel de agregación o segregación para elaborar el registro de actividades de tratamiento y debe valorar hasta qué punto esa agregación o segregación corresponde con las finalidades, las bases jurídicas y los grupos de individuos distintos.

La definición de las actividades de tratamientos permite obtener un conocimiento del ciclo de vida de los datos, de las actividades realizadas y de cualquier elemento que interviene en las mismas.

Una vez se han definido todas las actividades de tratamiento, se deben atender a las obligaciones que describe el RGPD sobre los responsables y los encargados, y analizar si es necesario incluir nuevas actividades de tratamiento. Las obligaciones están comprendidas en el artículo 5 ya mencionado en la sección 2.1.

Adicionalmente, el artículo 5 del RPGD establece que el responsable del tratamiento deberá garantizar el cumplimiento de los principios relativos al tratamiento y también ser la figura responsable de demostrarlo. Por tanto, es fundamental definir adecuadamente las actividades de tratamiento y documentar los análisis realizados, así como, dejar trazabilidad de estos y de las conclusiones que los soportan para poder garantizar la responsabilidad proactiva.

Una vez definidas todas las actividades de tratamiento, se procede a realizar el análisis de riesgo. Para el análisis de riesgo se establecen dos situaciones, la primera es que las actividades de tratamiento son de escaso riesgo o en cambio, las actividades de tratamiento comportan un alto riesgo. Si las actividades de tratamiento entrañan un alto riesgo, se deberá analizar cada actividad de forma individual, para concluir si entraña un alto riesgo y si se requiere de una evaluación de impacto sobre la protección de datos, en adelante, EIPD. En caso de que se determine que no es necesario realizar una EIPD, se debe documentar adecuadamente los motivos por los cuales se ha llegado a esa conclusión. En cualquier caso, se debe mantener evidencia de que se ha llevado a cabo este análisis.

El artículo 35.3 del RGPD describe los siguientes casos en los cuales se ha considerado que un tratamiento puede derivar en alto riesgo:

• Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se basan en un tratamiento automatizado como la elaboración de perfiles y sobre cuya base se toman decisiones que producen efectos jurídicos para las personas físicas o que les afectan de modo similar.

• Tratamiento a gran escala de las categorías especiales de datos personales, o datos sobre condenas e infracciones penales o medidas de seguridad conexas.

• Observación sistemática a gran escala de una zona de acceso público.

Los riesgos son variables y pueden cambiar ante variaciones en las actividades de tratamiento. Para garantizar una adecuada gestión de riesgos se debe tener en cuenta una monitorización continua de los riesgos y una evaluación periódica de la efectividad de las medidas de control definidas para reducir el nivel de exposición al riesgo.

2.1.12 Protección de datos desde el diseño y por defecto

El RGPD contiene dos principios para la implementación efectiva de la responsabilidad proactiva, el primero es la protección de datos desde el diseño y el segundo la protección de datos por defecto.

El principio de protección de datos desde el diseño supone que la protección de datos ha de estar presente en las primeras fases de concepción de un proyecto y formar parte de la lista de elementos a considerar antes de iniciar las sucesivas etapas de desarrollo. Estos requisitos se van a traducir en medidas técnicas y organizativas con el objeto de aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento.

Por su parte, la protección de datos por defecto consiste en que sólo sean objeto de tratamiento los datos personales que sean estrictamente necesarios para cada uno de los fines de tratamiento. Si fuera posible por la naturaleza del proceso, llegar a que no se traten datos de carácter personal.

El principio de protección de datos por defecto requiere que el responsable tenga en cuenta las siguientes obligaciones durante todo el ciclo de vida de los datos:

• Debe analizar los tipos de datos que se recaban con un criterio de minimización.

• Debe analizar los procesos asociados a dichos tratamientos para que se acceda a los mínimos datos personales necesarios para ejecutarlos.

• Debe implementar una política de conservación de datos que permita, con un criterio restrictivo, eliminar aquellos datos que no sean estrictamente necesarios.

• Debe limitar el acceso por parte de terceros a dichos datos personales.

El encargado del tratamiento también debe tener en cuenta los principios de la protección de datos desde el diseño y de la protección de datos por defecto.

2.1.13 Medidas de seguridad

La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de las oportunas medidas de carácter técnico y organizativo con el fin de garantizar el cumplimiento de lo dispuesto en el RGPD. La aplicación de tales medidas no puede depender únicamente de criterios económicos. A fin de poder demostrar que se cumple con lo dispuesto en el RGPD, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que respeten los principios de la protección de datos desde la concepción y de la protección de datos por defecto.

El RGPD no establece medidas de seguridad estáticas, al contrario que la LOPD de 1999, por lo que corresponde al responsable determinar aquellas medidas de seguridad que son necesarias para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales.

Para los tratamientos iniciados con anterioridad a la aplicación del RGPD, la normativa a cumplir era el Título VIII del Real Decreto 1720/2007 (RLD 1720/2007, de 21 de diciembre), donde se establecían unos controles mínimos de obligado cumplimiento para garantizar la seguridad de los datos. Dichas medidas de seguridad se deben de mantener y revisar. En ningún caso el RGPD se debe de entender como la eliminación automática de todas las medidas de seguridad ya existentes.

Según el artículo 32 del RGPD las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado se definen en función de: el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de los interesados. En definitiva, el primer paso para determinar las medidas de seguridad es la realización de un análisis de riesgo. Una vez evaluado el riesgo, será necesario determinar las medidas de seguridad encaminadas para reducir o eliminar los riesgos para el tratamiento de los datos.

Por otra parte, el responsable tendrá que redactar un documento de seguridad. Es un documento interno de la organización, que debe mantenerse siempre actualizado. Disponer del documento de seguridad es una obligación para todos los responsables y, en su caso, para los encargados del tratamiento.

2.1.14 Notificación de violaciones de seguridad

Cuando se produzca una violación o quiebra de seguridad, es decir, la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos, el responsable del tratamiento que la sufra, siempre que exista riesgo para los derechos y libertades de las personas físicas, deberá notificarlo:

• A la AEPD, en un plazo máximo de 72 horas.

• A las personas físicas cuyos datos personales se hayan visto afectados por la quiebra de seguridad, cuanto antes.

• Sin perjuicio de lo anterior, para las Administraciones Públicas, a efectos de notificación se tendrán en cuenta las obligaciones derivadas del Esquema Nacional de Seguridad y las instrucciones técnicas aplicables.

Existen excepciones, definidas en el artículo 34 del RGPD, para no comunicar la quiebra de seguridad a los afectados por la violación de seguridad:

• Si se han adoptado y aplicado medidas sobre los datos personales afectados, particularmente aquellas que hagan ininteligibles los datos para cualquier persona que no esté autorizada a acceder ellos como, por ejemplo, que se hayan cifrado los datos personales.

• El responsable ha adoptado medidas ulteriores que garanticen que ya no existe un alto riesgo para los derechos y libertades. El criterio de alto riesgo debe entenderse en el sentido de que sea probable que la violación de seguridad ocasione daños a los interesados.

• Que esta comunicación fuese un esfuerzo desproporcionado, optándose por una comunicación pública o medida semejante por la que se informe de forma efectiva a las personas afectadas.

El contenido mínimo de la comunicación de la quiebra de seguridad a la AEPD queda especificado en el artículo 33 del RGPD, siendo el siguiente:

• Naturaleza de la quiebra de seguridad.

• Categorías de personas afectadas, por ejemplo: menores, discapacitados, empleados, ciudadanos.

• Número aproximado de personas afectadas.

• Categorías de datos comprometidos, por ejemplo: identificativos, salud, laborales.

• Número de registros de datos personales afectados.

• Nombre y datos de contacto del delegado de protección de datos (si lo hubiere).

• Posibles consecuencias de la quiebra de seguridad sufrida.

• Medidas adoptadas o propuestas para remediar esta quiebra.

• Si procede las medidas aplicadas para paliar los posibles efectos negativos sobre los interesados.

Se considera que se tiene constancia de una violación de seguridad cuando hay una certeza de que se ha producido y se tiene un conocimiento suficiente de su naturaleza y alcance. La mera sospecha de que ha existido una quiebra o la constatación de que ha sucedido algún tipo de incidente sin que se conozcan mínimamente sus circunstancias no deberían dar lugar a la notificación, dado que en esas condiciones

no sería posible determinar hasta qué punto puede existir un riesgo para los derechos y libertades de los interesados.

Por otra parte, si el encargado del tratamiento sufre una quiebra de seguridad, éste debe notificar sin dilación al responsable la existencia de esta. El RGPD no indica ni el formato de dicha notificación ni el plazo máximo para que se realice dicha notificación ya que el plazo establecido para el responsable se fija a partir del conocimiento de la quiebra de seguridad. Por lo tanto, el responsable deberá fijar las obligaciones de notificación del encargado dentro del contrato que los relaciona, indicando un plazo máximo de notificación y a través de que medio se comunicará, además de adjuntar toda la documentación relevante de la quiebra, de tal forma que el responsable pueda cumplir con los requisitos que sí obliga el RGPD, en particular, en relación con los datos que es necesario notificar a terceros. El responsable también tiene la obligación de mantener un registro de los incidentes de seguridad que se han producido.

2.1.15 Evaluación de impacto sobre la protección de datos

La evaluación de impacto sobre la protección de datos es una herramienta con carácter preventivo que debe realizar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas. En la práctica, la EIPD permite determinar el nivel de riesgo que entraña un tratamiento, con el objetivo de establecer las medidas de control más adecuadas para reducir el riesgo hasta un nivel considerado aceptable.

Los riesgos para los derechos y libertades de los interesados, de diversa probabilidad y gravedad, pueden producirse debido a un tratamiento de datos capaz de provocar daños físicos, materiales o inmateriales.

La aplicación del RGPD no debe entenderse como la necesaria obligación de realizar la evaluación de impacto sobre todos los tratamientos que se realizan, sino que será necesario atender a las especificidades concretas de cada tratamiento. El RGPD, en el artículo 35.3, determina los siguientes supuestos por los que se debe realizar una evaluación de impacto:

• Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se basan en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se toman decisiones que producen efectos jurídicos para las personas físicas o que les afectan significativamente.

• Tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9.1 del RGPD o de los datos personales relativos a condenas e infracciones penales del artículo 10 del RGPD.

• Observación sistemática a gran escala de una zona de acceso público.

El RGPD también señala que cuando sea probable que un tipo de tratamiento, si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entraña un alto riesgo para los derechos y libertades, el responsable debe realizar, antes del tratamiento, una evaluación de impacto. Si se trata de operaciones similares que supongan riesgos similares, se puede realizar una única evaluación.

Corresponde al responsable del tratamiento la obligación de realizar la EIPD y no al delegado de protección de datos. Según el apartado 2 del artículo 35 del RGPD: "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". Por tanto, el delegado de protección de datos proporciona el asesoramiento necesario al responsable para el adecuado desarrollo de la ejecución de una EIPD.

A la hora de realizar una EIPD, se debe disponer de una metodología que considere los requerimientos exigidos por el RGPD en su artículo 35.7, donde se establece que la EIPD deberá incluir como mínimo:

• Una descripción sistemática de la actividad de tratamiento.

• Una evaluación de la necesidad y proporcionalidad del tratamiento respecto a su finalidad.

• Una evaluación de los riesgos.

• Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales.

De por si, el RGPD no se extiende a las operaciones de tratamiento que estaban en curso en el momento en el que el reglamento comenzó a ser de aplicación. Sin embargo, sí debe realizarse una evaluación de impacto si se han producido cambios en los riesgos del tratamiento.

La EIPD debe entenderse como un proceso de mejora continua, de forma que esta se revise siempre que se modifique o actualice cualquier aspecto relevante de las actividades de tratamiento. Ante cambios en la descripción del tratamiento o en la experiencia que muestre amenazas o riesgos desconocidos hasta entonces, se debe realizar una nueva evaluación de impacto. En caso de que los cambios sobre el tratamiento no sean significativos, y no generen nuevas amenazas y riesgos sobre los derechos y libertades de los interesados, se debe realizar una valoración de los cambios producidos y documentar claramente la no necesidad de implantar nuevas medidas de control adicionales. Además, se debe llevar a cabo una revisión de la implantación de las medidas de control definidas.

Cuando el resultado de la EIPD muestre que el riesgo del tratamiento es alto o muy alto, el responsable del tratamiento debe realizar una consulta a la autoridad de control competente mediante los canales de comunicación establecidos, tal y como señala el artículo 36 del RGPD: "el responsable consultará a la autoridad de control competente 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". La consulta a la

autoridad de control y en virtud de lo que se detalla en el apartado 3 del artículo 36 del RGPD, se debe incluir la siguiente información:

• Las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento.

• Los fines y medios del tratamiento previsto.

• Las medidas y garantías establecidas para proteger los derechos y libertades de los interesados.

• Los datos de contacto del delegado de protección de datos (si lo hubiere).

• La EIPD.

• Cualquier otra información que solicite la autoridad de control.

La documentación de las tareas, análisis y evaluaciones realizadas, así como las conclusiones obtenidas, deben ser documentadas. Es importante mantener trazabilidad de las acciones realizadas y disponer de una base que justifique las conclusiones o decisiones tomadas.

2.1.16 Delegado de protección de datos

El RGPD señala que el delegado de protección de datos es una persona con conocimientos especializado en derecho y en la práctica en materia de protección de datos. Las funciones del delegado se encuentran especificadas en el artículo 39 del RGPD, siendo las siguientes:

• Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones del RPGD y demás normativas aplicables en protección de datos.

• Supervisar el cumplimiento del RGPD y demás normativas aplicables en protección de datos, y de las políticas del responsable o encargado del tratamiento en dicha materia, incluida la asignación de responsabilidades, la concienciación y la formación del personal que participa en operaciones de tratamiento, y las auditorías correspondientes.

• Ofrecer el asesoramiento que se solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación conforme al artículo 35 del RGPD.

• Cooperar con la autoridad de control competente.

• Actuar como punto de contacto de la autoridad de control competente para cuestiones relativas al tratamiento, incluida la consulta previa del artículo 36 del RGPD, y a realizar consultas, en su caso, sobre cualquier otro asunto.

