TRABAJO DE FINAL DE GRADO

EL COMERCIO DE DATOS PERSONALES EN LA ACTUALIDAD.

¿Cómo reaccionan las empresas a la nueva regulación de protección de datos personales ?

Autora

Lidia Pérez Tomás

Directora

Concepción Blázquez Giménez

Grado de derecho

Facultad de Derecho

Curso 2019- 2020

Índice

Resumen

En un contexto social donde los dispositivos electrónicos y la conectividad están a la orden del dia, la UE se decide en 2016 a regular el uso de los datos personales con tal de ofrecer una eficaz protección al ciudadano, al mismo tiempo que ofrecer a las entidades la posibilidad de tratarlos y fomentar un mercado único digital europeo.

Ante el nuevo marco legislativo, las entidades que tratan los datos personales deben afrontar nuevos cambios. Este trabajo focaliza la atención en la comunicación de los datos personales entre entidades para realizar un ejercicio de analisi de los mismos para obtener un valor añadido.

Así, se abordarán las exigencias que el Reglamento 2016/679 juntamente con la normativa estatal plantean a tales entidades, modificando por ejemplo, las condiciones del consentimiento, exigiendo una actitud proactiva en materia de garantizar la protección de datos etc. En un enfoque más práctico, se abordan cuestiones como las bases legitimadoras del tratamiento, el tratamiento que se realiza, y las finalidades que persiguen, para analizar las políticas de privacidad tomadas por diferentes empresas líderes.

Abstract

In a social enviroment where electronic devices and connectivity are on our dayly basis, the EU decides in 2016 to regulate the use of personal data in order to offer effective protection to citizens, while at the same time giving entities the possibility of processing them and promoting an European digital single market.

In view of the new legislative framework, entities that process personal data must face new changes. This study focuses on the communication of personal data between entities in order to carry out an exercise of analysis to obtain an added value.

In that whay, the requirements that Regulation 2016/679 together with the state regulations impose to such entities will be aproched, modifying, for example, the conditions of consent, requiring a proactive attitude in terms of guaranteeing data protection, etc. In a more practical approach, issues such as the legitimacy of the processing, the processing carried out, and the objective pursued, will be addressed in order to analyse the privacy policies adopted by different leading companies.

Resum

En un context social on els dispositius electrònics i la connectivitat formen part de la nostre vida, la UE decideix el 2016 regular l'ús de les dades personals amb l'objectiu de oferir una protecció eficaç al ciutadà, i a l'hora oferir a les entitats la possibilitat de tractar-los i fomentar un mercat digital europeu únic.

Front el nou marc legislatiu, les entitats que tracten les dades personals han d'afrontar nous canvis. Aquest treball focalitza la atenció en la comunicació de dades personals entre entitats per realitzar un exercici de anàlisis d'aquests i obtenir un valor afegit.

Així doncs, s'abordaran las exigències que el Reglament 2016/679 juntament amb la normativa estatal plantegen a les entitats modificant, per exemple, les condicions del consentiment, exigint una actitud proactiva en matèria de garantir la protecció de dades etc. Amb una perspectiva més pràctica, s'examinaran qüestions com les bases legitimadores del tractament, el tractament que es realitza, i les finalitats que es persegueixen, per analitzar les polítiques de privacitat adoptades per diferents empreses líders.

Abreviaturas

AEPD: Agencia Española de Protección de Datos.

AIQ: AggregateIQ

Art(s).: artículo(s).

Directiva 95/46/CE: Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

EIPD: Evaluación de impacto de Protección de Datos.

GPS: Sistema de Posicionamento Global.

IBM: Internacional Business Machines.

INE: Instituo Nacional de Estadística.

LOPD: Ley Orgánica 3/2018, del 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Op. cit.: en la obra citada.

UE: Unión Europea.

Reglamento 2016/679: Reglamento (UE) 2016/679 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.

Ss.: Siguientes.

I. Introducción

*"*A diario se crean 2,5 trillones de bytes de datos, lo cual supone que el 90% de los datos en el mundo de hoy se han creado en los últimos 2 años*"*[1]. Estos datos han sido obtenidos a través de diferentes fuentes, ya sean señales de GPS, publicaciones en redes sociales o transacciones de compras realizados en plataformas digitales. En un contexto social donde la tecnología se ha introducido plenamente en la vida cotidiana, la creación de datos constantemente y el volumen de los mismos es una realidad.

En este mar de datos emerge un nuevo método de procesamiento de los mismos que revolucionará y redefinirá la nueva sociedad de la información. A partir de dicha tecnología, y partiendo de un escenario donde se dispone de una cantidad inmensurable de datos procedentes de diferentes orígenes de contenido muy diverso e internacional, el análisis Big Data aparece como un instrumento o planteamiento capaz de poner orden a todos estos y a partir un análisis extenso no tan tradicional basado en algoritmos, crear nueva información que tendrá un valor propio. Como IBM afirma, "el valor comercial de los datos proviene del significado que podemos cosechar de ellos*"*[2].

Este concepto, se ha introducido en gran cantidad de sectores, como se verá más adelante, pero por lo que concierna este estudio, cabe destacar el papel que ha adquirido este conocimiento en el sector empresarial.

De acuerdo con un estudio realizado por el Instituto Nacional de Estadística[3], en los años 2017 y 2018 más del 30% de las empresas que forman la muestra aseguran analizar datos a partir del sistema Big Data. Los datos eran obtenidos por la propia empresa a partir de sensores o dispositivos inteligentes, datos generados

[1] Hernández-Pérez, T (2016) *En la era de la web de los datos abiertos, después los datos masivos*. Cita originaria IBM (2016) https://www-01.ibm.com/software/data/bigdata/what-isbig-data.html

[2] Perry, J.S. (2017). *What is big data? More than volume, velocity and variety*. Recuperado de https://developer.ibm.com/dwblog/2017/what-is-big-data-insight/

[3] INE. (2019). *Encuesta de uso de TIC y Comercio electrónico (CE) en las empresas 2017- 2018.* Recuperado de https://www.ine.es/jaxi/Datos.htm?path=/t09/e02/a2017-2018/l0/&file=02013.px

por los medios sociales, e incluso datos por geolocalización a partir de dispositivos portátiles. Cabe destacar que el 80% de las empresas encuestadas afirman que el análisis de Big Data fue realizado por los propios empleados de la empresa, pero aun así, un 40% lo hicieron a partir de proveedores externos a la misma. Con esta información, se pone en evidencia la importancia que ha adquirido para las empresas la obtención de datos para su posterior análisis, y su mejor toma de decisiones.

Y es tal la importancia que adquiere que, según un estudio realizado por la International Data Corporation[4], se preveía que en el año 2019 los ingresos por soluciones de Big Data y analítica alcanzarían los 189.000 millones de dólares.

Pero dejando a un lado la información económica, debemos centrar la atención en la procedencia de los datos objeto de análisis. Los datos a los que nos referimos son los millones de datos que como hemos visto anteriormente, dejamos en internet. El uso y acceso a estos está estrechamente ligado con el derecho a la intimidad y privacidad, recogidos como derechos fundamentales por la Constitución Española, y es que como afirma la Dra. Cintia Castillo (2001),

> factores como la velocidad, la potencia y la capacidad de almacenamiento de los ordenadores pueden suponer una seria amenaza al derecho a la intimidad y privacidad de las personas, riesgo que se ve aumentado cuando se facilita la comunicación entre terminales separados por miles de kilómetros, y no existiendo ningún impedimento técnico para el tratamiento de los datos personales[5].

Para exponer de forma ilustrativa el alcance e impacto que llega a obtener el uso de los datos personales por medios y empresas, pudiendo incluso influir en nuestra intimidad y privacidad, se expondrá brevemente el mediático caso de 2018

[4] Fundación COTEC para la innovación (2017). *Generación de talento Big data en España.* Recuperado de https://www.ituser.es/big-data/2019/04/las-soluciones-de-big-data-y-analitica-creceran-un-12-en-2019

[5] Castillo Jiménez, C. (2001). Derecho y conocimiento. *Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información*. Volumen 1, 35-48. P. 38

de *Cambridge Analytica* y su campaña electoral para el actual presidente de los Estados Unidos, Donal Trump.

Todo empieza con una inversión muy elevada del republicano Robert Mercer a la compañía con la intención de hacer uso de "herramientas que podrían identificar a las personalidades de los votantes estadounidenses e influir en su comportamiento[6]". El problema surge cuando *Cambridge Analytica* carece de los datos personales que podrían ser de utilidad para tal fin. Ante esa situación, "Cambridge pagó para adquirir la información personal a través de un investigador externo que, según Facebook, afirmó que la estaba recopilando con fines académicos"[7].

Y siguiendo el mismo patrón, Facebook protagoniza un segundo escándalo de violación de la privacidad y de uso ilegal de datos personales con fines políticos, esta vez en territorio comunitario. En esta ocasión, la empresa que proceso los datos fue AIQ, estrechamente ligada con la compañía *Cambridge Analytica.* En este caso la compañía hizo nuevamente un uso no permitido de los datos personales de miles de usuarios de Facebook para realizar la campaña electoral de *Vote Leave* para el *Brexit*.

Así pues, debido al escándalo de Facebook en Estados Unidos, la Comisión Federal del Comercio de Estados Unidos ordeno a la compañía a pagar 5.000 millones de dólares por las malas prácticas en la seguridad de los datos de sus usuarios.

El caso expuesto demostró la gran arma que resulta en la actualidad la posesión de datos personales, de modo que motivó a la comisión federal de comercio de Estados Unidos a exigir una nueva estructura de privacidad de datos en Facebook. En el contexto comunitario, la importancia de exigir una regulación armonizada en materia de protección de datos personales y adaptar a la nueva realidad, se

[6] Rosenberg, M. Condessore, N. Cadwalladr, C. (2018). How Trump Consultants Exploited the Facebook Data of Millions. *The New York Times*. Recuperado de https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

[7] Rosenberg, M. Condessore, N. Cadwalladr, C., (2018). How Trump, *op. cit.*

puso de manifiesto en la comunicación 442[8] por parte de la Comisión Europea en 2014. En ella, la Comisión además de mostrar la preocupación por la necesidad de asegurar la protección de datos e información y reducir la desconfianza acerca de las prácticas que rodean la económica digital, muestra la necesidad de innovación en la que se encuentra Europa, frente a unos EEUU pioneros y expertos en el tratamiento de los macro datos.

Viendo la transcendencia que puede suponer la gestión de datos digitales, se plantea una reforma de la antigua Ley de Protección de Datos y Seguridad. El presente trabajo pretende abordar desde los conceptos más generales del procesamiento de datos en la actualidad, hasta la implementación de la nueva regulación de protección de datos, con el fin de conocer que exigencias deben cumplir las empresas para transmitir datos personales a cualquier otra entidad, ya sea pública o privada. Así pues, este trabajo se plantea como una revisión e investigación del derecho regulador de las garantías en materia de protección de datos y conocer como es finalmente la práctica o posición de una muestra de las empresas recopiladoras de datos.