El delegado de protección de datos debe desempeñar sus tareas y funciones con total independencia. Asimismo, el nivel del puesto de trabajo debe ser el adecuado para

poder relacionarse con la dirección del órgano u organismo en el que desempeñe sus funciones.

El delegado de protección de datos no es una figura de obligado cumplimiento. Sin embargo, el RGPD introduce los siguientes casos en la que su designación sí que será obligatoria:

• Autoridades y organismos públicos.

• Responsables o encargados que tengan entre sus actividades principales las operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala.

• Responsables o encargados que tengan entre sus actividades principales el tratamiento a gran escala de datos sensibles.

2.1.17 Regulación sobre el consentimiento en las *cookies*

No solo se necesita recabar el consentimiento para el tratamiento de datos personales, sino que también existen casos, como la instalación de las *cookies*, donde también es obligatorio. El apartado segundo del artículo 22 de la Ley de Servicios de la Sociedad de Información y Comercio Electrónico (art. 22 LSSI 34/2002, de 11 de julio), en adelante LSSI, establece que los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los interesados, a condición de que los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización, en particular, sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la normativa vigente de protección de datos.

El responsable debe recordar que cuando la instalación y/o utilización de una *cookie* conlleve el tratamiento de datos personales, los responsables del tratamiento deberán asegurarse del cumplimiento de las exigencias adicionales establecidas por la normativa sobre protección de datos personales, en particular en relación con los datos especialmente protegidos, además de la necesidad de adoptar cautelas adicionales en relación con los menores de edad.

Por otra parte, es necesario determinar el alcance de la normativa señalando que quedan exceptuadas del cumplimiento de las obligaciones establecidas en el artículo 22.2 de la LSSI las *cookies* utilizadas para alguna de las siguientes finalidades:

• Permitir únicamente la comunicación entre el equipo del usuario y la red.

• Prestar un servicio expresamente solicitado por el usuario.

En este sentido, las *cookies* exceptuadas según la guía sobre el uso de las *cookies* de la AEPD son aquellas que tienen por finalidad:

• *Cookies* de entrada del usuario.

• *Cookies* de autenticación o identificación de usuario, únicamente de sesión.

• *Cookies* de seguridad del usuario.

• *Cookies* de sesión de reproductor multimedia.

• *Cookies* de sesión para equilibrar la carga.

• *Cookies* de personalización de la interfaz de usuario.

• *Cookies* de complemento para intercambiar contenidos sociales.

Estas *cookies* quedan excluidas del ámbito de aplicación del artículo 22.2 de la LSSI, y por lo tanto, no sería necesario informar ni obtener el consentimiento sobre su uso. Por el contrario, es necesario informar y obtener el consentimiento para la instalación y utilización cualquier otro tipo de *cookies*, tanto de primera como de tercera parte, de sesión o persistentes, quedando sometidas al ámbito de aplicación del artículo 22.2 de la LSSI. Se debe tener en cuenta que una misma *cookie* puede tener más de una finalidad, por lo que existe la posibilidad de que mientras para una finalidad o tratamiento la *cookie* quede exceptuada del ámbito de aplicación del artículo 22.2 de la LSSI, pero no lo esté para otras finalidades, quedando sujetas al ámbito de aplicación de la Ley.

En el caso de que se empleen *cookies* de terceros para la prestación del servicio solicitado por el interesado y estas *cookies* quedan exceptuadas del ámbito de aplicación de la LSSI, se debe asegurar contractualmente que esas otras entidades o terceros no tratan los datos con ninguna otra finalidad que no sea la de prestar el servicio al interesado, puesto que, en caso contrario, sería necesario informar de esas otras finalidades y obtener el consentimiento.

Cuando se empleen *cookies* de terceros para alguna o algunas de las finalidades no exentas, tanto el editor como las otras entidades intervinientes en la gestión de las *cookies* tendrán la responsabilidad de garantizar que los usuarios están claramente informados acerca de las *cookies* y de las finalidades para las se trataran y de obtener el preceptivo consentimiento.

De esta forma, según muestra la guía sobre el uso de las cookies de la AEPD, cuando se instalen *cookies* de terceros se deben incluir en los contratos que se celebren entre los editores y los terceros, una o varias cláusulas en las que se asegure que se ofrecerá a los interesados la información requerida y que se articulará la forma a través de la cual se pueda obtener un consentimiento válido para la utilización de las *cookies*, así como sobre de las consecuencias de la revocación del consentimiento para el editor y, especialmente, para los terceros que lo obtuvieron a través del editor.

La información sobre las *cookies* facilitada en el momento de solicitar el consentimiento debe ser suficientemente completa para permitir a los usuarios entender la finalidad para las que se instalaron y conocer los usos que se les darán. En el caso de que un usuario preste su consentimiento para el uso de *cookies*, la información sobre cómo revocar el consentimiento y eliminar las *cookies* deberá de estar a su disposición de forma accesible y permanente. En todo caso, debe informarse al usuario sobre las consecuencias derivadas de la retirada de dicho

consentimiento como, por ejemplo, del impacto que puede tener en las funcionalidades de la página web.

En el anexo 10.2 se puede encontrar el sistema de capas. Es un sistema recomendado por la AEPD para mostrar toda la información exigida por la legislación de protección de datos sobre las *cookies*.

No podrá denegarse el acceso al servicio en caso de rechazo a las *cookies*, en aquellos supuestos en que tal denegación impida el ejercicio de un derecho legalmente reconocido al interesado.

Para la instalación y utilización de las *cookies* no exceptuadas será necesario en todo caso obtener el consentimiento del usuario. El consentimiento debe ser inequívoco. El consentimiento inequívoco es aquel que se ha prestado mediante una manifestación del interesado o mediante una clara acción afirmativa. El RGPD ya no admite el consentimiento tácito o de omisión, ya que se basan en la inanición. Además, debe ser explícito cuando se tratan datos especialmente protegidos y se tomen decisiones automatizadas.

La instalación de la *cookie* solo puede realizarse cuando el usuario disponga de la información preceptiva sobre las *cookies* y la forma de obtención del consentimiento y el mismo se preste a dar su consentimiento.

La guía sobre el uso de las *cookies* de la AEPD señala que debe indicarse si el consentimiento se presta sólo para la página web en la que se está solicitando o si se facilita también para otras páginas web del mismo editor o incluso para terceros asociados al editor en el marco de las finalidades de las *cookies* sobre las que se ha ofrecido información.

Un mismo editor que presta diferentes servicios a través de diferentes dominios puede a través de una sola página web informar y obtener el consentimiento para la instalación de las *cookies* que se envíen desde el resto de dominios, que sean de su titularidad y solo si ofrecen contenidos o tienen características similares siempre que se informe sobre cuáles son las páginas web o dominios de su titularidad desde los que se van a instalar las *cookies*, el tipo de *cookies* y las finalidades para la que se tratan y se recaba el consentimiento del usuario.

Siempre que un consentimiento haya sido obtenido de forma válida no es necesario obtenerlo cada vez que el interesado visite de nuevo la misma página web desde la que se presta el servicio. En todo caso, si las características o los fines de uso de las *cookies* cambian después de haber obtenido el consentimiento, será necesario informar a los interesados acerca de esos cambios y permitirles tomar una nueva decisión acerca de tales actividades.

Por último, la LSSI no define quién es el responsable de cumplir con la obligación de facilitar información sobre las *cookies* y obtener el consentimiento para su uso. Se hace necesario que las personas que participan en la instalación y utilización de las *cookies* colaboren para asegurar el cumplimiento de las exigencias legales establecidas

2.1.18 Regulación sobre la contratación de *cloud computing*

La AEPD ha desarrollado una guía para los clientes que contraten servicios de *cloud computing*. En esta guía se exponen los condicionantes que desde el punto de vista de los derechos de los ciudadanos y del ejercicio de las responsabilidades, el responsable tiene que tener en cuenta a la hora de utilizar un servicio de *cloud computing*.

Es importante identificar qué proveedores de *cloud* están localizados dentro del Espacio Económico Europeo. Esta localización afecta no sólo a la sede del proveedor de *cloud*, sino también a la localización de cada uno de los recursos físicos que emplea para implementar el servicio, de forma directa o subcontratada. Hay que tener en cuenta la localización de todos los recursos pues, por la misma naturaleza del servicio de *cloud*, los datos pueden estar en cualquier momento en cualquier sitio, pero los derechos y obligaciones relativos a dichos datos han de garantizarse siempre.

La contratación de servicios de *cloud computing* se realizará a través de un contrato de prestación de servicios. Resulta imprescindible que ese contrato incorpore entre sus cláusulas las garantías a las que obliga el RGPD.

El responsable debe decidir para qué datos personales contrata servicios de *cloud computing* y cuáles prefiere mantener en sus propios sistemas de información. Esta decisión es importante porque delimita las finalidades para las que el proveedor de *cloud* puede tratar los datos. En consecuencia, debe garantizarse expresamente que no utilizará los datos para otra finalidad que no tenga relación con los servicios contratados. La transferencia de datos a servicios de computación no excluye en principio a ningún tipo de dato.

El cliente que contrata servicios de *cloud computing* sigue siendo responsable del tratamiento de los datos personales. La responsabilidad no se desplaza al prestador del servicio, ni siquiera incorporando una cláusula en el contrato con esta finalidad. El que ofrece la contratación de *cloud computing* es un prestador de servicios que en el RGPD tiene la calificación de encargado del tratamiento.

El responsable debe solicitar y obtener información sobre si intervienen o no terceras empresas en la prestación de servicios de *cloud computing*. De ser así:

• Tiene que dar su conformidad a la participación de terceras empresas, al menos delimitando genéricamente los servicios en los que participarán. Para ello, el prestador del servicio de *cloud computing* tiene que informar sobre la tipología de servicios que pueden subcontratarse con terceros.

• Tiene que poder conocer las terceras empresas que intervienen.

• El proveedor de *cloud* debe asumir en el contrato que los subcontratistas le ofrecen garantías jurídicas para el tratamiento de los datos equivalentes a los que él mismo asume.

El contrato que firma el responsable ha de incorporar las cláusulas contractuales que se exponen en la guía para los clientes que contraten servicios de *cloud computing* de la AEPD, para garantizar la protección de los datos personales. A continuación, se muestran las cláusulas que debe de incorporar el contrato:

• El responsable debe de preguntar al prestador de servicios de *cloud computing* de si existen transferencias internacionales de datos y, en caso afirmativo, con qué garantías. Cuando los datos están localizados en terceros países podría suceder que una autoridad competente pueda solicitar y obtener información sobre los datos personales de los que el cliente es responsable. En este caso el cliente debería ser informado por el proveedor de esta circunstancia, salvo que lo prohíba la ley del país tercero.

• Las medidas de seguridad exigibles. Asimismo, el acceso a la información a través de redes de comunicaciones debe contemplar un nivel de medidas de seguridad equivalente al de los accesos en modo local.

• El responsable, como cliente, debe ser informado diligentemente por el proveedor de *cloud* sobre las incidencias de seguridad que afecten a los datos de los que el propio cliente es responsable, así como de las medidas adoptadas para resolverlas o de las medidas que el cliente ha de tomar para evitar los daños que puedan producirse.

• El responsable debe exigir, que el proveedor del servicio de *cloud* deba comprometerse a garantizar la confidencialidad utilizando los datos sólo para los servicios contratados. Asimismo, el proveedor del servicio *cloud* debe comprometerse a dar instrucciones al personal que depende de él para que mantenga la confidencialidad.

• El responsable debe tener la opción de exigir la portabilidad de la información a sus propios sistemas de información o a un nuevo prestador de *cloud* cuando considere inadecuada la intervención de algún subcontratista o la transferencia de datos a países que estime que no aportan garantías adecuadas en un formato que permita su utilización, en el plazo más breve posible, con total garantía de la integridad de la información y sin incurrir en costes adicionales. Para asegurarse que el proveedor *cloud* no conserva datos una vez el contrato a extinguido, deben preverse mecanismos que garanticen el borrado seguro de los datos cuando lo solicite el cliente y, en todo caso, al finalizar el contrato.

• Por otra parte, para garantizar los derechos de los propietarios de los datos personales que se van a tratar, el cliente de *cloud computing*, como responsable del tratamiento de datos, debe permitir el ejercicio de los derechos de los interesados. Para ello, el proveedor de *cloud* debe garantizar su cooperación y las herramientas adecuadas para facilitar la atención de dichos derechos.

2.1.19 Regulación sobre la reutilización de la información del sector público.

La reutilización de la información del sector público puede implicar el tratamiento de información personal que fue recabada para finalidades que pueden ser distintas a las propias de la entidad reutilizadora. En este aspecto, la AEPD ha desarrollado un documento con orientaciones sobre la protección de datos en la reutilización de la información del sector público.

En España el acceso a la información pública se encuentra regulado por la Ley 19/2013 de Transparencia, Acceso a la Información pública y Buen Gobierno (LTAIBG 19/2013, de 9 de diciembre), en adelante, LTAIBG.

La Ley contempla dos modalidades para la obtención de la información, la publicidad activa y el ejercicio individual del derecho de acceso a la misma.

La LTAIBG establece en su artículo 5.3, en relación con la publicidad activa, que serán de aplicación los límites al derecho de acceso a la información pública previstos en el artículo 14 y, especialmente, el derivado de la protección de datos de carácter personal, regulado en el artículo 15. Añadiendo a su vez que cuando la información contuviera datos especialmente protegidos, la publicidad sólo se llevará a cabo previa disociación de estos.

Dentro del capítulo sobre el derecho de acceso a la información pública, el artículo 15 de la Ley establece los requisitos para el acceso a los datos especialmente protegidos y los criterios de ponderación entre el derecho de acceso a la información pública y el derecho fundamental a la protección de datos personales, excluyendo su aplicación si los datos están previamente disociados y remarcando que la normativa de protección de datos personales es de aplicación al tratamiento posterior de la información a la que se haya accedido.

Una solución para conseguir la disociación de los datos es la seudonimización. Al utilizar la seudonimización se tiene como consecuencia que los datos personales dejan de considerarse datos de personas identificadas o identificables, de lo que se deriva que los tratamientos quedan excluidos del ámbito de aplicación del RGPD. No obstante, el RGPD exigen un elevado umbral de seudonimización, de forma que la disociación de los datos identificativos de los interesados resulte irreversible.