[8] COMISIÓN EUROPEA (2014). *Hacia una economía de los datos próspera.* COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES.

II. Marco teórico

Este análisis bibliográfico, como hemos visto, ira encaminado a examinar y conocer las exigencias a las que se enfrontan las empresas que dedican su actividad o que durante el desarrollo de su actividad formalizan contratos donde se comercializan datos de carácter personal, para poder crear valor en los mismos mediante el análisis Big Data.

Cabrá analizar así la Ley Orgánica de Protección de Datos Personales[9] (en adelante LOPD), promulgada en virtud del Reglamento Comunitario 2016/679 de Protección de Datos[10] (en adelante Reglamento 2016/679), que pretende regular y proteger los datos personales ante una sociedad de la información que es objeto de muchos avances desde la anterior Directiva 95/46/CE[11].

Pero antes de entrar a analizar el nuevo marco legal, cabe introducir ciertos aspectos que serán básicos y esenciales para la comprensión del mismo. En el presente título se abordarán los conceptos y aspectos sobre los que nace la necesidad de una regulación moderna adaptada a la nueva situación, así como la nueva LOPD, sus pilares fundamentales y las novedades introducidas respeto de la ley derogada.

Capítulo I. Los Datos personales y su tratamiento

El Reglamento 2016/679 determina en su artículo primero que el objeto del mismo será establecer "las normas relativas a la protección de las personas físicas

[9] Ley Orgánica 3/2018, del 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Boletín Oficial del Estado, 294. (2018).

[10] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Diario Oficial de la Union Europea, L 119. (2016).

[11] DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y 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 datos. Diario oficial de las Comunidades Europeas, L 281. (1995).

en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos"[12]. Vemos pues como el objeto de atención serán los datos personales y su tratamiento.

Datos personales, seudonimizados y anonimizados

Los datos personales son "toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente"[13]. En este sentido, como afirma Elena Gil[14] se contemplarán como datos personales todos aquellos datos que se puedan atribuir a una persona, incluyendo así una gran cantidad de información como la voz, el número de seguridad social, dirección y datos económicos.

Cabría diferenciar esta categoría expuesta de otra tipología de datos que presentan diferentes grados de identificación del sujeto, como podrían ser los datos personales seudonimizados o los datos personales anonimizados.

Mientras que en los datos personales anonimizados el sujeto es inidentificable, los datos personales seudonimizados son aquellos que pueden atribuirse a una persona física, pero que para ello requiere la utilización de información adicional. Para determinar si se dispone de los medios para conocer la identidad del sujeto, se atenderá a factores objetivos, como las tecnologías disponibles para tal fin, así como los costes y tempo que requiere. En este sentido, los datos seudonimizados deben considerarse información sobre una persona física identificable, y por lo tanto, recibirán la protección implementada por LOPD. La característica de identificable es clave para justificar la aplicación de la ley, dado que de ser considerados no identificables, pertenecerían a la categoría de datos

[12] REGLAMENTO (UE) 2016/679, *op.cit.,* art. 1.

[13] REGLAMENTO (UE) 2016/679, *op.cit.,* art. 4.

[14] Gil González, E. (2016). *Big data, privacidad y protección de datos.* Boletín Oficial del Estado. Madrid, P. 41.

anonimizados, los cuales no quedan sujetos al sistema de protección, como determina claramente el Reglamento 2016/679 [15].

Sin embargo, como más adelante se expondrá, la aparición de nuevos avances tecnológicos ha llevado a diferentes autores a la convicción de que los datos anonimizados, tratados de la manera idónea para tal fin, pueden facilitar la reidentificación del sujeto[16], y por lo tanto, atentar a su privacidad, y como consecuencia, supondría la comisión de una infracción considerada muy grave por el artículo 72 LOPD. Existen diversos procedimientos de anonimización, los cuales podrán ir desde la utilización de algoritmos de Hash o de cifrado, hasta la reducción o perturbación de datos[17].

Datos especiales

En ese espacio hacemos mención de una categoría de datos personales que recibe un tratamiento distinto, los datos especiales.

Estos se enumeran en la propia ley y se justifica su categoría dado que reciben una protección especial evitando así situaciones discriminatorias. Serán los datos que revelen información del sujeto acerca de su origen étnico o racial, sus opiniones políticas o religiosas, afiliación sindical, así como datos acerca de su salud, vida u orientación sexual. Recientemente, en aparición de la nueva regulación europea, se añaden además de otros aspectos que se verán en este título, los datos genéticos y biomédicos como datos de carácter especial.

Tratamiento de datos personales

El concepto de tratamiento hace referencia a

> Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación,

[15] REGLAMENTO (UE) 2016/679, *op.cit.*, Considerando 26.

[16] Gil González, E. (2016). *Big data op cit.*, p. 78.

[17] Agencia Española de Protección de Datos (2016). *Orientaciones y garantías en los procedimientos de anonimización de datos personales.*

> adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción[18].

Vemos como el concepto de tratamiento abarca gran cantidad de actividades, desde la simple recogida, hasta la difusión o transmisión. En este sentido, tomaremos en consideración los métodos de tratamiento que más están dando de qué hablar por sus numerosos beneficios y por su implicación tecnológica e innovadora, el análisis Big Data.

Antes pero, debemos hacer una clasificación de los mismos en dos grandes grupos, ya que esta clasificación tendrá relevantes implicaciones en virtud de la nueva legislación, más concretamente conllevara cierta implicación para el responsable del tratamiento.

La clasificación se realiza en función del grado de riesgo que comporta el tratamiento para los derechos y libertades de las personas, y las clasificaremos entre alto y bajo riesgo. Los encargados de realizar dichas clasificaciones y las consecuentes listas son las autoridades, que deberán comunicarla al Comité Europeo de Protección de Datos[19].

En el primer grupo de alto riesgo, contemplado en la lista elaborada por la Agencia Española de Protección de Datos[20] (en adelante AEPD), se contemplaran todas las actividades de tratamiento que cumpla con dos o más criterios de los establecidos en el listado, y siempre que este no se contempla expresamente en el grupo de bajo riesgo. Formaran parte de esta categoría los tratamientos que impliquen la toma de decisiones automatizadas y el uso de datos especiales, tratamientos que impliquen la utilización de nuevas tecnologías, entre otros.

En una segunda categoría nos encontramos con los tratamientos que implican un menor riesgo hacia los derechos de los interesados. La lista confeccionada por la

[18] REGLAMENTO (UE) 2016/679, *op.cit.,* art. 4.
[19] REGLAMENTO (UE) 2016/679, *op.cit.,* art. 35.4.

[20] Agencia Española de Protección de datos. (2019). *Lista orientativa de tipos de tratamiento que requieren Evaluación del Impacto Relativo a la Protección de Datos.*

Agencia Española de Protección de Datos[21] es derivado de un poder facultativo, pero que de ejecutarse, deberá ser comunicada al Comité Europeo de Protección de Datos. En ella encontramos tratamientos que se realicen bajo las directrices de las autoridades de control, o por obligación legal o interés público, e incluso el tratamiento que hagan profesionales autónomos como médicos o abogados, siempre que este no contemple ningún requisito de los contenidos en el otro listado. Se incluyen en esta categoría el tratamiento relacionado con la gestión interna de personal entre otros.

Capítulo II. Aproximación al Big Data y otras formas de tratamiento.

La aparición de las nuevas tecnologías, en el ámbito del análisis de datos, ha conllevado numerosas mejoras en cuanto a minimizar costes, tanto al acceso a la información, como al procesamiento de esta. El análisis es crucial para cualquier sector, ya sea para la selección de personal por parte del departamento de Recursos Humanos, hasta los avances en el campo de la medicina.

La introducción de nuevas tecnologías en el procedimiento de análisis de datos ha supuesto un aumento del volumen de la información, aumento de la capacidad de procesamiento de esa información, y mejora la toma de decisiones[22].

En este capítulo se tratará el fenómeno Big Data, entendido como un modo de obtención de gran cantidad de datos y procesamiento de los mismos que permita la toma de decisiones más acertadas.

¿Qué se entiende por Big Data?

La expresión Big Data hace referencia a dos fenómenos. En primer lugar, y atendiendo a la traducción literal "datos masivos" hace referencia a la gran

[21] Agencia Española de Protección de Datos. (2019). *Lista orientativa de tipos de tratamiento que no requieren Evaluación del Impacto Relativo a la Protección de Datos*.

[22] Todolí Signes, A. (2018). *La gobernanza colectiva de la protección de datos en las relaciones laborales: Big Data, creación de perfiles, decisiones empresariales automatizadas y los derechos colectivos*. Revista de Derecho Social, 69-88. P.69.

cantidad de datos que están al alcance actualmente y que pueden ser utilizados para fines muy diversos, y en segundo lugar,

> Alude también al conjunto de tecnologías cuyo objetivo es tratar grandes cantidades de información, de datos, empleando complejos algoritmos y estadística con la finalidad de hacer predicciones, extraer información oculta o correlaciones imprevistas y, en último término, favorecer la toma de decisiones[23].

Otros autores lo definen como una herramienta técnica que no solo permite ver, sino descubrir, en tanto que supone una visión transformadora que obtiene valor, de donde solo hay gran cantidad de información en bruto[24].

Este fenómeno se ha enfrentado tradicionalmente con dos grandes barreras, la incapacidad para almacenar datos suficientes, y el gran coste de procesamiento de la información. Pero esas barreras se han derribado con la innovación tecnológica contemporánea como por ejemplo el fenómeno *cloud computing*[25], el que permite almacenar gran capacidad de información, y avances en la potencia de cálculo y precisión algorítmica.

Como hemos mencionado anteriormente, los datos son en gran parte producidos por los propios sujetos voluntariamente en sus interacciones en la red, así pues creamos datos con sencillas búsquedas en la red, con *posts* en redes sociales, o con el uso del GPS.

Y no solamente se crean de ese modo, la autora Ana Garriga [26] defiende que gran parte de ellos son obtenidos gracias al *internet de las cosas*. Se trata de objetos

---

[23] Garriga Domínguez, A. (2016). Datos masivos, dispositivos de geolocalización, etiquetas y dispositivos RFID e internet de las cosas. *Nuevos retos para la protección de Datos Personales. En la Era del Big Data y de la computación ubicua.* Dykinson. Madrid. P.28.

[24] Morente Parra, V. (2019). *Big Data o el arte de analizar datos masivos.* Derechos y libertades, 225-260. P. 227.

[25] El "*cloud computing*" es un servicio que pone a dispisicion del usuario espacio virtual en el que puede almacenar y compartir grandes cantidades de datos.

[26] Garriga Dominguez, A. (2018) *La elaboración de perfiles y su impacto en los derechos fundamentales. Una primera aproximación a su regulación en el reglamento general de protección de datos de la Unión Europea*. Derechos y libertades, 107-139. P.113. La autora hace especial relevancia en que estos objetos cotidianos no son considerados "internet en las cosas" por llevar configurado un software con conexiona internet, sino que es un objeto que recopila

que forman parte de la vida cotidiana y que su conexión digital a internet hace que estén constantemente intercambiando información que será tratada como datos.