La seudonimización debe contemplarse desde una perspectiva dinámica que ha de atender a la evolución de los medios tecnológicos que puedan posibilitar la reidentificación. Por tanto, si se acude a la opción de la seudonimización, aunque no sea necesario aplicar la metodología de la EIPD, adecuada cuando la reutilización implique el tratamiento de datos personales, será preciso llevar a cabo un proceso de análisis de riesgos centrado en analizar las posibilidades de revertir la disociación.

2.1 Crítica al estado del arte

El RGPD entra en vigor el año en el que se está desarrollando este trabajo, en el 2018. A consecuencia de esto, la cantidad de Trabajos de Fin de Grado que tratan este tema es pequeña, prácticamente nula, siendo una nueva temática por explorar y analizar.

Por otra parte, la regulación sobre la protección de datos no se encuentra en un solo documento, es extensa y está dispersa entre el RGPD, la LOPD de 1999 y otros documentos que tratan aspectos específicos de la protección de datos. Además, para entender los requerimientos de las normativas, se requieren conocimientos especializados en derecho y en la práctica en materia de protección de datos.

2.2 Propuesta

Este trabajo pretende centrarse en los requisitos, tanto legales como técnicos, que los responsables y encargados de tratamientos de datos personales deben tener en cuenta desde la entrada en vigor del RGPD. Reúne todas las normativas relacionadas con la protección de datos que han sido aprobadas y que en el momento en el que se está desarrollando el trabajo, están en vigor. Entre estas normativas se encuentra el ya citado RGPD, impulsado por la Unión Europea, reglamentos que tratan aspectos específicos del RGPD como son la regulación del consentimiento de las *cookies*, la regulación de la contratación de los servicios *cloud computing*, la regulación sobre la reutilización de la información del sector público, la regulación sobre las evaluaciones de impacto, la regulación sobre los análisis de riesgos, regulación sobre medidas de seguridad, regulación sobre la protección de datos en Administraciones Públicas y regulación sobre los datos especialmente protegidos. Además, hay que tener en cuenta la antigua LOPD de 1999, ya que no todas las disposiciones de la Ley Orgánica han sido derogadas, algunas de ellas han sido modificadas o sustituidas y otras aún siguen en vigor, ya que el RGPD, otorga a los Estados miembros la libertad de actuar sobre disposiciones específicas, como la disposición sobre el tratamiento de personas fallecidas o la disposición sobre el consentimiento de los menores de edad.

Hay que tener en cuenta, que este trabajo no trata de abarcar los restantes puntos de vista a los que afecta la normativa de protección de datos, como pueden ser las personas físicas cuyos datos son tratados o las autoridades de control competentes encargadas de vigilar y auditar que el RGPD se cumple en todas las organizaciones que realizan actividades de tratamiento de datos.

3. Análisis del problema

Tras el análisis del catálogo de medidas que establece el RGPD, las disposiciones de la LOPD de 1999 que no han sido derogadas y las demás normativas relacionadas con la protección de datos, el siguiente paso es proceder a la realización de un estudio técnico. Este estudio tiene como objetivo establecer y clasificar las obligaciones que deben tener en cuenta los responsables y los encargados.

Al igual que en la sección “2. Estado del arte”, las obligaciones se expondrán mediante puntos sucesivos.

3.1 Requisitos técnicos sobre los tratamientos de datos

Como ya se ha dicho anteriormente, sobre el responsable recaen las principales obligaciones establecidas por el RGPD y es a él a quien le corresponde velar por el cumplimiento del reglamento en su organización. Las obligaciones que debe tener en cuenta un responsable son las que se muestran a continuación:

• Documentar e identificar la base legal sobre la que se desarrollan los tratamientos.

• Regular y formalizar la relación con el encargado de tratamiento.

• Garantizar y demostrar que el encargado realiza el tratamiento según el RGPD.

• Proporcionar información sobre las condiciones de los tratamientos y sobre como ejercer los derechos a los interesados de una forma concisa, transparente, inteligible y de fácil acceso con un lenguaje claro y sencillo.

• Obtener el consentimiento inequívoco para el tratamiento de los datos personales.

• Proponer e impulsar medidas para demostrar que los menores de 14 años han dado su consentimiento con la autorización de padres o tutores.

• Tener mecanismos para cancelar los datos de personas fallecidas una vez se ha informado de su óbito.

• Informar y obtener el consentimiento inequívoco y explícito en caso de tratamiento de datos especialmente protegidos.

• Asegurarse de que los datos sean adecuados y veraces, obtenidos lícita y legítimamente y tratados de un modo proporcional a la finalidad para la que fueron recabados.

• Facilitar y garantizar el ejercicio de los derechos interesados.

• Asegurar que en las relaciones con terceros que comporten el acceso a datos personales se cumpla lo dispuesto en el RGPD.

• Asegurar que si se realizan transferencias internacionales se cumplan las condiciones en lo dispuesto en el RGPD.

• Realizar un análisis de riesgo.

• Mantener registros relativos a todas las categorías de actividades de tratamiento.

• Aplicar medidas para garantizar la protección de datos desde el diseño y por defecto.

• Desarrollar y aplicar las medidas de seguridad necesarias para cada tratamiento.

• Establecer protocolos para la notificación de violaciones de seguridad.

• Realizar una evaluación de impacto sobre la protección de datos.

• Garantizar que el delegado de protección de datos, en el caso de que lo hubiere, cumple las funciones que el RGPD exige.

• Garantizar el cumplimiento de los deberes de secreto profesional y confidencialidad.

Todas estas obligaciones se irán analizando en los siguientes puntos, pudiendo extraer de ellas los requisitos técnicos que un responsable y un encargado deben tener en cuenta en su día a día.

3.1.1 Base legal del tratamiento

Por lo que respecta a las obligaciones del responsable en esta sección, el RGPD mantiene el principio recogido en la Directiva 95/46 de que todo tratamiento de datos necesita apoyarse en una base que lo legitime. En ese sentido, el RGPD no implica cambios en las obligaciones para los responsables, manteniéndose la obligación de identificar y documentar la base legal en que se apoya.

Sin embargo, aunque no está expuesto de forma explícita, se deduce del principio general de responsabilidad activa, las siguientes obligaciones que también debe tener en cuenta:

• Se debe incluir la base legal sobre la que se desarrolla el tratamiento al proporcionar la información en el momento de recoger los datos de los interesados.

• Se debe especificar y documentar los intereses legítimos en que se fundamentan las operaciones de tratamiento en casos como las evaluaciones de impacto sobre la protección de datos o en determinadas transferencias internacionales.

La identificación de la base legal es indispensable para estar en condiciones de demostrar que se cumple con las previsiones del RGPD. La identificación y documentación debe adaptarse al tipo de tratamiento y a las características de las organizaciones.

3.1.2 Contratación de un encargado de tratamiento

Como se ha mencionado en la sección 2.1.2 las relaciones entre un responsable y un encargado deben formalizarse en un contrato o en un acto jurídico que vincule al encargado respecto al responsable. Por lo que el responsable tiene la obligación de formalizar la relación si aún no se ha formalizado.

El responsable debe tener en cuenta el contenido mínimo de los contratos de encargo mencionado en la sección 2.1.2 y debe incluir aspectos como los que se muestran a continuación:

• Objeto, duración, naturaleza y la finalidad del tratamiento.

• Tipo de datos personales y categorías de interesados.

• Obligación del encargado de tratar los datos personales únicamente siguiendo instrucciones documentadas del responsable.

• Condiciones para que el responsable pueda dar su autorización previa, específica o general, a las subcontrataciones.

• Asistencia al responsable, siempre que sea posible, en la atención al ejercicio de derechos de los interesados.

• El deber de confidencialidad.

• Las medidas de seguridad que debe de adoptar el encargado para garantizar el cumplimiento con el RGPD.

• El destino de los datos al finalizar la prestación del servicio.

Ambos, encargado y responsable del tratamiento, pueden ser sancionados de acuerdo con el RGPD si incumplen sus obligaciones, aunque la responsabilidad última sobre el tratamiento sigue estando atribuida al responsable, que es quien determina la existencia del tratamiento y su finalidad.

En determinadas materias, los encargados tienen obligaciones propias que establece el RGPD, que no se circunscriben al ámbito del contrato que los une al responsable, y que pueden ser supervisadas separadamente por las autoridades de protección de datos. Estas obligaciones incluyen:

• Mantener un registro de actividades de tratamiento.

• Determinar las medidas de seguridad aplicables a los tratamientos que realizan.

• Designar a un delegado de protección de datos en los casos previstos por el RGPD.

3.1.3 Relación responsable – encargado

El reglamento de desarrollo de la LOPD de 1999 establecía la necesidad de diligencia en la selección de encargados. Según el RGPD, el responsable tiene la obligación de adoptar medidas apropiadas, incluida la elección de encargados, de forma que garantice y esté en condiciones de demostrar que el tratamiento se realiza conforme el RGPD.

Los responsables habrán de elegir únicamente encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del reglamento. Esta previsión se extiende también a los encargados cuando subcontraten operaciones de tratamiento con otros subencargados.

3.1.4 Notificación de ficheros

Tal y como se ha explicado en la sección 2.1.3, con el RGPD desaparece la obligación de notificar la inscripción de ficheros, tanto de responsables públicos o privados, en el registro de ficheros de la AEPD, o en el registro de la autoridad autonómica competente. No obstante, el RGPD incluye la nueva obligación de implementar un registro de actividades de tratamiento. El registro de actividades de tratamiento se analizará en un punto separado a este.

3.1.5 Transparencia e información a los interesados

Los responsables tienen la obligación de proporcionar la información relativa a las condiciones de los tratamientos y a los derechos a los interesados, tal y como se ha indicado en la sección 2.1.4, de una forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo. La LOPD de 1999 sólo exigía que la información se prestase de un modo expreso, preciso e inequívoco.

Otra obligación que tienen los responsables es la de informar al interesado cuando se recogen datos personales que les afectan. Este derecho de información es esencial porque garantiza que el consentimiento que se preste sea previo, específico e informado y es necesario para permitir el ejercicio de los derechos.

El artículo 5 de la LOPD de 1999 recoge la obligación que tienen los responsables de informar a los interesados sobre los puntos que ya han sido mencionados en la sección 2.1.4 y que se componen de los siguientes: la incorporación de los datos a un fichero, la identidad y dirección del responsable, la finalidad del fichero, los destinatarios de la información, el carácter obligatorio o facultativo de su respuesta a las preguntas que le sean planteadas al responsable, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos, así como de la posibilidad de ejercitar los derechos propios de los interesados.

El RGPD en este aspecto, añade las siguientes obligaciones:

• Se deberán evitar las fórmulas especialmente farragosas y que incorporan remisiones a los textos legales.

• Las cláusulas informativas deberán explicar el contenido al que inmediatamente se refieren de forma clara y accesible para los interesados, con independencia de sus conocimientos en la materia.

• Tal y como se comentó en la sección 2.1.4 se añaden nuevos datos a la lista de información que debe proporcionarse a los interesados y que consta de los siguientes puntos:

◦ Base jurídica del tratamiento.

◦ Intención de realizar transferencias internacionales.

◦ Datos del delegado de protección de datos (si lo hubiere).

◦ Elaboración de perfiles.

◦ El plazo o criterios de conservación de la información.

◦ El derecho a presentar una reclamación ante las autoridades de control competentes.

• La información a los interesados deberá facilitarse por escrito, incluidos los medios electrónicos cuando sea apropiado.

Esta información debe estar incluida en los cuestionarios o impresos de recogida de los datos. En el caso de utilizar internet como medio de recogida de los datos, existe la obligación de facilitar esta información a los usuarios que registran sus datos y debe de hacerse de modo que la información sea siempre previa al tratamiento.

En el caso de los menores de edad se exige que la información se exprese en un lenguaje que sea fácilmente comprensible.

Cuando los datos se recojan directamente de los interesados, la información debe facilitarse con carácter previo a la recogida de los datos personales.

3.1.6 Prestación del consentimiento

En los casos en que la base jurídica del tratamiento sea el consentimiento, el responsable tiene la obligación de garantizar que cumple con las características previstas por el RGPD. Se exige que el consentimiento sea informado, libre, específico y otorgado por los interesados mediante una manifestación que muestre su voluntad de consentir o mediante una clara acción afirmativa.

Según lo mostrado en la sección 2.1.5, el responsable tiene la obligación de garantizar que el consentimiento obtenido es inequívoco. A diferencia del reglamento de desarrollo de la LOPD, no se admiten formas de consentimiento tácito o por omisión,

ya que se basan en la inacción. En la sección 2.1.5 también se explican las situaciones en las que el responsable debe garantizar que el consentimiento obtenido, aparte de ser inequívoco debe ser explícito. Estas situaciones se dan en el tratamiento de datos sensibles, en la adopción de decisiones automatizadas y en las transferencias internacionales.

Los tratamientos iniciados con anterioridad al inicio de la aplicación del RGPD sobre la base del consentimiento, pueden seguir siendo legítimos siempre que ese consentimiento se hubiera prestado del modo en que prevé el propio RGPD, es decir, mediante una manifestación o acción afirmativa.

En el anexo 10.5, se muestran ejemplos sobre cómo recabar el consentimiento de forma correcta.

3.1.7 Tratamiento de datos de menores de edad

El RGPD se refiere en varios lugares a los tratamientos de los datos de los menores de edad:

• En la regulación de los intereses legítimos del responsable como base legal para el tratamiento, señalándose que no será aplicable cuando prevalezcan los derechos, libertades o intereses de los interesados que requieran protección de datos personales, especialmente cuando esos interesados sean niños.

• Al señalar que la información que se ofrece a los interesados en relación con el tratamiento o con el ejercicio de derechos deberá ser especialmente concisa, transparente, inteligible y proporcionada con lenguaje claro y sencillo cuando los interesados sean niños.

• En el contexto del derecho al borrado de los datos personales.

• Al establecer que las actividades de formación y sensibilización dirigidas a los niños deberán estar entre las prioridades de las autoridades de protección de datos.

• En el contexto de las explicaciones que ofrecen los considerandos del RGPD cuando se refieren a la realización de perfiles.

La mención más explícita a los menores, es decir, niños en la terminología del RGPD, está relacionada con la obtención del consentimiento en el ámbito de la oferta directa de servicios de la sociedad de la información. El reglamento prevé que, en ese entorno, el consentimiento solo será válido a partir de los 16 años, debiendo contar con la autorización de los padres o tutores legales por debajo de esa edad.

Sin embargo, en la sección 2.1.5 se menciona que el RGPD permite a los Estados miembros establecer una edad inferior para la prestación del consentimiento, siempre que no sea menor de 13 años ni mayor de 16. Como ya se ha mencionado en esa misma sección, en el caso de España la edad mínima se sitúa en los 14 años con carácter general, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. La normativa aplicable en este

aspecto es el reglamento de desarrollo de la LOPD de 1999. Para los menores de 14, el responsable tiene la obligación de requerir el consentimiento de los padres o tutores.

Según el RGPD, el responsable debe hacer esfuerzos razonables, teniendo en cuenta la tecnología disponible, para verificar que, para los niños menores de 14 años, el consentimiento se ha dado o se ha autorizado por los padres o tutores del menor.

3.1.8 Regulación de datos sobre personas fallecidas

En la sección 2.1.6, se explica la normativa aplicable en los casos de tratamientos de datos de personas fallecidas. En esta sección, se llega a la conclusión de que, en España, la normativa aplicable es el reglamento de desarrollo de la LOPD de 1999. En este reglamento se establece que desde el momento en el que el responsable es informado del fallecimiento de una persona cuyos datos estaban siendo tratados, tiene la obligación de proceder a la cancelación de estos datos.

3.1.9 Datos especialmente protegidos

En el caso de tratamientos de datos especialmente protegidos, el responsable tiene la obligación de advertir al interesado de su derecho a no prestar su consentimiento para el tratamiento de estos datos. El responsable necesita el consentimiento expreso y por escrito del interesado o que lo disponga una ley para recabar, tratar o ceder datos especialmente protegidos.

No se permite crear ficheros con la única finalidad de almacenar datos especialmente protegidos, a no ser, que se ampare en alguna de las excepciones definidas en la sección 2.1.7.

3.1.10 Calidad y proporcionalidad

En la sección 2.1 se mencionan los principios incluidos en el artículo 5 del RGPD. Estos principios se basan en garantizar y respetar la calidad y proporcionalidad de los datos. Por lo que respecta al responsable en este aspecto, se le atribuyen las siguientes obligaciones:

• Debe garantizar que los datos son tratados de manera lícita, leal y transparente.

• Debe garantizar que los datos son recogidos con fines determinados, explícitos y legítimos.

• Debe garantizar que los datos son adecuados, pertinentes y no excesivos en relación con la finalidad del tratamiento.

• Debe garantizar que los datos son exactos y responden con veracidad a la situación del interesado.

• Debe garantizar que los datos sólo se conservan durante el tiempo necesario para las finalidades del tratamiento para las que han sido recogidos.

• Debe aplicar medidas que garanticen la adecuada seguridad de los datos.

• Debe demostrar que cumple con todas estas obligaciones.

3.1.11 Derechos de los interesados

Los responsables deben facilitar a los interesados el ejercicio de sus derechos. En la sección 2.1.8 se describen las características de los procedimientos y de las formas. Además, los responsables deben posibilitar la presentación de solicitudes por medios electrónicos, especialmente cuando el tratamiento se realiza por estos medios.

El ejercicio de los derechos debe ser gratuito para el interesado, excepto en los casos en que se formulen solicitudes manifiestamente infundadas o excesivas, especialmente por repetitivas. El responsable puede cobrar un canon que compense los costes administrativos de atender a la petición o negarse a actuar. El canon no puede implicar un ingreso adicional para el responsable, sino que debe corresponderse con el verdadero coste de la tramitación de la solicitud.

La sección 2.1.8 muestra la lista de derechos de los interesados definida en la LOPD de 1999 tras la aplicación del RGPD. A continuación, se muestran los plazos que el responsable debe tener en cuenta a la hora de estimar una solicitud para aplicar un derecho y los plazos para procesar esa solicitud, en caso de aprobación. También se muestran las características técnicas que tiene cada derecho:

• El derecho de acceso: su plazo de estimación es de un mes desde la recepción de la solicitud. El acceso debe concederse en el plazo de 10 días una vez que la solicitud ha sido estimada.

El derecho de acceso puede ejercitarse a intervalos de 12 meses sin necesidad de que el titular de los datos personales alegue alguna justificación. Puede ejercerse en periodos inferiores cuando se tenga un interés legítimo. Para que se considere que se ha respetado este derecho, basta con que el interesado esté en posesión de un resumen completo de los datos presentados de forma inteligible, es decir, de forma que el interesado pueda tener conocimiento de estos y verificar que son exactos y que su tratamiento se ha realizado conforme lo impuesto por el RGPD. Si el interesado se encuentra disconforme, puede ejercer los derechos que el reglamento le confiere.

La información que facilite el responsable o el encargado debe comprender los datos de base del interesado y los resultantes de cualquier elaboración o proceso informático, así como el origen de los datos, los cesionarios de estos y la especificación de los concretos usos y finalidades para los que se almacenaron.

• El derecho de rectificación: su plazo de estimación es de un mes desde la recepción de la solicitud. La rectificación debe realizarse en el plazo de 10 días a partir del momento en el que se procesa la solicitud.

El derecho de rectificación exige al solicitante indicar el dato que es erróneo y la corrección que debe realizarse. Debe ir acompañada de la documentación justificativa de la rectificación solicitada, salvo que esta dependa exclusivamente del consentimiento del solicitante.

• El derecho de cancelación: su plazo de estimación es de un mes desde la recepción de la solicitud. La cancelación debe realizarse en el plazo de 10 días a partir del momento en el que se procesa la solicitud.

El derecho de cancelación requiere indicar si se revoca el consentimiento otorgado, en los casos en que la revocación proceda, o si se trata de un dato erróneo o inexacto, en cuyo caso deberá ir acompañada de la documentación justificativa. La cancelación dará lugar al bloqueo de los datos, excepto cuando sea preciso conservar éstos datos para la disposición de las Administraciones Públicas, Jueces y Tribunales. Una vez se ha cumplido con las Administraciones Públicas, Jueces y Tribunales, deberá procederse a la supresión.

• El derecho de oposición: su plazo de estimación es de un mes desde la recepción de la solicitud. Se deben de dejar de tratar los datos en el plazo de 10 días a partir del momento en el que se procesa la solicitud.

El derecho de oposición supone que el titular debe exponer los motivos fundados y legítimos relativos a una concreta situación personal, para que los datos dejen de ser tratados.

• El derecho al olvido: A este derecho se le aplican los mismos plazos que a los derechos de cancelación u oposición, es decir, un mes para la estimación y 10 días para la realizar la solicitud.

• El derecho de limitación del tratamiento: a este derecho se le aplican los mismos plazos y procedimientos que a los restantes derechos previstos en el RGPD. En el tiempo que dure la limitación, el responsable sólo podrá tratar los datos limitados, más allá de su conservación en los siguientes puntos:

◦ Con el consentimiento del interesado.

◦ Para la formulación, el ejercicio o la defensa de reclamaciones.

◦ Para proteger los derechos de otra persona física o jurídica.

◦ Por razones de interés público importante de la Unión Europea o del Estado miembro correspondiente.

Como consecuencia de la existencia de este derecho, se impide la práctica habitual que consiste en borrar los datos cuando se ejercitan otros derechos, ya que impide el ejercicio del derecho a la limitación del tratamiento.

• El derecho a la portabilidad: a este derecho se le aplican los mismos plazos que a los restantes derechos previstos en el RGPD. Implica que los datos personales del interesado se transmiten directamente de un responsable a otro, sin necesidad de que sean transmitidos previamente al propio interesado, siempre que ello sea técnicamente posible. No es aplicable:

◦ En caso de que el interesado haya solicitado la portabilidad de datos que le incumban pero que hayan sido proporcionados al responsable por terceros.

Existe la obligación de contestar al solicitante, aunque no figuren datos suyos y se debe de hacer por medios que permitan acreditar el envío y la recepción de la notificación.

Los derechos de los interesados no son absolutos. El responsable puede denegarlos cuando concurra en una causa legal. En caso de denegación, el responsable del fichero debe informar al interesado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las Comunidades Autónomas.

Toda denegación o restricción de acceso debe comunicarse por escrito al interesado precisando los fundamentos de hecho o de Derecho en los que se basa la decisión.

Si los datos a rectificar, cancelar o limitar hubieran sido cedidos previamente a un tercero, el responsable debe notificar al cesionario la rectificación, cancelación o limitación efectuada.

En el caso de los datos obtenidos de fuentes accesibles al público el titular de los datos tiene derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que le conciernan, en cuyo caso el responsable debe darlos de baja del tratamiento y cancelar las informaciones que sobre el titular figuren.

3.1.12 Cesión de datos a terceros

En la sección 2.1.9 se expone que, para comunicar datos a un tercero, es necesario el consentimiento previo del interesado. Es el responsable quien tiene la obligación de obtener este consentimiento y, además, debe obtenerlo siguiendo las características que marca el RGPD.

El responsable debe informar al interesado en el momento en que se efectúe la primera cesión indicando: la finalidad del tratamiento, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario. No será necesario informar cuando la cesión cumpla algunas de las excepciones definidas en la sección 2.1.9.

3.1.13 Transferencias internacionales

Como se menciona en la sección 2.1.10, se debe obtener la autorización previa del director de la AEPD cuando se tenga previsto realizar transferencias internacionales de datos a países que no proporcionan un nivel de protección adecuado y la transferencia no se ampare en alguno de los supuestos previstos el artículo 49 del RGPD. La transferencia la puede realizar tanto el responsable como el encargado. Para obtener la autorización del director de la AEPD, es obligatorio que la persona que vaya a realizar la transferencia internacional demuestre que se han obtenido las garantías adecuadas, como pueden ser, los contratos basados en las cláusulas tipo aprobadas por la Comisión Europea, o las reglas corporativas vinculantes de intragrupos empresariales.

Es necesario que el responsable o en su caso, el encargado, realizase una solicitud para comunicarse con el director de la AEPD. Esta solicitud deberá contener los siguientes datos: la finalidad, los colectivos de interesados, los datos objeto de transferencia y la documentación que incorpore las garantías exigibles para la obtención de la autorización, en la que conste una descripción de las medidas de seguridad concretas que van a ser adoptadas, tanto por el exportador como por el importador de los datos.

Cuando la transferencia internacional se ampare en alguna de las excepciones definidas en el artículo 49, tal y como se ha expuesto en la sección 2.1.10, el responsable o en su caso, el encargado, tiene la obligación de informar tanto a la AEPD como a los interesados.

3.1.14 Análisis de riesgo

Todos los responsables tienen la obligación de realizar una valoración del riesgo sobre los tratamientos que lleven a cabo, a fin de poder establecer qué medidas deben aplicar y cómo deben hacerlo.

Como se ha explicado en la sección 2.1.11, el análisis de riesgo debe tener en cuenta los siguientes puntos:

• Los tipos de tratamiento.

• La naturaleza de los datos.

• El número de interesados.

• La cantidad y variedad de tratamientos que realiza la organización.

En las grandes organizaciones, el análisis de riesgo deberá llevarse a cabo utilizando alguna de las metodologías de análisis de riesgo ya existentes. Para las organizaciones de menor tamaño y con tratamientos de poca complejidad, el análisis

será el resultado de una reflexión, mínimamente documentada, sobre las implicaciones de los tratamientos en los derechos y libertades de los interesados.

Según el artículo 29 de la directiva 2016/680 (Dir. 2016/680 del Consejo, de 27 de abril), si en la organización se llevan a cabo tratamientos de datos automatizado, el responsable o encargado del tratamiento, a raíz de una evaluación de los riesgos, tiene la obligación de definir y aplicar medidas destinadas a:

• El control de acceso a los equipamientos: se debe denegar el acceso a personas no autorizadas a los equipamientos utilizados para el tratamiento.

• El control de los soportes de datos: se debe impedir que los soportes de datos puedan ser leídos, copiados, modificados o cancelados por personas no autorizadas.

• El control del almacenamiento: se debe impedir que se introduzcan sin autorización datos personales conservados, o que estos puedan inspeccionarse, modificarse o suprimirse sin autorización.

• El control de los usuarios: se debe impedir que los sistemas de tratamiento automatizados puedan ser utilizados por personas no autorizadas por medio de instalaciones de transmisión de datos.

• El control del acceso a los datos: se debe garantizar que las personas autorizadas a utilizar un sistema de tratamiento automatizado solo puedan tener acceso a los datos personales para los que han sido autorizados.

• El control de la transmisión: se debe garantizar que sea posible verificar y establecer a qué organismos se han transmitido o pueden transmitirse los datos personales mediante equipamientos de comunicación de datos.

• El control de la introducción: se debe garantizar que pueda verificarse y constatarse a posteriori qué datos personales se han introducido en los sistemas de tratamiento automatizado y en qué momento y por qué persona han sido introducidos.

• El control del transporte: se debe impedir que durante las transferencias de datos personales o durante el transporte de soportes de datos, los datos personales puedan ser leídos, copiados, modificados o suprimidos sin autorización.

• El restablecimiento: se debe garantizar que los sistemas instalados puedan restablecerse en caso de interrupción.

• La fiabilidad y la integridad: se debe garantizar que las funciones del sistema no presenten defectos, que los errores de funcionamiento sean señalados y que los datos personales almacenados no se degraden por fallos de funcionamiento del sistema.

3.1.15 Registro de actividades de tratamiento

En la sección 3.1.4 se adelantaba que con el RGPD ya no es necesario notificar los ficheros en la AEPD, pero en su lugar, se debe llevar un registro de todas las actividades de tratamiento que lleva a cabo el responsable o el encargado. Los responsables y los encargados están obligados a cooperar con la autoridad de control competente y, por lo tanto, a poner los registros a su disposición, cuando los solicite, de modo que puedan servir para supervisar las operaciones de tratamiento.

Los responsables o los encargados del tratamiento que traten datos personales mediante sistemas de tratamiento no automatizado deben contar con métodos eficaces, como los registros diarios o de otro tipo, para demostrar la licitud del tratamiento, permitir el autocontrol y garantizar la integridad y la seguridad de los datos, con el fin de cumplir el principio de responsabilidad proactiva.