Resultará clave para comprender la esencia de Big Data, conocer sus características recogidas en tres o cinco, según el autor de referencia.

La primera característica nunca discutida es el *volumen.* Como hemos comentado anteriormente, Big Data parte de la base del análisis de tan grande cantidad de datos que es de imposible análisis por una persona. En segundo lugar, encontramos la *velocidad*, que hace referencia no a la velocidad con la que se crean, sino a la velocidad con la que fluyen para poder asegurar su tratamiento en un tiempo real.

En tercer lugar nos detenemos a la característica de la *variedad*, y es que con este sistema, se pueden analizar datos de cualquier tipo, siendo muy diverso el contenido de estos. Se puede distinguir en 3 tipos de datos según su estructura[27]. En primer lugar encontramos los datos estructurados, que serán los datos obtenidos con fuentes tradicionales, con un formato bien definido, como archivos, hojas de cálculo fundamentalmente. En segundo lugar, los semiestructurados, que son aquellos que no tienen formatos fijos pero contienen etiquetas y otros marcadores que permiten separar los elementos dato. Por último, encontramos los datos no estructurados, que conforman el 80% de los datos actuales. Estos son aquellos que no tienen una estructura uniforme, como por ejemplo audios, videos, fotos etc.

La capacidad de que esta gran variedad de datos pueda ser procesada mediante un misma tecnología, perite una ventaja muy destacada.

Además, otros autores han añadido a estas características clásicas dos más[28]. Por un lado cabe mencionar la *veracidad*. Esta característica hace referencia a la

información del uso que se hace sobre ese objeto, y lo procesa y envía. Nos ofrece un ejemplo de ese tipo de objetos, como serían las pulseras inteligentes o las "google glas".

[27] Joyanes Aguilar, L. (2013). *Big Data: análisis de grandes volúmenes de datos en organizaciones.* Alfaomega Grupo Editor. México DF.

importancia de que los datos sean de calidad y fiables, para proporcionar del mismo modo información veraz. Finalmente añaden el *valor*, la finalidad de todo esfuerzo del análisis.

Beneficios de la utilización de Big Data

En este punto analizaremos algunos ejemplos de los beneficios que ha conllevado el uso de Big Data en la sociedad actual.

Empezaremos con una aproximación al análisis de datos de la salud. Cristea Uivaru[29] los define como aquellos datos que contienen información que trata de las dolencias o enfermedades que han padecido, padecen o pueden padecer en un futuro los pacientes, además de contener información acerca de tratamientos médicos o información genética. Son datos que yacen en la esfera más íntima de la persona, y que merecen pues una especial protección. Es por ello que se clasifican en la categoría de datos de carácter personal especiales.

El tratamiento de estos datos con fines de investigación, permiten agilizar un proceso que anteriormente podía tardar años, reduciéndolo a meses, incluso días. Como afirma Federico de Montalvo[30], los algoritmos permitirán comparar una cantidad desmesurada de procesos asistenciales con mayor precisión y conocer cuáles son los tratamientos para cada una de sus enfermedades y diagnósticos. En este mismo sentido, el autor explica que los resultados obtenidos tendrán mayor solidez dado que se basarán en una población mayor. Así pues se manifiesta no

---

[28] Gil González, E. (2016). *Big data, op. cit.* La autora añade una sexta característica, la *visualización*. La autora asegura que para poder comprender los datos y tomar decisiones es fundamental visualizarlos, y nos ilustra su explicación con un ejemplo, según el cual si se obtiene una predicción de los crímenes que se cometen después de un partido de futbol, y donde, y en vez de analizar las coordenadas se sitúan en el mapa, la visualización será mucho más favorecedora a la comprensión de los resultados.

[29] Cristea Uivaru, L. (2018). *La protección de datos de carácter sensible: Historia Clínica Digital y Big Data en Salud.* J.M. Bosch Editor. P. 46.

[30] De Montalvo Jääskeläinen, F. (2019). *Una reflexión desde la teoría de los derechos fundamentales sobre el uso secundario de los datos de salud en el marco del Big Data*. Revista de derecho político nº 106, 43-75. P. 47. El autor apunta en este artículo que los datos clínicos no deben ser comprendidos como meros informadores de un proceso asistencial, y que se convierten en una fuente de conocimiento y avance en la Medicina y Biología.

solo la importancia de la gestión de los datos para la realización del Historial Clínico, sino para un fin secundario que será la investigación posterior.

Otro ejemplo de un uso claramente beneficioso del análisis de datos personales se puede encontrar en la organización de las ciudades, más concretamente en la gestión del tráfico de los núcleos urbanos, las llamadas *Smart cities.* La movilidad representa un factor clave para el desarrollo de la vida social y económica de muchas ciudades. Para que este desarrollo sea posible es necesaria una correcta planificación de los diferentes medios de transportes. Debemos poner en relieve que

> la movilidad se ve necesariamente condicionada por las dinámicas sociales, que cambian a lo largo del tiempo y que en parte dependen de otros factores de cambio, como la planificación urbana, las inversiones industriales y comerciales o la disponibilidad de servicios públicos.[31]

A partir del análisis de la oferta y la demanda en los medios de transporte público, junto a un mapeo constante de los recorridos y tránsito, se puede gestionar de forma más eficiente que nunca la red de transporte urbana. Pero ello implicará la recogida y elaboración de información de diversos sujetos, a los que se incluirán algunas administraciones públicas.

Helena Villarejo, profesora de Derecho Administrativo, asegura que esta cesión de datos es beneficiosa para todos los intervinientes[32]; las administraciones que podrán mejorar la oferta de servicios de transporte, las empresas de transporte que podrán analizar los datos para planificar sus servicios y modelos de negocio, y los usuarios, que recibirán un servicio más individualizado y permitirá la compra de billetes online.

Y en esta misma dirección también se pronunció el Parlamento Europeo en 2014, apostando por un sistema de Smart City mediante el aprovechamiento de las

[31] Mantelero, A. (2015). *Smart cities, movilidad inteligente y protección de los datos personales.* IDP. Revista de Internet, Derecho y Política nº 21, 37-49. P. 39.

[32] Villarejo Galende, H. (2015). *Smart cities: una apuesta de la unión europea para mejorar los servicios públicos urbanos*. Revista de Estudios Europeos nº 66, 25-51.

Tecnologías de la Información y Comunicación para aumentar la eficacia, reducir costes y mejorar la calidad de vida en las ciudades. Y por ello, se prevé que el programa Horizonte 2020, el cual daba respaldo económico para el desarrollo de *Smart Cities*, contó con una financiación prevista de 16.000 millones de euros aproximadamente.

Una vez más, encontramos que el uso de Big Data ha entrado en el ámbito público para ofrecer una mejor servicio de seguridad ciudadana y gestión de emergencias. Y es que como afirma Antonio Pires[33], el futuro de la seguridad publica más eficiente pasa por la capacidad de recopilar y analizar la información. Asegura que con el correcto análisis de los grandes volúmenes de datos disponibles, se podrán abordar las operaciones de seguridad con una menor cantidad de recursos. A partir de la visualización de los datos procedentes de la ciudad, el centro de mando inteligente puede proporcionar a las autoridades municipales una respuesta más eficaz y rápida, incluso anticiparse a los problemas que puedan surgir.

El autor ejemplifica los beneficios que desprenden la gestión de datos personales para ofrecer un sistema más eficaz de seguridad, exponiendo los casos de Rio de Janeiro y el ministerio de justicia de Reino Unido.

Para afrontar los acontecimientos que tenían lugar en la capital, la copa del mundo de 2014 y los juegos olímpicos de 2016, se puso en marcha el Centro inteligente de Operaciones. Este centro recibe datos de toda la ciudad y hace un seguimiento y análisis de los mismos, lo que permite una agilidad ante la gestión de actos de delincuencia o de incidentes de emergencia.

Con un fin similar, el ministerio de justicia de Reino Unido empezó un proyecto dirigido a comprender y predecir el comportamiento de los infractores o reincidentes, lo que requirió un trabajo de recopilación de todos los datos archivados en el ministerio y riguroso análisis con indicadores acerca de estado de ánimo, consumo de alcohol entre otros.

[33] Pires, A. (2014). *Una gestión inteligente de la seguridad pública.* Revista de obras públicas nº 3550: Smart cities, 45-48.

Análisis de los aspectos conflictivos

El consentimiento, como veremos en el capítulo tercero, es un elemento esencial para el trato legítimo de los datos.

Establece la directiva que para que el tratamiento sea legítimo, debe contar con una causa justificativa de tipo legal o necesaria, o contar con el consentimiento del propio interesado. Vemos pues como el consentimiento se manifiesta como un instrumento fundamental para la protección de los datos. "Este permite respetar la autonomía de los individuos sobre la toma de sus decisiones"[34].

Este consentimiento, entendido como "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen"[35], puede verse condicionado. En numerosas ocasiones, las nuevas tecnologías como dispositivos móviles, aplicaciones o los servicios de localización, hacen uso de políticas que aunque cumplen con la normativa de protección de datos, reciben un consentimiento dudosamente voluntario.

Y es que en muchas ocasiones, esas políticas de privacidad son trasladadas a los usuarios como unas condiciones contractuales creadas unilateralmente, y de modo que el usuario debe aceptarlas, o no acceder al contenido deseado. Además, se hace evidente la desinformación del interesado en cuanto al posterior tratamiento o de los derechos que goza. En definitiva, se limita la libertad de acción del interesado.

Por otro lado, el método de Big Data procesa la información de forma totalmente objetiva a partir de algoritmos y estadísticas, pero ¿qué calidad de resultados obtiene?

Diferentes autores han expuesto la posibilidad de que, de no ser revisados atentamente los resultados o conclusiones obtenidas, hay gran margen de error en

[34] Gil González, E. (2016). *Big data, op. cit.*, p. 56.

[35] REGLAMENTO (UE) 2016/679, *op. cit.*, art. 4.

las correlaciones hechas. Adrián Todolí [36] nos expone un supuesto en el que se ve claramente el error por no atender a cuestiones subjetivas. Plantea un hipotético supuesto en el que un selector de personal de una empresa de IBEX 35 esté buscando una persona para actuar como consejero. Mediante el análisis de los datos precedentes y dado que estadísticamente se comprueba que 9 de cada 10 consejeros son hombres, el análisis confirmaría que un hombre es más probable que encaje mejor en el puesto.

Otro claro ejemplo es el proporcionado por Elena Gil[37]. La autora plantea que el análisis puede mostrar relaciones entre variables que son fruto de la casualidad, y no de la causalidad. Para confirmar su convicción, expone un análisis realizado por el matemático polaco J. Neyman en 1952. Este observó que en las regiones en las que habitaban más cigüeñas, se daban más nacimientos, parecía haber una relación entre ambas variables. Pero esto no explica que haya una relación causal, por eso el autor explica que la conexión entre ambas variables se justifica con una tercera variable, que es la calidad de la cosecha. Vemos pues como las relaciones que se puedan observar a partir del análisis de gran cantidad de datos, deben ser observadas y revisadas con perspectiva.

Otro producto de la aplicación del tratamiento de datos que entra en conflicto con los derechos del interesado, es la toma de decisiones automatizadas. En ocasiones, la toma de decisiones automatizadas puede crear situaciones de discriminación o indefensión para el interesado. Todolí[38] nos ofrece de nuevo un ejemplo en el que se refleja claramente esta actividad, donde la intervención humana es prácticamente inexistente.

El supuesto se contextualiza en un departamento de recursos humanos. En este hacen uso de la inteligencia artificial para analizar perfiles y minimizar el coste temporal que requiere analizar personalmente los perfiles de los candidatos que se inscriben en una oferta laboral. Así pues, filtran los perfiles obtenidos con

[36] Todolí Signes, A. (2018). *La gobernanza op. cit.*, p. 74

[37] Gil González, E. (2016). *Big data op cit.*, p. 38

[38] Todolí Signes, A. (2018). *La gobernanza op. cit.*, p. 76 y ss.

distintos criterios, ya sea nota media académica, universidad de procedencia u otros indicadores. La decisión de eliminar candidatos sin una intervención humana se hace evidente.

Seguidamente nos expone un supuesto en el que la decisión automatizada resulta menos evidente. En este caso el departamento plantea la posibilidad de un despido. El perfil del empleado ha sido detectado por el resultado de un análisis que afirma la obtención de una mala reputación online. El despido no se realizara directamente por el sistema informático, sino que será comunicado al empleado por el responsable de recursos humanos. Este escenario, ¿es producto de una decisión automatizada? La protección que hace el legislador frente a estas situaciones para asegurar los derechos del interesado se abordara nuevamente en el próximo capítulo.

Por último, debemos mencionar la demostrada capacidad de incidir en el comportamiento humano si se aplica una buena estrategia a partir de los resultados del análisis de datos. Este supuesto puede verse reflejado claramente en el mundo del marketing.

El marketing ha sido definido por numerosos expertos desde posiciones muy diversas, contemplándolo como una actividad destinada a comunicar, crear e intercambiar ofertas que tienen valor para los clientes, como la actividad destinada a identificar y satisfacer necesidades humanas, actividad de administrar las relaciones con los clientes etc. H. Silva lo define como "un proceso de planeación que busca la satisfacción total de los consumidores mediante un pronóstico acertado de lo que necesitan y desean de manera puntual y precisa"[39]. En los recientes años se ha popularizado el conocido *data-driven marketing* o Big Data Marketing, lo que no es más que "la utilización de la información (data) de los clientes para conducir apropiadamente los esfuerzos de las comunicaciones de marketing"[40].

[39] Silva Guerra, H. González Ortiz, J. Martínez Díaz, D. Giraldo Oliveros, M. Juliao Esparragoza, D. (2014) *Marketing: conceptos y aplicaciones.* Universidad del norte, Colombia.

[40] Goyzueta Rivera, S. (2015). *Big Data Marketing: una aproximación.* Perspectivas nº 35, 147-158.

El marketing ha evolucionado a lo largo del tiempo en función del comportamiento social y las innovaciones tecnológicas. Y es en la actualidad donde el comercio electrónico y las tecnologías como el Big Data han hecho marcar un avance en materia de marketing. A partir del análisis de datos, se aporta una nueva oportunidad para las empresas y sus departamentos de marketing, que podrán obtener información valiosa de sus clientes y futuros clientes en cuanto a gustos, preferencias e intereses se refiere. Y esta información, como es de suponer, se obtendrá mediante diversos canales, redes sociales, internet de las cosas etc. También tiene incidencia en la elaboración de estudios de mercado. Estos ya no se deberán necesariamente realizar con una muestra de la población, ahora pueden hacerse con todos los datos de la red y con costes menores.

Así pues, gracias a la aparición de las nuevas tecnologías y el estudio de los datos masivos, se plantean estrategias de marketing mucho más personalizadas, dado que se conoce el comportamiento de compra y consumo del cliente, información de uso redes sociales. Esta información permite crear la red de influencia, y como consecuencia, una mayor capacidad de incisión en el comportamiento del cliente.

Capítulo III. Revisión de la legislación aplicable comunitaria y estatal

En el presente capítulo se analizara la nueva legislación tanto comunitaria como estatal en materia de protección de datos, la cual trata de encontrar el equilibrio entre la protección de los datos personales y la libre circulación de los mismos dentro de la unión.

Legislación comunitaria: el Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos.

El Reglamento 2016/69 aprobado en 27 de abril de 2016, tiene por objetivo crear un espacio de libertad, seguridad y justicia dentro de la unión para favorecer el progreso económico y social, asegurando asimismo el bienestar de las personas.

El derecho a la protección de datos, se contempla por la Unión como un derecho fundamental, pero este no es de carácter absoluto y por lo tanto debe convivir en equilibrio con otros derechos, con arreglo al principio de proporcionalidad.

Además, la UE es claramente consciente del desarrollo económico que proporcionaría un sistema de leyes que fomenten una económica de datos segura, "dando lugar a más oportunidades de negocio y un aumento de la disponibilidad de conocimientos y de capital, en particular para las pymes, así como servir de estímulo más eficaz para la investigación y la innovación pertinentes"[41].

El articulado de interés para la presente investigación se dividirá en tres partes principales. En primer lugar, los principios que regirán el tratamiento de datos personales, seguidamente los derechos que se reconocen al interesado, posteriormente la introducción de las diversas figuras que intervienen en el tratamiento.

Todo tratamiento que se realice sobre datos personales debe ser lítico, leal y transparente. Los datos deben ser recogidos para fines determinados, y solo se permitirá el ulterior tratamiento siempre que este esté relacionado con el fin inicial, o con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. Los datos deberán ser limitados y pertinentes al fin perseguido, además de exactos y actualizados, debiendo existir la posibilidad de suprimir o rectificar aquellos que no tengan relevancia.

En cuanto al plazo de conservación de los datos, este deberá ser el necesario para el fin del tratamiento, y posteriormente se podrán mantener exclusivamente para atender a los fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. Estos deberán ser conservados y tratados garantizando su protección.

Deteniéndonos un poco en la licitud del tratamiento, se agrupan las causas que legitiman el tratamiento de datos en tres; en primer lugar el consentimiento del interesado, en segundo lugar una causa de carácter imperativo, es decir, cuando es

[41] COMISIÓN EUROPEA, *Hacia una economía op. cit.*, p. 6.

necesario para el cumplimiento de un contrato o una obligación legal para el responsable del tratamiento[42], y finalmente para fines de interés público. Estos dos últimos grupos son denominados en el reglamento como *otras bases legitimas conforme al Derecho de la Unión o de los Estados miembros*. El consentimiento es la clave y el principal indicador para determinar si un tratamiento es licito, siempre que no se encuentre basado en una obligación o supuesto de los comentados.

> 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[43].

Se enciende que este podrá consistir en marcar una casilla de un sitio web, y debe darse por todos los tratamientos que persigan el fin. Quedan fuera de lo establecido por el Reglamento las casillas ya marcadas y el silencio entendido como consentimiento. Además, "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."[44]

Interesa destacar que el Reglamento 2016/679 legitima al Responsable del tratamiento para tratar datos personales en su interés legítimo, siempre que este no prevalezcan con los intereses o derechos y libertades del interesado en materia de protección de datos, y contempla los fines de mercadotecnia como intereses legítimos.

---

[42] En este grupo se contemplarán tres condiciones de licitud reguladas en el artículo 6 del reglamento. Los apartados b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales, c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento, y f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

[43] REGLAMENTO (UE) 2016/679 *op. cit.*, Considerando 32.

[44] REGLAMENTO (UE) 2016/679 *op. cit.*, Considerando 42.

En cuanto al principio de transparencia, este implica que toda la información que se dirija al público o al interesado en cuanto a la protección de sus datos, debe ser fácilmente accesible y de fácil comprensión, consiguiéndose con el uso de un lenguaje claro y sencillo. El principio de transparencia también consistirá en informar al interesado de sus derechos reconocidos en virtud del Reglamento 2016/679 y fórmulas para ejercerlos. Los principales derechos reconocidos a los interesados son los siguientes:

- Derecho de acceso del interesado.

Este derecho consiste en facultar al interesado para conocer si su datos se están tratando, y de ser si, conocer del responsable información entorno al fin que persigue, las categorías de datos, los destinatarios si los hubiera, el origen de los datos si no fueran dados por el interesado etc. El interesado recibirá copia de la información solicitada, y el responsable podrá percibir un precio por el coste administrativo. Además, como se establece en la Resolución de la AEPD, la información podrá ser enviada por correo electrónico *y utilizar algún sistema de encriptado para salvaguardar el contenido.*[45]

- Derecho a la rectificación.

El interesado podrá exigir la responsable la modificación de datos personales que sean inexactos o equívocos. En tal caso, el responsable tendrá la obligación no solo de realizar los cambios, sino que deberá además notificar tales cambios[46] a quienes se les hayan comunicado los datos.

- Derecho de supresión (derecho al olvido).

El derecho al olvido responde a la pretensión del interesado de obtener la supresión de sus datos personales por parte del responsable sin dilación alguna cuando concurra alguna de las causas tasadas por el Reglamento[47]. Asimismo, se

[45] Agencia Española de Protección de Datos. Resolución nº R/00657/2019 de 3 de febrero de 2020.

[46] Garriga Dominguez, A. (2016) Principios de calidad de los datos y derechos de los interesados: el núcleo esencial del derecho a protección de datos personales en la LOPD. *Nuevos retos para la protección de Datos Personales. En la Era del Big Data y de la computación ubicua.* P. 212.

añade la obligación del responsable no solo de suprimir dichos datos, sino que de haberlos hecho públicos, deberá tomas las medidas razonables para comunicar la supresión a los demás responsables que estén tratando los datos.

Sin embargo, este derecho no es absoluto, y no será posible cuando el tratamiento sea necesario para el ejercicio del derecho a la libertad de expresión e información, para el cumplimiento de obligaciones legales de los responsables, razones de interés público y para la formulación o el ejercicio o la defensa de reclamaciones. Es evidente la colisión que se produce entre el derecho a la supresión y otros derechos fundamentales como la libertad de expresión o de información, y por eso los tribunales se han pronunciado en diferentes ocasiones, informando que

> hay que buscar un justo equilibrio entre el interés legítimo de los internautas en tener acceso a la información en una búsqueda que verse sobre el nombre de una persona y los derechos fundamentales de la misma y puede resultar que, por razones concretas, como el papel desempeñado por el mencionado interesado en la vida pública, la injerencia en sus derechos fundamentales está justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información de que se trate.[48].

- Derecho a la limitación del tratamiento.

Mientras se estén gestionando las solicitudes de rectificación y suspensión, y en otros supuestos expresados en el artículo 18 del Reglamento, el interesado podrá limitar el tratamiento de sus datos personales.