Los responsables y los encargados tienen la obligación de supervisar que los registros de actividades de tratamiento contenga los siguientes puntos, que ya fueron definieros en la sección 2.1.3:

• Nombre y datos de contactos del responsable.

• Fines del tratamiento.

• Nombre y datos de contacto del delegado de protección de datos (si lo hubiere).

• Categorías de datos personales.

• Categorías de los interesados.

• Descripción de las medidas técnicas y organizativas de seguridad.

• Categorías de destinatarios de comunicaciones, incluidos terceros países u organizaciones internacionales.

• En el caso de haber transferencias internacionales como las indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas.

• Cuando sea posible, plazos previstos para la supresión de las diferentes categorías de datos.

Las organizaciones que empleen a menos de 250 trabajadores están exentas de realizar un registro de actividades de tratamiento, a menos que el tratamiento que realicen pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional o incluya categorías especiales de datos o datos relativos a condenas e infracciones penales.

Deben conservarse registros, como mínimo, de las operaciones llevadas a cabo mediante sistemas de tratamiento automatizado, entre las que se incluyen: la recopilación, la modificación, la consulta, la comunicación, la transmisión, la combinación o la supresión de datos. Los datos identificativos de la persona que consulta o comunica los datos personales deben quedar registrados y, a partir de

dichos datos, el responsable o el encargado, debe de garantizar la posibilidad de establecer la justificación de las operaciones de tratamiento.

Los registros se deben utilizar únicamente para comprobar la licitud del tratamiento de datos, a efectos de autocontrol y para garantizar la integridad y la seguridad de los datos y los procesos penales.

3.1.16 Protección de datos desde el diseño y por defecto

Se ha mencionado en la sección 2.1.12 el principio de protección de datos desde el diseño. Este principio conlleva que, desde el inicio, los responsables deben tomar medidas organizativas y técnicas para integrar en los tratamientos garantías que permitan aplicar de forma efectiva los principios del RGPD. Un ejemplo de dichas medidas, que se establece de forma expresa en el propio reglamento, es que el tratamiento incorpore medidas para la seudonimización de los datos personales o la minimización de datos.

En esa misma sección, también se menciona el principio de protección de datos por defecto. Este principio significa que independientemente del conjunto de datos recogidos por el responsable con el objeto de implementar los distintos servicios que se proporcionan al interesado, el responsable ha de compartimentar el uso del conjunto de datos entre los distintos tratamientos de tal forma que no todos los tratamientos accedan a todos los datos, sino que actúen solo sobre aquellos que sean necesarios y en los momentos en que sea estrictamente necesario. A este aspecto hay que añadir, como se cita en la sección 2.1.12, que si fuera posible por la naturaleza del proceso, llegar incluso a que no se traten datos de carácter personal.

Los responsables deben adoptar medidas que garanticen que solo se traten los datos necesarios en lo relativo a la cantidad de datos tratados, la extensión del tratamiento, los periodos de conservación y la accesibilidad a los datos.

Estas obligaciones se incluyen dentro de las que debe aplicar el responsable con anterioridad al inicio del tratamiento y también cuando se esté desarrollando.

3.1.17 Medidas de seguridad

Con el objetivo de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el RGPD, el responsable y el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos.

Según el artículo 32 del RGPD y el artículo 9 de la LOPD, tanto el responsable como el encargado deben tener en cuenta los siguientes puntos:

• La aplicación de las medidas de seguridad deben garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los datos y sistemas.

• Las medidas de seguridad se aplican tanto a los ficheros como a los tratamientos.

• Las medidas de seguridad deben aplicarlas el responsable y el encargado del tratamiento.

• Deben aplicarse medidas de seguridad a ficheros y tratamientos en soportes no automatizados.

• Las medidas deben ir orientadas a garantizar la seudonimización y el cifrado de datos personales.

• Las medidas de seguridad deben tener la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

• Se debe establecer un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Tal y como se ha explicado en la sección 2.1.13, el esquema de medidas de seguridad previsto en el reglamento de desarrollo de la LOPD de 1999 deja de ser válido tras la aplicación del RGPD. Los responsables deben revisar y analizar si seguir aplicando las mismas medidas que se establecieron según los resultados de un análisis de riesgo. Según el análisis, los responsables tienen que concluir si las medidas establecidas son las necesarias para ofrecer un nivel de seguridad adecuado. Si no son las necesarias, se deben completar con medidas adicionales o prescindir de alguna de ellas.

El artículo 9 de la LOPD de 1999 condiciona las medidas anteriores al estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. Sin embargo, en la sección 2.1.13 se menciona que el artículo 32 del RGPD añade los siguientes puntos:

• El coste de la técnica.

• Los costes de aplicación.

• La naturaleza, el alcance, el contexto y los fines del tratamiento.

• Los riesgos para los derechos y libertades.

El responsable tiene la obligación de implicarse en la definición, difusión y control de las normas de seguridad entre el personal encargado de llevarlas a cabo o simplemente de respetarlas.

Otra obligación que tienen los responsables y los encargados es la de redactar un documento de seguridad. En la guía de seguridad de datos de la AEPD se muestran los apartados mínimos que debe incluir el documento de seguridad:

• Especificación detallada de los recursos protegidos.

• Medidas, normas, procedimientos, reglas y estándares de seguridad.

• Funciones y obligaciones del personal, estructura y descripción de los ficheros y sistemas de información.

• Procedimiento de notificación, gestión y respuesta ante incidencias.

• Procedimiento de copias de respaldo y recuperación de datos.

• Medidas adoptadas en el transporte, destrucción y/o reutilización de soportes y documentos.

• Identificación del responsable de seguridad y control periódico del cumplimiento del documento.

En caso de haber contratado la prestación de servicios por terceros para determinados ficheros, en el documento de seguridad se debe hacer constar esta circunstancia, indicando una referencia al contrato y su vigencia, así como los ficheros objeto de este tratamiento.

Si se ha contratado la prestación de servicios en relación con la totalidad de los ficheros y tratamientos de datos del responsable, y dichos servicios se prestan en las instalaciones del encargado, se puede delegar en él la elaboración del documento de seguridad.

3.1.18 Notificación de violaciones de seguridad

En la sección 2.1.14 se explica que cuando se produce una violación en la seguridad de los datos, el responsable tiene la obligación de notificarla a la autoridad de protección de datos competente, a menos que sea improbable que la violación suponga un riesgo para los derechos y libertades de las personas afectadas. En esta sección también se menciona el plazo de notificación máximo a la autoridad de protección de datos competente. El plazo es de 72 horas desde que el responsable tiene constancia de que se ha producido una violación. Los responsables también tienen la obligación de documentar todas las violaciones de seguridad que hayan sufrido.

El contenido mínimo de la comunicación de la quiebra de seguridad a la autoridad de protección de datos queda definido en la sección 2.1.14 y comprende los siguientes puntos:

• Naturaleza de la quiebra de seguridad.

• Categorías de datos y de interesados afectados.

• Medidas adoptadas por el responsable para solventar la violación.

• Si procede las medidas aplicadas para paliar los posibles efectos negativos sobre los interesados.

• Número aproximado de personas afectadas.

• Número de registros de datos personales afectados.

• Nombre y datos de contacto del delegado de protección de datos (si lo hubiere).

• Posibles consecuencias de la quiebra de seguridad sufrida.

En los casos en que sea probable que la violación de seguridad entrañe un alto riesgo para los derechos o libertades de los interesados, el responsable debe complementar la notificación a la autoridad con una notificación a los interesados afectados por la violación.

Puede haber casos en que la notificación no pueda realizarse dentro del plazo de 72 horas por la complejidad en determinar completamente el alcance de la violación. En estos casos, es posible hacer la notificación con posterioridad, siempre que el responsable documente los motivos que han ocasionado el retraso.

3.1.19 Evaluación de impacto sobre la protección de datos

Los responsables de tratamiento deben realizar una evaluación de impacto sobre la protección de datos con carácter previo a la puesta en marcha de aquellos tratamientos que sea probable que conlleven un alto riesgo para los derechos y libertades de los interesados tras la realización de un análisis de riesgo. Para los tratamientos iniciados con anterioridad a la aplicación del RGPD y que presentan un alto riesgo, los responsables también tienen que realizar una evaluación de impacto.

A la hora de realizar una EIPD, se debe disponer de una metodología que considere los mínimos definidos en la sección 2.1.15, y que se muestran a continuación:

• Una descripción sistemática de la actividad de tratamiento prevista.

• Una evaluación de la necesidad y proporcionalidad del tratamiento respecto a su finalidad.

• Una evaluación de los riesgos.

• Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales.

En los casos en que la EIPD haya identificado un alto riesgo que, que a juicio del responsable no puede mitigarse por medios razonables en términos de tecnología disponible y costes de aplicación, el responsable debe consultar a la autoridad de protección de datos competente. La autoridad de supervisión puede emitir recomendaciones o ejercer cualquier otro de los poderes que el RGPD le confiere, entre ellos el de prohibir la operación de tratamiento.

La consulta a la autoridad de control ha sido detallada en la sección 2.1.15. A continuación se muestran los contenidos que se deben de incluir en ella:

• Las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento.

• Los fines y medios del tratamiento previsto.

• Las medidas y garantías establecidas para proteger los derechos y libertades de los interesados.

• Los datos de contacto del delegado de protección de datos (si lo hubiere).

• La EIPD.

• Cualquier otra información que solicite la autoridad de control.

Es posible realizar una única EIPD para varios tratamientos similares que entrañen altos riesgos también similares.

Puede ser necesario llevar a cabo una nueva evaluación cuando cambien las condiciones del tratamiento o cuando varíen los riesgos asociados al mismo.

En el anexo 10.1 se muestra la estructura recomendada por la AEPD en su guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD para llevar a cabo evaluaciones de impacto sobre la protección de datos.

3.1.20 Delegado de protección de datos

El delegado ha de ser nombrado atendiendo a sus cualificaciones profesionales y, en particular, a su conocimiento de la legislación y la práctica de la protección de datos. La designación del delegado y sus datos de contacto deben hacerse públicos por los responsables y encargados y deben ser comunicados a las autoridades de supervisión competentes.

Se permite nombrar un solo delegado para un grupo empresarial siempre que sea accesible desde cada establecimiento del grupo.

Las funciones del delegado se encuentran especificadas en la sección 2.1.16, siendo las siguientes:

• Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones del RPGD y demás normativas aplicables en protección de datos.

• Supervisar el cumplimiento del RGPD y demás normativas aplicables en protección de datos, y de las políticas del responsable o encargado del tratamiento en dicha materia, incluida la asignación de responsabilidades, la concienciación y la formación del personal que participa en operaciones de tratamiento, y las auditorías correspondientes.

• Ofrecer el asesoramiento que se solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación conforme al artículo 35 del RGPD.

• Cooperar con la autoridad de control competente.

• Actuar como punto de contacto de la autoridad de control competente para cuestiones relativas al tratamiento, incluida la consulta previa del artículo 36 del RGPD, y a realizar consultas, en su caso, sobre cualquier otro asunto.

3.1.21 Deber de confidencialidad

En el artículo 28 y 90 del RGPD, se exige a quienes intervengan en cualquier fase del tratamiento a guardar secreto profesional sobre los datos, subsistiendo la obligación aún después de finalizar su relación con el responsable.

El responsable debe garantizar que las personas autorizadas para tratar datos personales se comprometan a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.

3.2 Identificación y análisis de soluciones posibles

Tras realizar un estudio técnico tanto del RGPD como de los artículos vigentes de la LOPD de 1999, el siguiente paso es extraer los requisitos técnicos que los responsables y en ocasiones, los encargados, deben tener en cuenta para garantizar el cumplimiento con la normativa de protección de datos. Con estos requisitos se construirán las preguntas que compondrán la guía que se implementará en la aplicación. El objetivo principal es realizar una aplicación sencilla, sin la necesidad de desarrollar una base de datos. De hecho, la aplicación se entenderá como un programa en el que el usuario, en este caso un responsable o un encargado de tratamiento, pueda contestar de forma afirmativa o negativa a las preguntas. Una vez finalizado el formulario, el usuario tendrá disponible los resultados en un informe con un formato .txt, donde se indicarán las preguntas que se han contestado de forma negativa, es decir, los requisitos técnicos que no cumple y, por lo tanto, debe de solucionar para así cumplir con la legislación. Si todas las preguntas se han contestado de forma afirmativa, significa que el usuario cumple con el reglamento y el informe no indicará ningún punto negativo.

Una vez se han analizado las funciones que tendrá la aplicación, lo siguiente es buscar un lenguaje de programación que pueda interactuar con un entorno gráfico, ya que la aplicación se basará en la interacción con el usuario. Entre las opciones que cumplen esta característica están los lenguajes de programación: Php, Android y JavaFX.

La opción de Php va orientada al desarrollo de una aplicación web. Hay que tener en cuenta las desventajas de una aplicación de estas características. Por una parte, requiere que el usuario tenga internet en todo momento, desde que inicia la aplicación hasta que finaliza. Por otra parte, requiere de un servidor para mantener la aplicación disponible en todo momento y para cualquier usuario que quiera utilizarla. Sin embargo, se obtendrían las siguientes ventajas: la aplicación sería más accesible, podría accederse a ella por cualquier dispositivo y no requeriría de espacio en el dispositivo donde se ejecutara.

La opción de Android va orientada al desarrollo de una aplicación para móviles inteligentes y tabletas que soporten Android. Como aspecto positivo a remarca es que para ejecutarla no sería necesario internet, dando la libertad al usuario poder usarla en cualquier momento. Sin embargo, esta opción sí que requeriría de espacio en la memoria. Además, quedarían excluidos dispositivos con sistema operativo iOS y sistema operativo Windows Mobile, al igual que los ordenadores.

La última opción planteada, la de JavaFX, iría orientada al desarrollo de una aplicación de escritorio para ordenadores. En principio, se podría ejecutar en cualquier sistema operativo. Al igual que la opción de Android, se podría iniciar en cualquier momento, independientemente de la existencia de conexión a internet o no. Como en la opción de Android requeriría de espacio en la memoria, aunque su tamaño total no pasaría de los 200 kilobytes. También hay que tener en cuenta que se necesitaría tener instalado Java para su utilización.