- Derecho de portabilidad de datos.

---

[47] REGLAMENTO (UE) 2016/679, *op. cit.*, art. 17. Algunas de las circunstancias que motiven la supresión son: que los datos personales ya no sean necesarios en relación al fin por el que fueron recogidos, cuando el interesado retire su consentimiento, cuando el interesado se oponga al tratamiento y no exista una obligación legal para mantenerlo, cuando se tratan los datos de forma ilícita, entre otras.

[48] Recurso 509/2017 de la Sección 1ª, sala de lo contencioso administrativo de la Audiencia Nacional. Fundamento jurídico 4.

Se reconoce el derecho al interesado de solicitar la portabilidad de sus datos personales ya estructurados a otro responsable de tratamiento cuando el tratamiento este basado en el consentimiento, o el tratamiento se realicen por medios automatizados.

- Derecho de oposición y decisiones individuales automatizadas.

El reglamento reconoce la interesad el derecho a oponerse al tratamiento de sus datos, una vez fueron cedidos, cuando este tratamiento este basado en el mero consentimiento del interesado.

Por su parte, el responsable del tratamiento podrá oponerse a esta pretensión cuando acredite interés legítimo en el tratamiento. Anteriormente se anunció que el Reglamento consideraba la mercadotecnia como interés legítimo, pero debemos destacar que en su articulado, se dispone que "cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles"[49].

Además se dispone que el interesado tenga derecho a no ser objeto de decisiones automatizadas cuando estas produzcan efectos jurídicos contra él.

El responsable del tratamiento deberá atender a las solicitudes sin dilación indebida, y en el plazo máximo de un mes. De no ser así, deberá justificar su demora.

Como afirma la sala de lo contencioso administrativo de la Audiencia nacional,

> el derecho fundamental a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho a la intimidad, con

[49] REGLAMENTO (UE) 2016/679, *op. cit.*, art. 21.

el objeto de garantizar a la persona un poder de control sobre sus datos personales[50].

El Reglamento 2016/679 regula tres figuras entrono al tratamiento, estos son el responsable del tratamiento, el encargado del tratamiento y el delegado de Protección de Datos.

El responsable del tratamiento se define como "persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento"[51]. Este sujeto deberá aplicar las medidas técnicas y organizativas[52] apropiadas teniendo en cuenta la naturaleza de los datos y los fines del tratamiento, para poder demostrar que el tratamiento es de conformidad con el reglamento, es decir, exige una actitud proactiva. Además deberá tener un registro de las actividades de tratamiento que se realiza bajo su control.

Por otro lado, el encargado del tratamiento es definido como "persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento"[53]. Este debe ofrecer garantías suficientes para aplicar las medidas técnicas y organizativas con tal de que el tratamiento se realice conforme lo establecido en el Reglamento. En el supuesto en que el encargado pretenda recurrir a otro encargado para el tratamiento, deberá recibir la autorización previa y escrita del responsable.

El encargo u orden de tratamiento del responsable al encargado deberá formalizarse mediante un contrato[54] o acto jurídico, donde se establezca el objeto, la duración la naturaleza y la finalidad del tratamiento, el tipo de datos a tratar,

[50] Recurso 509/2017 de la Sección 1ª, sala de lo contencioso administrativo de la Audiencia Nacional.

[51] REGLAMENTO (UE) 2016/679, *op. cit.*, art 4.

[52] Las medidas técnicas y organizativas para garantizar la seguridad de los datos personales a que se refiere el reglamento, son principalmente las establecidas en el artículo 32, la seudonimización y cifrado, sistemas de tratamiento que aseguren la confidencialidad, integridad, disponibilidad, capacidad para restaurar la disponibilidad y el acceso a los datos, y un proceso de verificación y valoración de la eficacia de las medidas técnicas y organizativas.

[53] REGLAMENTO (UE) 2016/679, *op. cit.*, art. 4.

[54] Se adjunta mediante Anexo I un ejemplo de contrato entre responsable y encargado.

entre otras estipulaciones imperativas que contempla el Reglamento en su artículo 28.

A ambas figuras se les obliga a notificar a la autoridad de control cualquier violación de la seguridad de los datos en el menor tiempo posible, y a notificar al interesado si la violación supone un riesgo para él.

Finalmente se introduce la figura del delegado de protección de datos. Este se contempla como "una persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos"[55] que deberá ser designado por el responsable y el encargado cuando el tratamiento se lleve a cabo por una autoridad u organismo púbico, cuando se haga tratamiento que requiera observación habitual de interesados a gran escala, o se traten gran cantidades de datos especiales. En los demás casos, se contempla la designación de un delegado de protección de datos como un poder facultativo. Sus funciones serán principalmente se asesoramiento a responsable y encargado, así como demás empleados, supervisar el cumplimiento efectivo de las disposiciones del Reglamento 2016/679, asesorar en la elaboración de las evaluaciones de impacto.

Esta figura mediara entre el responsable y encargado y la autoridad de control, aunque podrá formar parte de la plantilla de la entidad tratadora de datos o desempeñar sus funciones en virtud de un contrato de servicios.

Haciendo un último análisis de la legislación comunitaria, esta también contempla la creación de códigos de conducta y certificación, la creación y supervisión de los cuales se atribuye a los estados miembros, las autoridades de control y el comité y la comisión.

Además se contemplan las disposiciones específicas para los supuestos de transferencias de datos personales a terceros países u organizaciones internacionales. En estas se fijan unos principios de protección, según los cuales, se permitirá la transferencia de datos para su tratamiento a terceros países siempre

[55] REGLAMENTO (UE) 2016/679, *op. cit.*, Considerando 97.

y cuando la Comisión haya decidido y comprobado que el en el país de destino se garantiza un nivel de protección de datos adecuado[56].

Finalmente se establecen las funciones y poderes de la autoridad de control, que será de creación de los estados miembros, y el régimen de responsabilidad y sanción ante el incumplimiento del Reglamento 2016/679.

Legislación estatal: Ley Orgánica 3/2018 de Protección de Datos personales y garantía de los derechos digitales.

Si bien el nuevo Reglamento 2016/679 tuvo eficacia y aplicación directa sobre los estados miembros a partir del 25 de mayo de 2018, los Estados Miembros contaron con un plazo de dos años aproximadamente para adaptar su legislación estatal a las nuevas directrices en materia de protección de datos y libre circulación de estos.

En este sentido, el Parlamento español aprobó y publicó el 6 de diciembre la Ley Orgánica 3/2018 de Protección de datos y Garantía de los Derechos Digitales[57]. A continuación se analizará esta ley, fijándose en los preceptos que son más que una mera transposición del Reglamento Europeo.

En primer lugar y destacando las introducciones que se encuentran en la nueva LOPD española, destacamos la tutela de los derechos en protección de datos de las personas fallecidas. Partiendo de la base que se establece que la LOPD no será de aplicación a las personas fallecidas[58], en su artículo 3 se contempla la legitimación de los familiares del fallecido, para solicitar al encargado o responsable del tratamiento acceso a los datos de la persona fallecida y, en su

[56] El reglamento establece, sin embargo, que dicha transferencia no necesitara de una autorización específica. El trabajo de la comisión finalizara con un acto de ejecución, y este se someterá revisión periódica cada 4 años. Cuando no se haya obtenido dicho acto, el encargado y responsable deberán ofrecer garantías suficientes y que los interesados cuenten con derechos exigibles.

[57] Cabe hacer mención del Real Decreto Ley 5/2018, de 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, que se contempla como una norma transitoria hasta la creación de la necesaria Ley Orgánica, y que abordara materias necesarias pero siempre respetando el orden constitucional y la reserva de ley orgánica. El real decreto Ley 5/2018 abordó temas referentes a la actividad de la Agencia Española de Protección de Datos, así como el régimen sancionador principalmente.

[58] Ley Orgánica 3/2018, *op. cit.*, art. 2.2.b)

caso, su rectificación o suspensión[59]. En caso de tratarse de menores, la legitimación se extenderá al Ministerio Fiscal.

Seguidamente se transponen del Reglamento 2016/679 los principios del tratamiento y los derechos de los interesados. Se contempla como en el reglamento lo que algunos autores denominan información por capas, "esta norma prevé la posibilidad de suministrar al afectado únicamente la información básica, e indicar una dirección electrónica u otro medio que permita a dicho afectado acceder a la restante información de forma sencilla e inmediata"[60]

Se marcan las distinciones y funciones de las tres figuras comentadas, y cabe detenerse en el Delegado de protección de datos. La LOPD determina que deberá ser designado para los supuestos previstos en el Reglamento 2016/679, y añade supuestos nuevos. Se determina la obligación de designar un delegado a las entidades: colegios profesionales, centros educativos, entidades que exploten redes y presten servicios de comunicaciones electrónicas, entidades dedicadas a la creación publicitaria y comercial, entidades financieras y aseguradoras entre otras.

En cuanto a los códigos de conducta, la LOPD determina que estos deberán ser aprobados por la AEPD, o la autoridad autonómica competente. La certificación en su caso, se realizará por la Entidad Nacional de Acreditación, y comunicara las concesiones denegaciones o revocaciones a la AEPD.

A continuación se contempla la autoridad de control, la AEPD. Esta es definida como

> una autoridad administrativa independiente de ámbito estatal, de las previstas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, con

[59] El interesado, sin embargo, puede eliminar esas facultades reconocidas a sus familiares, haciendo mención expresa en vida.

[60] Minero, G. (2019). *Nuevas tendencias en materia de protección de datos personales. La nueva Ley Orgánica y la jurisprudencia más reciente.* Anuario jurídico y económico. Núm. 52, 125- 148. P. 131.

> personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones[61].

Entre las funciones de la AEPD, destacan principalmente la de investigación y la realización de planes de auditoria preventiva. Además también tendrá potestad de regulación, es decir, dictar disposiciones que fijen criterios de actuación.

La LOPD recoge detalladamente todos aquellos hechos que pueden constituir infracción por no respetar las normas recogidas en el Reglamento 2016/679 y en la Ley Estatal, y las clasifica en leves, graves y muy graves y se establece la sanción[62] que va aparejada a cada infracción. Además de esa sanción administrativa, el Reglamento 2016/679 prevé la imposición de una indemnización al responsable dirigida al perjudicado. Sin embargo, algunos autores como P. de Miguel Asensio[63] critican la falta de coordinación entre la tutela civil y la supervisión administrativa.

Modificaciones introducidas por la nueva ley

El nuevo marco legislativo en materia de protección de datos tanto a nivel comunitario como estatal ha supuesto una gran innovación. En el presente apartado se intentará puntualizar y remarcar los aspectos modificados o introducidos por la nueva ley.

En primer lugar, destacamos la modificación que sufre el requisito del consentimiento. La Directiva 95/46/CE no exigía un consentimiento expreso, por lo tanto se permitían las casillas ya marcadas o consentimiento por inacción, lo que hacía que el titular de los datos no fuera consciente de que sus datos fueran

---

[61] Ley Orgánica 3/2018, *op. cit.*, art 44.

[62] La sanción administrativa y su cuantía se regula en el Reglamento 2016/679, pudiendo llegar a ser las multas de hasta 20.000.000€, o tratándose de una empresa, de máximo el 4% del volumen de negocio total anual del ejercicio financiero anterior. Sin embargo, los estados miembros podrán regular nuevas infracciones que no estén contempladas en el Reglamento.

[63] Miguel Asensio, P.A. (2017). *Competencia y derecho aplicable en el Reglamento General sobre Protección de datos de la Unión Europea*. Revista Española de Derecho Internacional, 75- 108. Recuperado de http://bibliotecaculturajuridica.com/EDIT/1665/competencia-y-derecho-aplicable-en-el-reglamento-general-sobre-proteccion-de-datos-de-la-union-europea.html/

recabados. El nuevo Reglamente exige claramente un consentimiento libre, especifico, informado e inequívoco.

En cuanto a los derechos de los interesados, la nueva legislación introduce nuevos derechos, como el derecho de portabilidad y el derecho a la limitación del tratamiento, y regula de una forma mucho más extensa el derecho a supresión (derecho al olvido).

En la nueva legislación sin embargo, se expresan con más claridad las causas que motivan le ejercicio y el alcance de tal derecho. Con lo que se refiere al alcance, es destacada la Sentencia del Tribunal de Justicia en el asunto C-131/12, donde la Audiencia Nacional plantea unas cuestiones prejudiciales acerca del derecho al olvido en los motores de búsqueda en el caso más conocido como Spain versus Google. Esta establece que

> para respetar los derechos que establecen estas disposiciones, siempre que se cumplan realmente los requisitos establecidos en ellos, el gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de estas páginas web.[64]

Otra novedad que se refleja en el Reglamento 2016/679 y que tendrá fuertes implicaciones para el encargado y responsable del tratamiento es la obligación de una responsabilidad proactiva, que se manifiesta a lo largo del texto legislativo. Eso se traduce en la necesidad de que los responsables del tratamiento analicen los datos que tratan, de qué forma y para que finalidad. A partir de ahí, deberán establece medidas para asegurar el cumplimiento del Reglamento 2016/679, en definitiva, “este principio exige que las organizaciones tengan una actitud

[64] Sentencia del Tribunal de Justicia (Gran Sala) de 13 de mayo de 2014 (petición de decisión prejudicial planteada por la Audiencia Nacional — España) — Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González. (Asunto C-131/12)

consciente, diligente i proactiva ante todos los tratamientos de datos personales que se lleven a cabo"[65].

De acuerdo con esta exigencia de responsabilidad proactiva, se establece la necesidad de realizar una evaluación de impacto relativa a la protección de datos de forma previa al tratamiento, cuando sea probable que este, entrañe un alto riesgo para los derechos y libertades de las personas, y siempre si hace uso de nuevas tectologías.

Finalmente, se introduce en el Reglamento la figura del delegado de protección de datos. Anteriormente las funciones del delegado se realizaban por parte del responsable del tratamiento, o por el encargado de protección de datos. Vemos como esta figura era totalmente potestativa, dado que sus funciones podían ser realizadas simplemente entre el responsable del tratamiento en comunicación directa con la autoridad de control.

[65] Autoritat catalana de Protecció de Dades (2020). *Principals novetats del RGPD*. Recuperado de https://apdcat.gencat.cat/ca/documentacio/RGPD/novetats/

III. Objetivos y metodología

Este trabajo parte de la situación actual donde existen numerosas entidades recopiladoras o receptoras de datos, que ceden o transfieren los mismos a otras para su posterior análisis.

Este Título se dedicara a analizar y recopilar las obligaciones o responsabilidades que se exigen a las entidades que como hemos mencionado, transfieren datos. Así pues, contextualizaremos el supuesto dentro del territorio comunitario para poder acudir a la legislación Europea, y acotando más el campo de análisis, situaremos tanto a las entidades intervinientes como a las personas físicas que ceden los datos dentro del territorio Español.

A continuación se determinará con concertación las obligaciones que debe cumplir la primera entidad interviniente, la receptora de datos para transferirlos, y en segundo lugar se analizarán las exigencias de aquellas empresas que los han recibido y se dedican al análisis de datos, buscando aumentar la efectividad de campañas publicitarias y decisiones empresariales.

Capítulo I. Implicaciones de la nueva legislación para la transmisión o cesión de datos.

El acto de comunicar datos mediante su transmisión, difusión o cualquier forma habilitadora de acceso, es concebido por el Reglamento 2016/679 como un simple tratamiento de datos.

A lo largo del Reglamento 2016/679, concebimos tres tipos de transmisión diferentes. En primer lugar, se regula la transmisión de datos de un país de la unión a un tercer país u organización internacional, y como ya se ha expuesto en el título segundo, se exigen en este ámbito diferentes garantías en forma de autorización.

Trato distinto es el que reciben las transmisiones de datos dentro de la unión. El Reglamento no exige garantías explicitas para tal tipo de tratamiento,

simplemente se deberían cumplir las prerrogativas para el caso de que el tratamiento sea de alto riesgo, lo cual se analizará más adelante.

En la transmisión de datos dentro de la unión, el reglamento menciona un supuesto en especial. En su considerando 48, la Comisión aclara que la transmisión de datos personales entre entidades de un mismo grupo empresarial, puede suponer un interés legítimo para los responsables de las empresas que conforman el grupo, en tanto que respondan a fines administrativos.

Así pues, parece que el reglamento permite la transmisión de datos personales dentro de la unión, sin exigir garantías específicas al tratarse de tal tratamiento. Esto responde a la voluntad clara y manifestada en reiteradas ocasiones a lo largo del texto reglamentario además de otras comunicaciones, como la COM (2014), de facilitar la inversión en nuevas herramientas, sistemas y procesos basados en los datos, y facilitar el crecimiento de un mercado único digital.

Legitimación del tratamiento

Partiendo de esta premisa, se entiende que la primera de las obligaciones que concierna a la primera entidad, es la necesidad de obtener el consentimiento del interesado. Este será la principal base legal que supondrá la licitud del tratamiento.

En este punto cabe destacar la necesidad de aclaración de ciertos aspectos de dicho artículo. En su apartado primero letra F, se dispone que el tratamiento será lícito cuando 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"[66].

Se dispone que constituirá interés legítimo para el responsable del tratamiento será en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información, y la seguridad de los servicios conexos ofrecidos. Además, se expone también que existirá interés legítimo del

[66] REGLAMENTO (UE) 2016/679, *op. cit.,* art 7.1.f

responsable, cuando el tratamiento sea para fines de marketing, o prevención de fraude. El interés legítimo no podrá prevalecer ante los interesas y derechos del interesado.

Parece desprenderse pues que la transmisión de datos no constituye interés legítimo, y por lo tanto, salvo que no sea necesario por alguna de las causas restantes enumeradas en el artículo 6, deberá contar con el consentimiento del interesado.

El consentimiento, atendiendo a los principio del tratamiento, deberá ser dado para unas finalidades concretas. Así pues, no será posible la recogida de datos para un fin, pero el posterior tratamiento con finalidad de distinta naturaleza. Puede interpretarse que la finalidad de transmitir a un tercero los datos deberá ser aceptada por el interesado. Las finalidades podrán ser diversas, pero deberán ser todas consentidas.

Registro de actividades de tratamiento

Como se ha comentado anteriormente, el nuevo Reglamento exige una actitud por parte del responsable y encargado del tratamiento proactiva. Para ello, encontramos varias obligaciones que trataran de demostrar la diligencia en el tratamiento y el cumplimiento de los preceptos del reglamento.

La primera obligación se encuentra en el artículo 30 y consiste en la elaboración, por parte del responsable y en su caso el encargado de tratamiento, de un registro de las actividades de tratamiento que se elaboren bajo su responsabilidad. En él se expresara de forma detallada entre otros asuntos, información de responsable del tratamiento, encargado de tratamiento y delegado de protección de datos, fines del tratamiento, categorías de interesados y datos, y tratamiento realizado.

Es de especial relevancia para nuestro caso de estudio, la obligación de hacer constar en el registro los destinatarios a quien serán comunicados los datos, ya sea a terceros países y organizaciones internacionales o no.

Este registro será de obligado cumplimiento para las organizaciones que empleen más de 250 personas, todas aquellas que realicen un tratamiento

considerado de riesgo para los derechos y libertades de los interesados, y aquellas que traten datos especiales o de condenas e infracciones penales. El registro deberá ser puesto a disposición de la autoridad de control si así lo solicita.

Garantía de seguridad en protección de datos

De acuerdo con la técnica, costes y fines del tratamiento, y con los riesgos para los derechos y libertades de los interesados, se exige al responsable y encargado del tratamiento apliquen las medidas técnicas, y organizativas adecuadas para garantir un nivel de seguridad adecuado al riesgo, es decir, las conocidas medidas de protección de datos desde el diseño y por defecto[67]. Estos mecanismos, como se establece en el artículo 32, pueden ser:

a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.[68]

Con tal de demostrar el cumplimiento en materia de seguridad, se establece la posibilidad de adherirse a un código de conducta o a un mecanismo de certificación. Los códigos de conducta deberán ser promovidos por los estados miembro, el Comité y la Comisión. Asimismo, asociaciones y otros organismos representativos de categorías de responsables o encargados de tratamiento podrán elaborar, modificar o ampliar códigos de conducta. Cuando

[67] Estos dos principios son claves para entender la responsabilidad proactiva. La AEPD establece que la protección desde el diseño busca que la protección de datos se establezca en las primeras fases del diseño del proyecto, y la privacidad por defecto, hace referencia a que solo sean objeto de tratameinto los datos necesarios para cumplir el fin.

[68] REGLAMENTO (UE) 2016/679, *op. cit.*, art 32.

así sea, la autoridad de control deberá previamente comprobar que el código elaborado respeta íntegramente el Reglamento.

Con tal de garantizar la seguridad y confidencialidad de los datos, y poder garantir la cibersegurdad necesaria para la salvaguarda de la información, la Organización internacional para la estandarización, crea la normativa ISO 27000. Estas buscan la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), que consiste en "*el conjunto de políticas, procedimientos y directrices junto a los recursos y actividades asociados que son administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información esenciales*[69]*".* Las claves para comprender el objetivo de estas normas son la confidencialidad de la información, integridad, y la disponibilidad. Estas normas prevén obtención de un certificado que acredite la correcta implementación de un SGSI. La Caja Guipúzcoa San Sebastián Kutxa[70] fue la primera entidad financiera del País Vasco en obtener dicho certificado, y lo contempla como una etiqueta de compromiso con la seguridad de la información, que ofrece tanto ventajas a la entidad, como confianza para sus clientes.

Evaluación de impacto relativa a la protección de datos

En la línea de la responsabilidad proactiva exigida por el Reglamento, debemos observar si de acuerdo con la naturaleza del tratamiento, se debe realizar una evaluación del impacto en la protección de datos.