3.3 Solución propuesta

La opción elegida para desarrollar la aplicación es la de utilizar el lenguaje de programación JavaFX, en la plataforma NetBeans IDE 8.1 junto con el programa SceneBuilder para el diseño gráfico. Esta solución se ha elegido por los siguientes motivos:

• La idea principal de la aplicación es que se puede ejecutar, al menos en su primera versión, en ordenadores. Por lo que la opción de Android, en un principio, se descarta.

• Un aspecto positivo de JavaFX, es que no obliga a la conexión permanente a internet, por lo que está flexibilidad es un aspecto que ha hecho descartar la opción de Php. También hay que destacar que con la opción de JavaFX, no existe una dependencia a un servidor.

• NetBeans permite separar la parte de programación con la parte de la interfaz gráfica. Permite, por una parte, escribir el código necesario para programar las funcionalidades de la aplicación y por otra, diseñar la interfaz.

• SceneBuilder ofrece múltiples opciones gráficas como, por ejemplo, una gran variedad de contenedores, botones o áreas de texto. Además, permite asignar funcionalidades específicas a cada opción gráfica. De esta forma se enlaza el código que contiene las funcionalidades con el código que contiene la interfaz.

El desarrollo de la aplicación se dividirá en las siguientes fases. En la primera, se diseñará la interfaz gráfica. Una vez diseñada, se procederá a la siguiente fase, donde se programarán las funcionalidades. Las funcionalidades se irán añadiendo de forma progresiva, analizando si cada una de ellas se ha implantado de forma positiva. Por último, al ser una aplicación sencilla, la validación de la aplicación se hará de forma manual, analizando si cada función que realiza el programa la realiza correctamente.

4. Diseño de la solución

El diseño de la aplicación se divide en dos partes, una parte es el diseño de la estructura de la aplicación y la otra es el diseño de las funcionalidades.

La aplicación consta de distintas ventanas. La primera ventana sirve de inicio. A continuación, se mostrará un primer formulario. Con este formulario se pretende que el responsable o el encargado no conteste a ciertas preguntas si está exento a cumplir el requisito técnico del que estas preguntas tratan. Por ejemplo, si no trata datos de menores de edad, está exento de responder las preguntas del tratamiento de datos de menores de edad. En la ilustración 1 se puede observar su contenido.

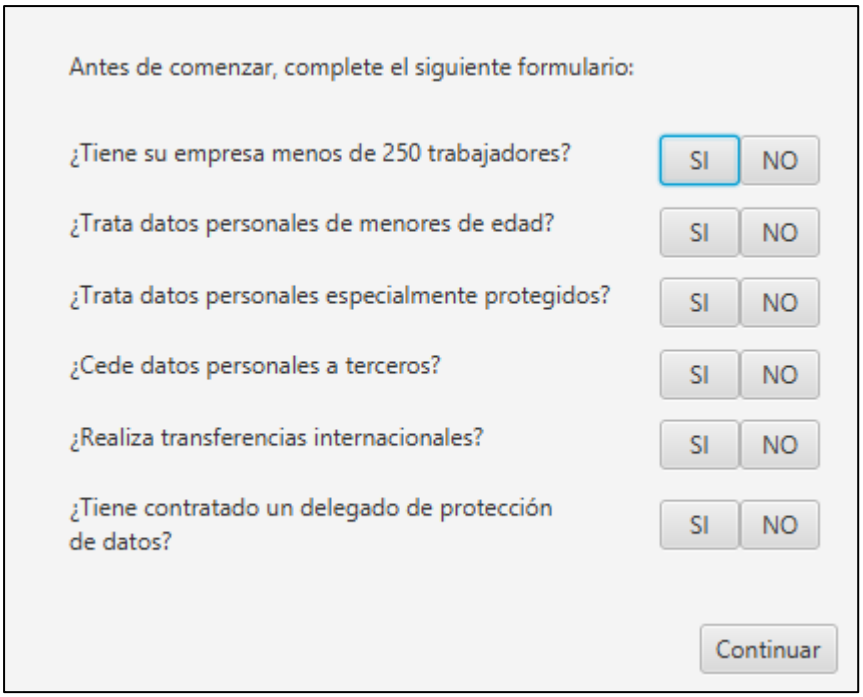

Ilustración 1. Formulario de entrada. Fuente: elaboración propia

La siguiente ventana mostrará el listado completo de requisitos técnicos. Cada requisito esta acompañado con un botón de abrir, donde se mostrarán todas las preguntas que lo componen. En la ilustración 2 se muestra el listado completo.

Ilustración 2. Listado de requisitos técnicos. Fuente: elaboración propia

Cada pregunta, se podrá responder de forma afirmativa, negativa o si se da el caso, de no responderla, si la pregunta está sujeta a una situación opcional. Cuando se ha respondido a todas las preguntas, se podrá pulsar el botón de completar que hará que el requisito se marque como completado. Si no se han completado todas las preguntas obligatorias de ese requisito, se mostrará un aviso indicando que aún existen preguntas sin contestar. En la ilustración 3, se puede observar un ejemplo de un requisito técnico, donde se muestran las preguntas que lo contienen con sus respectivas opciones

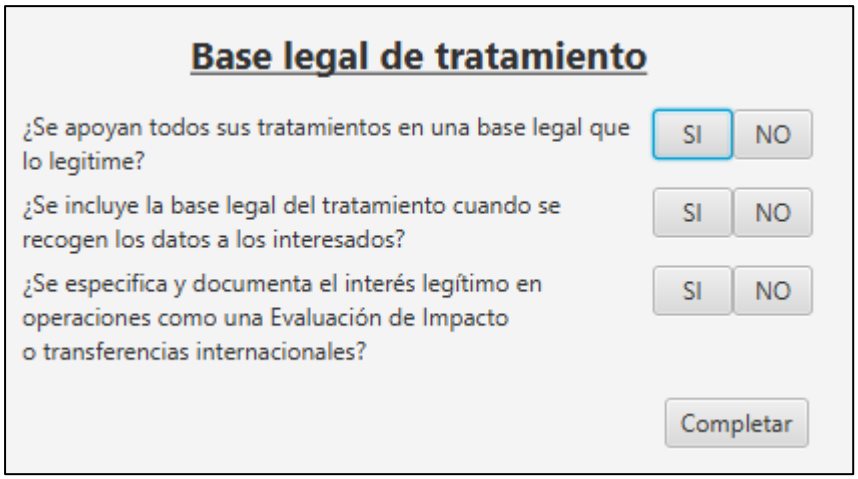

Ilustración 3. Ejemplo de un requisito técnico. Fuente: elaboración propia

Por último, existe un botón para finalizar la aplicación en la ventana donde se muestran todos los requisitos. Si no se han completado todos los requisitos, saldrá una alerta para confirmar la finalización del programa. Si se han completado todos, se mostrará un mensaje donde se indica que el informe ha sido generado.

Por los que respecta al diseño de funcionalidades, la principal función de la aplicación es la generación del informe que contenga los aspectos que no cumple el responsable o el encargado. Cada vez que una pregunta se responda de forma negativa, se añadirá al informe. Otra funcionalidad, con un aspecto secundario, es la de generar avisos como, por ejemplo, en el caso de que alguna pregunta no se haya respondido si esta tiene un carácter obligatorio o si se quiere finalizar la aplicación sin haber completado todos los requisitos. Otras funcionalidades secundarias son la de cambiar el color de los botones de si/no cuando son pulsados o la de mostrar el estado de completado cuando un formulario de un requisito ha sido completado. La última funcionalidad prevista es que las opciones que se marquen en el primer formulario afecten a los requisitos que se puedan completar, bloqueando su acceso en caso de el usuario esté exento de completarlo.

5. Conclusiones

El desarrollo del estudio técnico ha dado como resultado una guía que abarca las obligaciones que tanto los responsables como los encargados deben de tener en cuenta para el cumplir con toda la normativa relativa a la protección de datos. El diseño de la aplicación permite exponerlas de forma sistemática y ordenada, estando cada una de ellas catalogadas dentro de un principio general. Las obligaciones expuestas son independientes del tamaño de la organización o del tipo de administración.

El informe resultante de la ejecución de la aplicación sirve como lista de aspectos a corregir o introducir para cumplir con el RGPD. La aplicación se ha realizado con el objetivo de no necesitar altos conocimientos en materia de protección de datos ni de derecho.

La aplicación está operativa y se puede utilizar. Hay que tener en cuenta que con la entrada en vigor del anteproyecto de la Ley Orgánica de Protección de Datos, es decir, la que será la nueva LOPD, pueden añadirse nuevas obligaciones o se pueden modificar ciertos aspectos en aquellas disposiciones en las que el RGPD da libertad a los Estados miembros de incluir modificaciones. Este anteproyecto no se ha introducido en la aplicación por dos motivos. El primero de ellos es que aún no ha sido aprobado y por lo tanto no es aplicable, y se quería evitar introducir disposiciones que entrarían en contradicción con los artículos en vigor de la LOPD de 1999, como sería el caso del tratamiento de datos de personas fallecidas. El segundo motivo es por tener el estado de anteproyecto y la incertidumbre que pesa sobre esta nueva Ley Orgánica, que en el momento en el que se realiza el trabajo, no se tiene fecha para su aprobación en el Congreso de los Diputados de España.

Sin embargo, en relación con el anteproyecto de la LOPD, sí que ha sido aprobado el Real Decreto-ley (RDL 5/2018, 27 de julio), el cual contiene medidas para la adaptación del Derecho español al RGPD. Este Real Decreto-ley no afecta directamente a este trabajo ya que abarca medidas dirigidas a la autoridad de control competente en España, como son disposiciones en relación con la inspección de protección de datos, disposiciones en el régimen sancionador y disposiciones para el procedimiento en casos de vulneración de la normativa de protección de datos.

En lo referente a versiones futuras, se pretende actualizar la aplicación una vez la nueva LOPD entre en vigor, añadiendo las nuevas obligaciones y modificaciones que incluya.

Con respecto a limitaciones en el proyecto, existía la intención de realizar la aplicación en un formato de aplicación web a parte del formato que tiene en el momento en el que este trabajo es finalizado, pero debido a las complicaciones surgidas para montar un servidor para apoyar a la aplicación y a la falta de tiempo, se ha excluido esta idea. Aunque no se descarta que, en un futuro, si la aplicación evoluciona con éxito, retomar esta intención.

Hay que recalcar que este trabajo, como se ha dicho anteriormente en la sección 2.3, solo abarca un punto de vista de todos los que afectan las normativas de protección de datos, por lo que existe la posibilidad de realizar una guía semejante a esta, pero desde la perspectiva de los titulares de los datos o de las autoridades de control competentes.

En lo personal, este trabajo me ha permitido entender y analizar la normativa de protección de datos. Mejora mis perspectivas de como la legislación protege tanto a los titulares de los datos como los datos en si. Sobre todo, el RGPD, que pone principal atención en proteger los derechos y libertades de las personas afectadas por los tratamientos de datos. Profesionalmente me ha permitido obtener conocimientos sobre materia de protección de datos, ya que se han tratado las obligaciones que deben de cumplir los responsables y encargados con respecto al RGPD y las demás normativas aplicables en protección de datos. Me abre un mercado laboral relacionado con la supervisión del cumplimiento del RGPD y con el asesoramiento e información de este.

6. Relación del trabajo desarrollado con los estudios cursados

Este trabajo abarca dos temas que han sido cursados durante la carrera. Estos dos temas son la normativa de protección de datos y la programación de aplicaciones. Si empezamos por el tema de programación, múltiples asignaturas son las que enseñan tanto aspectos generales como aspectos específicos de los lenguajes de programación. Entre ellas hay que destacar dos asignaturas, ingeniería del software, que dota al alumno de unas directrices para el desarrollo de aplicaciones e interfaz persona computador, que es la asignatura que más cercana es en el diseño de una interfaz. De hecho, en este trabajo se utiliza uno de los programas estudiados para el diseño de interfaces, SceneBuilder.

Por otra parte, el tema de normativa de protección de datos se ha dado en la asignatura de Deontología y Profesionalismo. En esta asignatura se aplican las bases de la protección de datos, de forma que se tratan los aspectos legislativos que se deben tener en cuenta en los tratamientos de datos personales. También se hace hincapié en los derechos que pueden ejercer los titulares de los datos.

7. Referencias

ⓘ Agencia española de protección de datos (2018). “Guía práctica de análisis de riesgo en los tratamientos de datos personales sujetos al RGPD”.

ⓘ Agencia española de protección de datos (2017). “Directrices para la elaboración de contratos entre responsables y encargados”.

ⓘ Agencia española de protección de datos (2013). “Guía para clientes que contraten servicios de *cloud computing*”.

ⓘ Agencia española de protección de datos (2013). “Guía sobre el uso de las *cookies*”.

ⓘ Agencia española de protección de datos (2018). “Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD”.

ⓘ Agencia española de protección de datos (2018). “Protección de datos y administración local”.

ⓘ Agencia española de protección de datos (2010). “Guía de Seguridad de Datos”.

ⓘ Agencia española de protección de datos (2016). “Orientaciones sobre la protección de datos en la reutilización de la información del sector público”.

☮ España. Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Boletín Oficial del Estado, 14 de diciembre de 1999, núm. 298, pp. 43088 – 43099.

☮ España. Ley 34/2002, de 11 de julio, servicios de la sociedad de la información y de comercio electrónico. Boletín Oficial del Estado, 12 de julio de 2002, núm. 166.

☮ España. Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. Boletín Oficial del Estado, 10 de diciembre de 2013, núm. 295, pp. 97922 – 97952.

☮ España. Anteproyecto, s/f, de Ley Orgánica de protección de datos de carácter personal.

☮ Unión Europea. Directiva (UE) 95/46/CE del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos. Diario Oficial de la Unión Europea L 281, 23 de noviembre de 1995, pp. 31-50.

☮ España. Real Decreto-ley 1720/2007, 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Boletín Oficial del Estado, 19 de enero de 2008, núm. 17.

☭ España. Real Decreto-ley 5/2018, 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos. Boletín Oficial del Estado, 30 de julio de 2018, núm. 183.

☭ Unión Europea. Directiva (UE) 2016/680 del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. Diario Oficial de la Unión Europea L 119, 4 de mayo de 2016, pp. 89 – 131.

☭ Unión Europea. Reglamento (UE) 2016/697 del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Diario Oficial de la Unión Europea L 119, 4 de mayo de 2016, pp. 1 – 88.