Para ello, y de acuerdo con el artículo 35 del Reglamento 2016/679, se observan las listas[71] orientativas elaboradas por la AEPD. Se has establecido 11 criterios según los cuales los tratamientos que cumplan algunos de ellos deberán realizar la evaluación de impacto. El tratamiento que es objeto de análisis actualmente, no cumple con ninguno de los 11 criterios establecidos[72].

---

[69] Iso 27000.es (2020) *SGSI: Información fundamental sobre el significado y sentido de implementación y mantenimiento de los sistemas de Gestión de la Seguridad de la Información*. Recuperado de http://www.iso27000.es/sgsi.html

[70] *Kutxanet obtiene la ISO 27001* (2009). Banca Electrónica. Núm. 125, 19-20.

[71] Agencia Española de Protección de datos. (2019). *Lista orientativa op. cit.*

Designa de Delegado de Protección de Datos

Por último, debemos analizar si la designa del delegado de protección de datos sería necesaria para esta primera entidad. El artículo 37 del Reglamento 2016/679 establece una lista cerrada de supuestos en que se debe designar el delegado.

En este caso, si la entidad receptora de datos fuera un autoridad pública, debería ser designado un delegado, y de tratarse de una entidad privada, solamente estará en la obligación de realizar dicha designación aquellas entidades que se dediquen a la observación habitual y sistemática de datos a grande escala, o aquellas e que se traten categorías especiales de datos. Aun así, las organizaciones pueden nombrar voluntariamente un DPD, dado que les puede ser de utilidad.

Los criterios establecidos para determinar que entidades deben designar un delegado de protección de datos parecen confusos, dado que el término *gran escala* parece indeterminado. El Grupo de Trabajo sobre protección de datos del artículo 29[73] aclara que no se puede determinar una cifra exacta en relaciona número de datos procesados y personas afectadas que pueda aplicarse a toda situación. Pr ello recomienda que se tengan en cuenta diferentes factores como número de afectados, volumen de datos duración de la actividad de tratamiento o alcance geográfico de la actividad del tratamiento.

En las mismas Directrices, el Grupo de trabajo ofrece ejemplos de tratamientos que son considerados a gran escala a efectos de designa de delegado de personal, y cita los datos de un hospital, datos de desplazamiento de personas a través del transporte público, datos de una compañía de seguros o de un banco.

Para determinar si la entidad receptora de datos debe designar o no un delegado de protección de datos, deberíamos atender al supuesto concreto, y conocer qué tipo de datos trata, y cuál es la actividad de la entidad, para conocer el alcance de los datos que trata.

[73] Grupo de Trabajo sobre protección de datos del artículo 29 (2016). *Directivas sobre delegados de protección de datos (DPD).*

Capítulo II. Implicaciones del nuevo marco legislativo para el tratamiento de los datos masivos.

A continuación, procederemos a analizar las obligaciones de la segunda entidad, la cual recibe de la primera los datos y almacena y analiza los mismos con la tecnología Big Data.

Información al interesado

A diferencia del supuesto analizado anteriormente, esta entidad no ha obtenido los datos mediante el consentimiento del interesado, sino que los ha obtenido de un tercero. Para este escenario y con el fin de proteger los derechos y libertades del interesado, los legisladores europeos incorporan en el Reglamento 2016/679 la obligación del responsable del tratamiento de facilitar la siguiente información: identidad y contacto del responsable y/o encargado del tratamiento, datos de contacto del delegado de personal, si lo hubiese, los fines del tratamiento y la base jurídica que lo legitima, la categoría de datos que dispone, los destinatarios, incluidos terceros países u organizaciones internacionales.

El encargado del tratamiento, conforma a lo establecido en el artículo 14.2 del Reglamento, deberá facilitar un seguido de información al interesado en cuanto al tratamiento que realizará. En su caso, deberá informar de los derechos que goza el interesado para proteger su privacidad, el plazo durante el cual van a ser tratado los datos, la fuente de la que proceden los datos personales, incluido si proceden de fuentes de acceso público, e informar de la existencia de decisiones automatizadas y elaboración de perfiles.

Todo este conjunto de información, deberá ser facilitada al interesado en un plazo razonable que no exceda de un mes desde que se obtuvieron los datos.

Legitimación del tratamiento

Todo tratamiento debe estar legitimado por alguna de las causas contenidas en el artículo 6 del Reglamento 2016/679, como hemos dicho anteriormente. Después de un riguroso análisis de dichas causas, planteo dos supuestos que se darían para la realización de un tratamiento legítimo.

En primer lugar, se plantea la hipótesis en que la primera entidad, tuviera en consideración su objetivo de transferir los datos para un posterior análisis, y hubiera obtenido el consentimiento del interesado para tal fin.

En segundo lugar, tal y como es previsto en el artículo 14.4 del Reglamento 2016/679,

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

Así, se dispone el deber meramente de informar al interesado previamente, cuando los datos son tratados para un fin distinto por el que cual fueron obtenidos.

Las afirmaciones anteriores, dejan en evidencia que el tratamiento realizado por la segunda entidad, podrá ser legítimo cuando el interesado presta su consentimiento inicialmente para tal fin, o cuando el responsable de la segunda entidad ofrece toda la información prevista en el reglamento al interesado, además de los fines que persigue el tratamiento ulterior, pudiendo el interesado ejercer su derecho a oposición.

Evaluación de impacto de protección de datos

En tanto que esta segunda entidad procederá al análisis de los datos mediante la nueva tecnología explicada anteriormente, Big Data, deberemos conocer si este tratamiento específico requiere una evaluación de impacto en protección de datos.

Acudiremos a la lista que proporciona la AEPD donde se determina que tratamientos, por su especial riesgo en materia de protección de datos, requieren la elaboración de la evaluación de impacto prevista en el Reglamento. En el criterio 10 facilitado, se determina que deberán realizar la evaluación los

> tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo para los derechos y libertades de las personas.

Determinamos entonces, que esta segunda entidad que tratara los datos mediante las técnicas de análisis Big Data, deberá realizar una evaluación del impacto. Para ello, de acuerdo con lo establecido en el punto séptimo del artículo 35 del Reglamento 2016/679, la evaluación deberá contener como mínimo la siguiente información:

- Descripción de las operaciones de tratamiento, los fines del mismo, y si estuviera persiguiendo un interés legítimo.
- Evaluación de la necesidad y proporcionalidad de acuerdo con el fin perseguido.
- Evaluación del riesgo que ello supone para los derechos y libertades de los interesados.
- Explicación de las medidas adoptadas para afrontar los riesgos.

Dicha evaluación deberá realizarse, de acuerdo con el principio de protección desde el diseño, antes de empezar el mencionado tratamiento. Este será responsabilidad principal del responsable de tratamiento, quien podrá recibir soporte del encargado de tratamiento. Además, la entidad hubiera designado un delegado de protección de datos, este deberá aconsejar en cuanto a la idoneidad de la evaluación, metodología etc.

La Autoridad Catalana de Protección de Datos ofrece en su portal web una propuesta de Evaluación de Impacto[74], que incorpora además de la información mínima mencionada de forma muy completa y detallada, información acerca de transferencia de los datos tratados, si estos de transfieren a terceros países u organizaciones internacionales.

Cuando el resultado de la evaluación concluya que hay un alto riesgo, el responsable deberá hacer una consulta previa a la autoridad de control. Esta

[74] Se adjunta la propuesta de Evaluación de impacto de Protección de datos realizada por la APDCAT en el Anexo II.

cuando considere que no se ha mitigado de forma suficiente el riesgo, deberá comunicar al responsable en el plazo de 8 semanas deberá asesorar al encargado o responsable. Este plazo podrá ser prorrogado 6 semanas más en función de la complejidad del tratamiento.

Adema s de lo expuesto anteriormente, la segunda entidad deberá cumplir con el deber de realizar un registro de tratamiento y garantizar la seguridad en materia de protección de datos. En el caso que sea preciso, si se tratara de una autoridad u organismo público, si se realizara una observación sistemática habitual del interesado, o si se trataran datos especiales o datos de infracciones o condenas penales a gran escala deberá designarse un DPD.

IV. Resultado y discusión

A continuación, se expondrán las distintas decisiones empresariales que se pueden tomar en relación al tratamiento de datos, cuando su recogida va dirigida a obtener un beneficio empresarial, ya sea mediante la comunicación o transmisión de los mismos, o mediante el análisis de los datos obtenidos. Seguidamente de cada decisión empresarial planteada, se analizaran las políticas de privacidad de datos de conocidas entidades como Movistar, Facebook o Google que han tomado estas posiciones para conocer en que basan su legitimación y los fines que se informan al interesado.

Una primera política adoptable frente a la voluntad de tratar los datos personales con tal de darle valor a los mismos es la anonimización de estos. Se establece claramente en el Reglamento que "los principios de protección de datos no deben aplicarse a la información anónima"[75].

Este proceso de anonimización, como se ha comentado anteriormente, debe partir de dos características claves. En primer lugar, los datos no pueden ser identificables o relacionables con el interesado, y en segundo lugar, se deben tener en consideración el conjunto de medios que se disponen en cada momento por tal de no hacer posible una reversión del anonimato.

La principal problemática es que el tratamiento este tipo de datos queda al margen de las prerrogativas en materia de protección de datos personales, y no se encuentra regulado. Las únicas indicaciones que se encuentran actualmente sobre este proceso y como debe realizarse para garantir la privacidad, es el realizado en la Opinión del Grupo de Trabajo del Artículo 29, y las orientaciones realizadas por las autoridades de control de los Estados Miembros.

De ellos se desprende la recomendación de actuar acorde con un seguido de principios como la protección por diseño y por defecto o el principio de información y transferencia. Asimismo, se recomienda la creación de un equipo

[75] REGLAMENTO (UE) 2016/679, *op. cit.*, Considerando 26.

de trabajo equivalente al establecido en el Reglamento 2016/679, y la evaluación de riesgos de reidentificación.

En definitiva, esta opción permitirá mantener los beneficios y minimizar los riesgos en privacidad. Por otro lado, es evidente que las técnicas conocidas de anonimización se encuentran con la dificultad de "crear un conjunto de datos verdaderamente anónimo conservando, sin embargo, toda la información subyacente requerida"[76].

La entidad que analizaremos a continuación, Movistar, declara en su política de privacidad de datos que esta tendrá una composición mixta, compuesta por datos personales y datos anonimizados. Así, asegura que los datos tratados *podrán* ser objeto de un proceso de anonimización irreversible especialmente para proyectos de Big Data e informa al interesado que cuando estos sean anonimizados no deberán aplicarse los principios de protección de datos de carácter personal.

Podemos observar que al tratar datos personales que luego podrán ser anonimizados, la entidad presenta una política de privacidad atendiendo a las disposiciones en materia de protección de datos, y que en los supuestos en que se anonimicen datos, el tratamiento posterior que se pueda realizar con técnicas Big Data no deberá someterse a las evaluaciones de impacto que establece la legislación.