8. Anexos

8.1 Etapas de una evaluación de impacto sobre la protección de datos

La AEPD en su guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD, estructura la EIPD en tres etapas y recomienda un flujo de ejecución. Las tres etapas se dividen en: análisis del contexto, la gestión de riesgos y la conclusión y validación. Cada una de estas etapas se componen de las actividades que se muestra a continuación:

• Análisis del contexto.

1. Describir el ciclo de vida de los datos: se basa en realizar una descripción detallada del ciclo de vida y del flujo de datos en el tratamiento. Además, esta actividad incluye la identificación de los datos tratados, intervinientes, terceros, sistemas implicados y cualquier elemento relevante que participe en la actividad de tratamiento.

2. Analizar la necesidad y proporcionalidad del tratamiento: esta actividad se compone de la realización de un análisis que abarque la base de legitimación, la finalidad, la necesidad y la proporcionalidad del tratamiento que se pretenden llevar a cabo.

• Gestión de riesgos.

3. Identificar amenazas y riesgos: en esta actividad se procede a la identificación de las amenazas y riesgos potenciales a los que están expuestos las actividades de tratamiento.

4. Evaluar los riesgos: después de identificar las amenazas y los riesgos, se realiza una evaluación de la probabilidad y el impacto de que se materialicen los riesgos a los que está expuesta la organización.

5. Tratar los riesgos: esta actividad trata de proponer soluciones sobre los riesgos identificados, con el objetivo de minimizar la probabilidad y el impacto de que estos se materialicen hasta un nivel de riesgo aceptable que permita garantizar los derechos y libertades de las personas físicas cuyos datos son tratados.

• Conclusión y validación.

6. Plan de acción y conclusiones: por último, cuando se han realizado todas las actividades mencionadas anteriormente, queda realizar un informe de conclusiones de la EIPD, donde se documente el resultado obtenido junto con el plan de acción que incluya las medidas de control a implantar para gestionar los riesgos identificados y poder garantizar los derechos y libertades de las personas físicas y, en el caso de haber realizado una consulta a la autoridad de control, incluir el resultado de la consulta.

8.2 Sistema de capas para mostrar la información relativa a las *cookies*

La AEPD en su guía sobre el uso de las *cookies*, recomienda una estructura donde se muestra toda la información obligatoria que se debe comunicar a los usuarios antes de recabar su consentimiento para la instalación de las *cookies*. La estructura se basa en un sistema de capas. Este sistema consiste en mostrar la información esencial en una primera capa y en una segunda capa ofrecer la información adicional.

En la primera capa se incluiría la siguiente información:

• Advertencia del uso de *cookies* no exceptuadas que se instalan al navegar por dicha página o al utilizar el servicio solicitado.

• Identificación de las finalidades de las *cookies* que se instalan. Información sobre si la instalación y uso de las *cookies* será solo del editor responsable de la web, o también de terceros asociados a él.

• En su caso, advertencia de que, si se realiza una determinada acción manifiestamente afirmativa, se entenderá que el usuario acepta el uso de las *cookies*.

Estará disponible un enlace a una segunda capa informativa en la que se incluye una información más detallada. Esta información se facilitará a través de un formato que sea visible para el usuario y que deberá mantenerse hasta que el usuario realice la acción requerida para la obtención del consentimiento.

En la segunda capa se incluiría la siguiente información:

• Definición y función de las *cookies*.

• Información a través de un cuadro o listado sobre el tipo de *cookies* que utiliza la página web y su finalidad.

• Información sobre la forma de desactivar o eliminarlas las *cookies* a través de las funcionalidades facilitadas por el editor, las herramientas proporcionadas por el navegador o el terminal o través de las plataformas comunes que pudieran existir, para esta finalidad, así como la forma de revocación del consentimiento ya prestado.

• Información sobre la identificación de quién utiliza las *cookies*, es decir, si la información obtenida por las *cookies* es tratada solo por el editor y/o también por terceros con los que el editor haya contratado la prestación de un servicio para el cual se requiera el uso de *cookies*, con identificación de estos últimos.

8.3 Sanciones del anteproyecto de la Ley Orgánica de Protección de Datos

Con la aplicación del RGPD, como se ha mencionado durante todo el trabajo, muchas de las disposiciones de la Ley Orgánica de Protección de Datos de 1999 quedan derogadas y, en consecuencia, también sus sanciones correspondientes. Por lo tanto, ante esta situación las sanciones aplicables son las definidas en el RGPD. Sin embargo, en el momento en el que el trabajo es desarrollado, están disponibles las sanciones que traerá la futura Ley Orgánica de Protección de Datos, en este momento, en estado de anteproyecto, por lo que se deberían tener en cuenta para el futuro. Las sanciones se muestran a continuación:

En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados, y en particular las siguientes:

a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679.

b) El tratamiento de datos personales sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el artículo 6 del Reglamento (UE) 2016/679.

c) El incumplimiento de los requisitos exigidos por el artículo 7 del Reglamento (UE) 2016/679 para la validez del consentimiento.

d) La utilización de los datos para una finalidad que no sea compatible con la finalidad para la cual fueron recogidos, sin contar con el consentimiento del afectado o con una base legal para ello.

e) El tratamiento de datos personales de las categorías a las que se refiere el artículo 9 del Reglamento (UE) 2016/679, sin que concurra alguna de las circunstancias previstas en dicho precepto y en el artículo 10 de esta ley.

f) El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad fuera de los supuestos permitidos por el artículo 10 del Reglamento (UE) 2016/679 y en el artículo 20 de esta ley.

g) El tratamiento de datos de carácter personal relacionados con infracciones y sanciones administrativas fuera de los supuestos permitidos por el artículo 4.

h) La omisión del deber de informar al afectado acerca del tratamiento de sus datos de carácter personal conforme a lo dispuesto en los artículos 13 y 14 del Reglamento (UE) 2016/679 y 21 de esta ley orgánica.

i) La vulneración del deber de confidencialidad establecido en el artículo 6.

j) La exigencia del pago de un canon para facilitar al afectado la información a la que se refieren los artículos 13 y 14 del Reglamento (UE) 2016/679 o por atender las solicitudes de ejercicio de derechos de los afectados previstos en los artículos 15 a 22

del Reglamento (UE) 2016/679, fuera de los supuestos establecidos en su artículo 12.5.

k) El impedimento o la obstaculización o la no atención reiterada del ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

l) La transferencia internacional de datos de carácter personal a un destinatario que se encuentre en un tercer país o a una organización internacional, cuando no concurran las garantías, requisitos o excepciones establecidos en los artículos 44 a 49 del Reglamento (UE) 2016/679.

m) El incumplimiento de las resoluciones dictadas por la autoridad de protección de datos competente en ejercicio de los poderes que le confiere el artículo 58.2 del Reglamento (UE) 2016/679.

n) El incumplimiento de la obligación de bloqueo de los datos establecida en el artículo 29 cuando la misma sea exigible.

ñ) No facilitar el acceso del personal de la autoridad de protección de datos competente a los datos personales, información, locales, equipos y medios de tratamiento que sean requeridos por la autoridad de protección de datos para el ejercicio de sus poderes de investigación.

o) La resistencia u obstrucción del ejercicio de la función inspectora por la autoridad de protección de datos competente.

Tendrán la misma consideración y también prescribirán a los tres años las infracciones a las que se refiere el artículo 83.6 del Reglamento (UE) 2016/679.

En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquél, y en particular las siguientes:

a) El tratamiento de datos de carácter personal de un menor de trece años sin recabar su consentimiento, cuando tenga capacidad para ello, o el del titular de su patria potestad o tutela, conforme al artículo 8 del Reglamento (UE) 2016/679.

b) No acreditar la realización de esfuerzos razonables para verificar la validez del consentimiento prestado por un menor de trece años o por el titular de su patria potestad o tutela sobre el mismo, conforme a lo requerido por el artículo 8.2 del Reglamento (UE) 2016/679.

c) El impedimento o la obstaculización o la no atención reiterada de los derechos de acceso, rectificación, supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando éste, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación.

d) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el diseño y por defecto e integrar las garantías necesarias en el tratamiento, en los términos exigidos por el artículo 25.1 del Reglamento (UE) 2016/679.

e) La falta de adopción de las medidas técnicas y organizativas apropiadas para garantizar que, por defecto, sólo se tratarán los datos personales necesarios para cada uno de los fines específicos del tratamiento, conforme a lo exigido por el artículo 25.2 del Reglamento (UE) 2016/679.

f) El incumplimiento de la obligación de designar un representante del responsable o encargado del tratamiento no establecido en el territorio de la Unión Europea, conforme a lo previsto en el artículo 27 del Reglamento (UE) 2016/679.

g) La falta de atención por el representante en la Unión del responsable o del encargado del tratamiento de las solicitudes efectuadas por la autoridad de protección de datos o por los afectados.

h) La contratación por el responsable del tratamiento de un encargado de tratamiento que no ofrezca las garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas conforme a lo establecido en el Capítulo IV del Reglamento (UE) 2016/679.

i) Encargar el tratamiento de datos a un tercero sin la previa formalización de un contrato u otro acto jurídico escrito con el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679.

j) La contratación por un encargado del tratamiento de otros encargados sin contar con la autorización previa del responsable, o sin haberle informado sobre los cambios producidos en la subcontratación cuando fueran legalmente exigibles.

k) La infracción por un encargado del tratamiento de lo dispuesto en el Reglamento (UE) 2016/679 y la presente ley orgánica, al determinar los fines y los medios del tratamiento, conforme a lo dispuesto en el artículo 28.10 del citado reglamento.

l) No disponer del registro de actividades de tratamiento establecido en el artículo 30 del Reglamento (UE) 2016/679.

m) No poner a disposición de la autoridad de protección de datos que lo haya solicitado, el registro de actividades de tratamiento, conforme al apartado 4 del artículo 30 del Reglamento (UE) 2016/679.

n) No cooperar con las autoridades de control en el desempeño de sus funciones en los supuestos no previstos en el artículo 72 de esta ley orgánica.

ñ) El tratamiento de datos de carácter personal sin llevar a cabo una previa valoración de los riesgos que el mismo pudiera generar en los derechos de los afectados, y en particular en su derecho a la protección de datos de carácter personal, conforme a lo dispuesto en el artículo 30.

o) El incumplimiento del deber del encargado del tratamiento de notificar al responsable del tratamiento las violaciones de seguridad de las que tuviera conocimiento.

p) El incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.

q) El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos de conformidad con lo previsto en el artículo 34 del Reglamento (UE) 2016/679 si el responsable del tratamiento hubiera sido requerido por la autoridad de protección de datos para llevar a cabo dicha notificación.

r) El tratamiento de datos de carácter personal sin haber llevado a cabo la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales en los supuestos en que la misma sea exigible.

s) El tratamiento de datos de carácter personal sin haber consultado previamente a la autoridad de protección de datos en los casos en que dicha consulta resulta preceptiva conforme al artículo 36 del Reglamento (UE) 2016/679 o cuando la ley establezca la obligación de llevar a cabo esa consulta.

t) El incumplimiento de la obligación de designar un delegado de protección de datos cuando sea exigible su nombramiento de acuerdo con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 33 de esta ley orgánica.

u) No posibilitar la efectiva participación del delegado de protección de datos en todas las cuestiones relativas a la protección de datos personales, no respaldarlo o interferir en el desempeño de sus funciones.

v) La utilización de un sello o certificación en materia de protección de datos que no haya sido otorgado por una entidad de certificación debidamente acreditada o en caso de que la vigencia de este hubiera expirado.

w) Obtener la acreditación como organismo de certificación presentando información inexacta sobre el cumplimiento de los requisitos exigidos por el artículo 43 del Reglamento (UE) 2016/679.

x) El desempeño de funciones que el Reglamento (UE) 2016/679 reserva a los organismos de certificación, sin haber sido debidamente acreditado conforme a lo establecido en el artículo 40 de esta ley orgánica.

y) El incumplimiento por parte de un organismo de certificación de los principios y deberes a los que está sometido según lo previsto en los artículos 42 y 43 de Reglamento (UE) 2016/679.

z) El desempeño de funciones que el artículo 41 del Reglamento (UE) 2016/679 reserva a los organismos de supervisión de códigos de conducta sin haber sido previamente acreditado por la autoridad de protección de datos competente.

aa) La falta de adopción por parte de los organismos acreditados de supervisión de un código de conducta de las medidas que resulten oportunas en caso de que se hubiera producido una infracción del código, conforme exige el artículo 41.4 del Reglamento (UE) 2016/679.

Se consideran leves y prescribirán al año las restantes infracciones de carácter meramente formal de los artículos mencionados en los apartados 4 y 5 del artículo 83 del Reglamento (UE) 2016/679 y, en particular, las siguientes:

a) El incumplimiento del principio de transparencia de la información o el derecho de información del afectado por no facilitar toda la información exigida por los artículos 13 y 14 del Reglamento (UE) 2016/679.

b) La exigencia del pago de un canon para facilitar al afectado la información exigida por los artículos 13 y 14 del Reglamento (UE) 2016/679 o por atender las solicitudes de ejercicio de derechos de los afectados previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679, cuando así lo permita su artículo 12.5, si su cuantía excediese el importe de los costes afrontados para facilitar la información o realizar la actuación solicitada.

c) No atender las solicitudes de ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, salvo que resultase de aplicación lo dispuesto en el artículo 72.1.k) de esta ley orgánica.

d) No atender los derechos de acceso, rectificación, supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando éste, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación, salvo que resultase de aplicación lo dispuesto en el artículo 73.c).

e) El incumplimiento de la obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento exigida por el artículo 19 del Reglamento (UE) 2016/679.

f) El incumplimiento de la obligación de informar al afectado, cuando así lo haya solicitado, de los destinatarios a los que se hayan comunicado los datos personales rectificados, suprimidos o respecto de los que se ha limitado el tratamiento.

g) El incumplimiento de la obligación de suprimir los datos referidos a una persona fallecida cuando ello fuera exigible conforme al artículo 3.

h) La falta de formalización por los corresponsables del tratamiento del acuerdo que determine las obligaciones, funciones y responsabilidades respectivas con respecto al tratamiento de datos personales y sus relaciones con los afectados al que se refiere el artículo 26 del Reglamento (UE) 2016/679 o la inexactitud en la determinación de estas.

i) No poner a disposición de los afectados los aspectos esenciales del acuerdo formalizado entre los corresponsables del tratamiento, conforme exige el artículo 26.2 del Reglamento (UE) 2016/679.

j) La falta del cumplimiento de la obligación del encargado del tratamiento de informar al responsable del tratamiento acerca de la posible infracción por una instrucción recibida de éste de las disposiciones del Reglamento (UE) 2016/679 o de esta ley orgánica, conforme a lo exigido por el artículo 28.3 del citado reglamento.

k) El incumplimiento por encargado o subencargado de las estipulaciones impuestas en el contrato o acto jurídico que regula el tratamiento o las instrucciones del responsable del tratamiento, salvo que esté legalmente obligado a ello conforme al Reglamento (UE) 2016/679 y la presente ley orgánica o en los supuestos en que fuese necesario para evitar la infracción de la legislación en materia de protección de datos y se hubiese advertido de ello al responsable o al encargado del tratamiento.

l) Disponer de un registro de actividades de tratamiento que no incorpore toda la información exigida por el artículo 30 del Reglamento (UE) 2016/679.

m) La notificación incompleta o defectuosa a la autoridad de protección de datos de la información relacionada con una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.

n) El incumplimiento de la obligación de documentación de cualquier violación de seguridad, exigida por el artículo 33.5 del Reglamento (UE) 2016/679.

ñ) El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos que entrañe un alto riesgo para los derechos y libertades de los afectados, conforme a lo exigido por el artículo 34 del Reglamento (UE) 2016/679, salvo que resulte de aplicación lo previsto en el artículo 73.q) de esta ley orgánica.

o) Facilitar información inexacta a la autoridad de protección de datos, en los supuestos en los que el responsable del tratamiento deba elevarla una consulta previa, conforme al artículo 36 del Reglamento (UE) 2016/679.

p) No publicar los datos de contacto del delegado de protección de datos, o no comunicarlos a la autoridad de protección de datos, cuando su nombramiento sea exigible de acuerdo con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 35.3 de esta ley orgánica.

q) El incumplimiento por los organismos de certificación de la obligación de informar a la autoridad de protección de datos de la expedición, renovación o retirada de una certificación, conforme a lo exigido por los apartados 1 y 5 del artículo 43 del Reglamento (UE) 2016/679.

r) El incumplimiento por parte de los organismos acreditados de supervisión de un código de conducta de la obligación de informar a las autoridades de protección de datos acerca de las medidas que resulten oportunas en caso de infracción del código, conforme exige el artículo 41.4 del Reglamento (UE) 2016/679.

Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

De acuerdo con lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

a) El carácter continuado de la infracción.

b) La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.

c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.

d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.

e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.

Será posible, complementaria o alternativamente, la adopción, cuando proceda, de las restantes medidas correctivas a las que se refiere el artículo 83.2 del Reglamento (UE) 2016/679.

Será objeto de publicación en el Boletín Oficial del Estado la información que identifique al infractor, la infracción cometida y el importe de la sanción impuesta cuando la autoridad competente sea la Agencia Española de Protección de Datos, la sanción fuese superior a un millón de euros y el infractor sea una persona jurídica.

8.4 Tipología de contrato responsable – encargado

El documento diseñado por la AEPD que contiene las directrices para la elaboración de contratos entre responsables y encargados recomienda una tipología de contrato que incluye los requerimientos exigidos por el RGPD. La recomendación del tipo de contrato es la siguiente:

1. Objeto del encargo del tratamiento

Mediante las presentes cláusulas se habilita a la entidad
.....,

encarga da del tratamiento, para tratar por cuenta de
.....,

responsable del tratamiento, los datos de carácter personal necesarios para prestar el servicio de
.....

El tratamiento consistirá en: (añadir una descripción detallada del servicio).

Concreción de los tratamientos a realizar: (marcar las actividades que va a realizar el encargado).

◦ Recogida.

◦ Registro.

◦ Estructuración.

◦ Modificación.

◦ Conservación.

◦ Extracción.

◦ Consulta.

◦ Comunicación por transmisión.

◦ Difusión.

◦ Interconexión.

◦ Cotejo.

◦ Limitación.

◦ Supresión.

◦ Destrucción.

◦ Conservación.

◦ Comunicación.

Otros: .....

2. Identificación de la información afectada

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, la entidad/órgano ....., responsable del tratamiento, pone a disposición de la entidad ....., encargada del tratamiento, la información que se describe a continuación:

• .....

• .....

3. Duración

El presente acuerdo tiene una duración de
.....

Una vez finalice el presente contrato, el encargado del tratamiento debe suprimir/devolver al responsable o a otro encargado que designe el responsable (indicar la opción que proceda) los datos personales y suprimir cualquier copia que esté en su poder.

4. Obligaciones del encargado del tratamiento

El encargado del tratamiento y todo su personal se obliga a:

a. Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.

b. Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento. Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el encargado informará inmediatamente al responsable.

c. Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga:

1. 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.

2. Las categorías de tratamientos efectuados por cuenta de cada responsable.

3. 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 del RGPD, la documentación de garantías adecuadas.

4. Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:

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) El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

d. No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles.

El encargado puede comunicar los datos a otros encargados del tratamiento de este responsable, de acuerdo con las instrucciones del responsable. En este caso, el responsable identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación.

Si el encargado debe transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al responsable de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

e. Subcontratación (Escoger una de las opciones)

Opción A

No subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios del encargado.

Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al responsable, con una antelación de ....., indicando los tratamientos que se pretende subcontratar e identificando de forma clara

e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo establecido.

El subcontratista, que también tendrá la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el encargado del tratamiento y las instrucciones que dicte el responsable. Corresponde al encargado inicial regular la nueva relación de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad...) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

Opción B

Se autoriza al encargado a subcontratar con la empresa ..... las prestaciones que comporten los tratamientos siguientes: .....

Para subcontratar con otras empresas, el encargado debe comunicarlo por escrito al responsable, identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo de .....

El subcontratista, que también tiene la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el encargado del tratamiento y las instrucciones que dicte el responsable. Corresponde al encargado inicial regular la nueva relación, de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad...) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

f. Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice su objeto.

g. Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

h. Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

i. Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

j. Asistir al responsable del tratamiento en la respuesta al ejercicio de los derechos de:

1. Acceso, rectificación, supresión y oposición

2. Limitación del tratamiento

3. Portabilidad de datos

4. A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles)

(Escoger una de las opciones)

Opción A

El encargado del tratamiento debe resolver, por cuenta del responsable, y dentro del plazo establecido, las solicitudes de ejercicio de los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, en relación con los datos objeto del encargo.

Opción B

Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, ante el encargado del tratamiento, éste debe comunicarlo por correo electrónico a la dirección..... (dirección que indique el responsable). La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.

k. Derecho de información

(Escoger una de las opciones)

Opción A

El encargado del tratamiento, en el momento de la recogida de los datos, debe facilitar la información relativa a los tratamientos de datos que se van a realizar. La redacción y el formato en que se facilitará la información se debe consensuar con el responsable antes del inicio de la recogida de los datos.

Opción B

Corresponde al responsable facilitar el derecho de información en el momento de la recogida de los datos.

l. Notificación de violaciones de la seguridad de los datos

El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida, y en cualquier caso antes del plazo máximo de ....., y a través de....., las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si se dispone de ella se facilitará, como mínimo, la información siguiente:

a) Descripción de 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) 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) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

d) Descripción de las medidas adoptadas o propuestas 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.

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

(Escoger alguna o las dos opciones)

Opción A

Corresponde al encargado del tratamiento comunicar las violaciones de la seguridad de los datos a la Autoridad de Protección de Datos.

La comunicación contendrá, como mínimo, la información siguiente:

a) Descripción de 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) Nombre y datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

c) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

d) Descripción de las medidas adoptadas o propuestas 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.

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

Opción B

Corresponde al encargado del tratamiento comunicar en el menor tiempo posible las violaciones de la seguridad de los datos a los interesados, cuando sea probable que la

violación suponga un alto riesgo para los derechos y las libertades de las personas físicas.

La comunicación debe realizarse en un lenguaje claro y sencillo y deberá, como mínimo:

a) Explicar la naturaleza de la violación de datos.

b) Indicar 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.

m. Dar apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

n. Dar apoyo al responsable del tratamiento en la realización de las consultas previas a la autoridad de control, cuando proceda.

o. Poner disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.

p. Implantar las medidas de seguridad siguientes:

(Escoger una o las dos opciones)

Opción A

Las medidas de seguridad siguientes, de acuerdo con la evaluación de riesgos realizada por ....., en fecha .....:

•.....

•.....

•.....

Opción B

Las medidas de seguridad establecidas en .....

En todo caso, deberá implantar mecanismos para:

a) Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

b) Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

c) Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.

d)Seudonimizar y cifrar los datos personales, en su caso.

q. Designar un delegado de protección de datos y comunicar su identidad y datos de contacto al responsable.

r. Destino de los datos

(Escoger una de las tres opciones)

Opción A

Devolver al responsable del tratamiento los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida la prestación.

La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado.

No obstante, el encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

Opción B

Devolver al encargado que designe por escrito el responsable del tratamiento, los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida prestación.

La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado.

No obstante, el encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

Opción C

Destruir los datos, una vez cumplida la prestación. Una vez destruidos, el encargado debe certificar su destrucción por escrito y debe entregar el certificado al responsable del tratamiento.

No obstante, el encargado puede conservar una copia, con los datos debidamente boqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

5. Obligaciones del responsable del tratamiento

Corresponde al responsable del tratamiento:

a) Entregar al encargado los datos a los que se refiere la cláusula 2 de este documento.

b) Realizar una evaluación del impacto sobre la protección de datos personales de las operaciones de tratamiento a realizar por el encargado.

c) Realizar las consultas previas que corresponda.

d) Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del encargado.

e) Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

8.5 Ejemplos para recabar el consentimiento cumpliendo con las exigencias del RGPD

Tal y como se ha mencionado en la sección 2.1.5 y en la sección 2.1.6 en los casos en que la base jurídica de los tratamientos sea el consentimiento, el responsable tiene la obligación de garantizar que el consentimiento cumple con las características previstas por el RGPD.

El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal.

Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento.

A continuación, se muestran mecanismos de obtención del consentimiento validos en el caso de servicios de la sociedad de la información:

• A través de la aceptación de los “Términos y condiciones de uso de la página web” o de su “Política de privacidad” al solicitar el alta en un servicio.

• Durante el proceso de configuración del funcionamiento de la página web o aplicación.

• En el momento en que se solicite una nueva función ofrecida en la página web o aplicación.

• Antes del momento en que se vaya a descargar un servicio o aplicación ofrecido en la página web.

El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta.

Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño. El consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños.

Cuando el tratamiento se lleva a cabo con el consentimiento del interesado, el responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento. En particular en el contexto de una declaración por escrito efectuada sobre otro asunto, debe haber garantías de que el interesado es consciente del hecho de que da su consentimiento y de la medida en que lo hace.

Debe proporcionarse un modelo de declaración de consentimiento elaborado previamente por el responsable del tratamiento con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, y que no contenga cláusulas abusivas. Para que el consentimiento sea informado, el interesado debe conocer como mínimo la identidad del responsable del tratamiento y los fines del tratamiento a los cuales están destinados los datos personales. El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno.

9 Glosario

Metadato: se refiere a un grupo de datos que describen el contenido informativo de un objeto. El concepto de metadatos es análogo al uso de índices para localizar objetos en vez de datos. Los metadatos en etiquetas son un enfoque importante para que cuando un objeto está almacenado conjuntamente con otros, pueda ser descrito para facilitar las búsquedas que pudieran tratar de encontrarlo a partir de sus características distintivas.

Seudonimización: se refiere al tratamiento de datos personales de tal manera que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

Espacio Económico Europeo: el Espacio Económico Europeo comprende todos los Estados miembros de la Unión Europea, más Noruega, Islandia y Liechtenstein. Se instauró con motivo de un acuerdo entre países de la Unión Europea y de la Asociación Europea de Libre Comercio, excepto Suiza. Su creación permitió a los países de la Asociación Europea de Libre Comercio participar en el mercado interior de la Unión Europea sin necesidad de adherirse a la Unión. La Asociación Europea de Libre Comercio está compuesta por Austria, Dinamarca, Reino Unido, Noruega, Portugal, Suecia y Suiza.

Comisión Europea: es el órgano ejecutivo y de iniciativa legislativa sobre el Parlamento europeo y el consejo de la Unión Europea. Se encarga de proponer la legislación, la aplicación de las decisiones, la defensa de los tratados de la Unión y del día a día de la Unión. La Comisión actúa como un gabinete de gobierno, con los 28 miembros de la comisión.

Evaluación de impacto sobre la protección de datos: es una herramienta que permite evaluar de manera anticipada cuáles son los potenciales riesgos a los que están expuestos los datos personales en función de las actividades de tratamiento que se llevan a cabo con los mismos. El análisis de riesgos para un determinado tratamiento permite identificar los riesgos que se ciernen sobre los datos de los interesados y establecer una respuesta adoptando las salvaguardas necesarias para reducirlos hasta un nivel de riesgo aceptable.

Protección de datos desde el diseño: el principio de protección de datos desde el diseño supone que la protección de datos ha de estar presente en las primeras fases de concepción de un proyecto y formar parte de la lista de elementos a considerar antes de iniciar las sucesivas etapas de desarrollo. Estos requisitos se van a traducir en medidas técnicas y organizativas con el objeto de aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento.

Protección de datos por defecto: consiste en que sólo sean objeto de tratamiento los datos personales que sean estrictamente necesarios para cada uno de los fines de

tratamiento. Si fuera posible por la naturaleza del proceso, llegar a que no se traten datos de carácter personal.

Autoridad de control\ autoridad de supervisión\ autoridad de protección de datos: la autoridad pública independiente establecida por un Estado miembro.

Autoridad de control competente\ autoridad de supervisión competente\ autoridad de protección de datos competente: autoridad de control a la que afecta el tratamiento de datos personales debido a que:

a) el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control.

b) los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento.

c) se ha presentado una reclamación ante esa autoridad de control.