Como la recogida de los datos es anterior a la anonimización, y la simple recogida es concebida como una forma de tratamiento, se establecen en la política de privacidad las bases que lo legitiman. Entre ellas encontramos además del consentimiento del interesado, la necesidad para ejecución del contrato[77] y el

[76] Grupo de Trabajo sobre protección de datos del artículo 29 (2014). *Dictamen 05/2014 sobre técnicas de anonimización.*

[77] Mediante esta base legal, se confirma que se trataran datos acerca de cómo se utiliza el producto que ofrecen, páginas web y apps Movistar, se podrá acceder al sistema de información crediticia para comprobar la solvencia del cliente, e incluso se establece el uso de los datos para fines estadísticos y de estudios de mercado hasta los 3 meses posteriores en que el sujeto ha dejado de ser cliente.

interés legítimo[78]. Como ya hemos avanzado, Movistar asegura que para los proyectos Big Data, procederá a la anonimizacion, donde "los datos de carácter personal reales son sustituidos por identificadores únicos irreversibles, de tal manera que no sea posible ejecutar el proceso a la inversa"[79].

Por otro lado, se puede adoptar una política basada en el tratamiento de los datos personales, bajo las garantías establecidas en el Reglamento. Tras el estudio realizado, concluimos que una entidad que quiere comunicar los datos personales que dispone a otra entidad, deberá hacerlo constar en la política de privacidad explícitamente, y contar con el consentimiento del interesado. Del mismo modo, la entidad que reciba los datos, deberá informar al interesado la finalidad de los tratamientos que va a realizar, ya sea para fines publicitarios o de estudio de mercado.

Esta decisión, aunque conllevara adherir a los datos un valor añadido y con el beneficio de ser estos identificables, al contrario que sucede con la primera opción explicada, puede suponer un riesgo en la confianza del cliente.

El estudio[80] realizado con los datos recogidos por INE, Eurostat, INCIBE-INTECO y ONTSI rebela que del total de personas que afirma hacer uso de internet cuotidianamente, un 59,7% confía bastante en internet, un 32% afirma confiar poco o nada, y solamente un 8,3% confía mucho en internet. Estos datos fueron recogidos en 2018, y muestra una sociedad donde a pesar de afirmar tener poca confianza alrededor de internet, sigue haciendo uso del mismo y proporcionando una gran cantidad de datos personales en él.

Teniendo en cuenta este bajo grado de confianza de los internautas, las entidades deberán realizar una toma de decisiones en cuanto a su política de privacidad decidiendo entre la adquisición de datos personales y el rendimiento que estos conllevan, o mantener la imagen y confianza de sus clientes.

---

[78] Mediante el interés trataran datos principalmente para fines administrativos, y para ofrecer al cliente ofertas personalizadas.

[79] Movistar (2019). *Política de privacidad.* Recuperado de http://www.movistar.es/particulares/centro-de-privacidad/#Quien

[80] Ministerio de Economia y empresa, ONTRI & red.es (2019). *Esquema de indicadores de confianza digital en España. Abril 2019.*

Esta política de privacidad se puede observar en la empresa Amazon Europa. Está detalla claramente que la entidad hace uso de los datos personales para poder ofrecer una publicidad acorde con tus intereses. Expresan que recogen información acerca de las interacciones de los clientes en la web, contenido y servicio de Amazon. De esta finalidad principal se desprende mucha información. A continuación analizaremos cual es la base legitimadora que permite hacer este tratamiento, y si esta información es compartida con otras entidades.

En cuanto a la base legitimadora del tratamiento, no se establece claramente esta en la política de privacidad, como sucede en el caso de Movistar, sin embargo, como de detallan las finalidades, se entiende de forma indirecta que el consentimiento será la base legitimadora. Destacamos de las finalidades indicadas la publicidad y la identificación de preferencias y recomendaciones, dado que esas finalidades son las que planteamos en este estudio, conseguidas mediante la aplicación de Big Data.

En segundo lugar, Amazon establece en su política de privacidad la intención clara de comunicar los datos personales a terceros para poder lograr sus fines. Sin embargo, aclara que "la información relativa a nuestros clientes es una parte fundamental de nuestro negocio y no participamos en actividades de venta de la información personal de nuestros clientes a terceros"[81]. Así, se procede a la comunicación de información personal a terceros proveedores para que presten servicios de análisis de datos, asistencia de marketing, y ofrecer resultados de búsqueda y enlaces entre otros.

En conclusión a lo observado, se entiende que la entidad comunica la información personal para ser analizada y poder obtener un valor añadido y poder acompañar una campaña publicitaria y de marketing más efectiva, pero esta comunicación no se realiza como una actividad lucrativa en si misma.

Finalmente, se presenta una política de privacidad basada en el tratamiento de datos personales, pero donde el análisis de los mismos es realizado dentro del

[81] Amazon Europa (2019). *Aviso de privacidad de amazon.es*. Recuperado de https://www.amazon.es/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=200545460

grupo empresarial, dando valor a los datos ya ordenados, y ofreciendo los resultados y conclusiones que se derivan del mismo como producto.

En esta decisión, se deberá indicar el fin por el que se trataran los datos, pero al ser un mismo grupo empresarial, no dará la imagen al interesado de la pérdida de control y privacidad sobre sus datos, dado que los mimos permanecen en un mismo grupo de empresas. El análisis de los datos y la elaboración de perfiles permitirán la segmentación de los usuarios para ofrecer un mejor público para campañas publicitarias.

Permitirá además a la entidad conservar los datos y con él su valor, siendo las otras entidades interesadas en la información las que deberán solicitar los servicios.

Esta posición es la elegida por entidades como Facebook y Google. Estas entidades ofrecen servicios de publicidad en su web a terceros, es por esto que obtienen más valor analizando los datos para ofrecer un mejor servicio, que comunicarlos a un tercero, además de que cuidan más la imagen ante los usuarios.

En este sentido, observaremos las finalidades del tratamiento que realiza, su base legitimadora y si hay comunicación de los datos. La finalidad que más relevancia tiene a efectos de este trabajo es la de ofrecer mediciones, análisis y otros servicios empresariales. Admiten hacer uso de la información personal recogida, incluida la de la actividad realizada fuera de los productos Facebook, "para ayudar a los anunciantes y otros socios a medir la eficacia y distribución de sus anuncios y servicios, así como a entender qué tipo de personas usan sus servicios y cómo estas interactúan con sus sitios web, apps y servicios"[82]

En cuanto a la legitimación del tratamiento, se basa en el cumplimiento de las condiciones del servicio que presta Facebook. La esencia del servicio de Facebook consiste en conectar personas, pero además fomentar el crecimiento de las empresas, ofreciendo servicios de publicidad. En las condiciones, se establece

[82] Facebook (2018). *Política de datos.* Recuperado de https://www.facebook.com/privacy/explanation

también que el servicio es gratuito, pero que como contraprestación, se mostraran anuncios a los usuarios de acuerdo con los intereses personales.

Por último, en cuanto a la comunicación de datos personales, Facebook tras el escándalo vivido anteriormente, opta por detallar de forma clara que en la entidad no se venden los datos a terceros. Por lo contrario, los datos personales son tratados por el conjunto de empresas de Facebook, y ofrece a sus clientes información útil pero que en ningún caso contiene elementos identificables.

V. Conclusiones

Tras la lectura bibliográfica y el análisis del marco legal adoptado en la Unión Europea, se puede determinar que la comunicación de datos personales para el posterior análisis mediante técnicas Big Data para conseguir un mayor valor de los datos y así conseguir una mejor toma de decisión, ya sea en cuanto a estrategias de marketing o de políticas de venta, es posible.

De este modo, las empresas se ven plenamente beneficiadas y pueden prestar un servicio más eficiente, una venta más personalizada acorde con los intereses del cliente, y mejorar así sus rendimientos.

Desde esta perspectiva económica, parece que el nuevo marco legislativo se presenta como un avance en cuanto a desarrollo económico para las empresas, además de todos los beneficios que conlleva el uso de los datos personales, ya expuestos anteriormente. Aun así, es evidente que el Reglamento 2016/679 y su aplicación dejan espacios y dudas respecto de la protección de la privacidad e intimidad. A continuación se expondrán las cuestiones que tras el trabajo realizado, se concluye que pueden suponer un riesgo para los derechos de los interesados.

Las cuestiones principales se centran en dos grandes ejes, la legitimación del tratamiento y la evaluación del impacto de este sobre los datos personales.

El legislativo europeo plantea la legitimación del tratamiento en diversas causas. El consentimiento es la principal fuente de legitimación, y se determina claramente como debe ser este. Sin embargo, como hemos podido observar en las diversas políticas de privacidad analizadas, las empresas buscan otras formas de hacer caber este tipo de tratamiento de forma legal.

Por un lado, se plantea la posibilidad de realizar el tratamiento en tanto que este se encuentra estipulado en las condiciones del servicio que está solicitando, de ese modo, se alagará como base legitimadora lo estipulado en el artículo 6.1 apartado b) del Reglamento 2016/679.

En tanto que estas son impuestas de forma unilateral por el empresario que presta los servicios, es decir, sin negociación de las partes, podrían asemejarse a las clausulas generales de contratación. Estas son reguladas en la Ley de Condiciones Generales de Contratación[83], y en ella se estipula que no se incorporaran aquellas cláusulas que no sean debidamente informadas al consumidor, o aquellas que sean ilegales, ambiguas u oscuras. Del mismo modo, se determinaran nulas aquellas cláusulas que sean abusivas o causen un perjuicio al consumidor.

Podemos concluir en este punto que si la legitimación se encuentra en el cumplimiento del contrato o condiciones del servicio, condiciones impuestas por el empresario unilateralmente, deberían estas ser impugnables mediante la acción individual del interesado, pudiendo ser declaradas nulas o no incorporadas, produciendo los efectos recogidos en el artículo 10[84].

Paralelamente, otras entidades optan por basar sus tratamientos en su interés legítimo, tal y como lo permite el apartado f) del artículo 6.1 del Reglamento 2016/679. Este concepto es ambiguo y no se ha desarrollado a lo largo del texto normativo, ni se ha aportado una lista taxativa de lo que comprende el interés legítimo. Lo que se determina es una regla de ponderación, según el cual el interés legítimo no podrá prevalecer sobre los intereses o derechos y libertades fundamentales del interesado que requieran la protección de datos personales. La determinación de la existencia de interés legítimo requerirá una evaluación minuciosa.

Y así lo confirma la AEPD en su informe 2016-0278, donde se afirma que para determinar la existencia de interés legítimo por parte del responsable de tratamiento deberá realizarse un "ejercicio de ponderación entre dicho interés

[83] Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación. Boletín Oficial del Estado, 89. (1998).

[84] Ley 7/1998, *op. cit.*, art. 14

legítimo y los derechos fundamentales de los afectados prevaleciera el primero sobre el segundo"[85].

Así mismo, como se ha comentado anteriormente, el Reglamento 2016/679 establece como interés legítimo el tratamiento con fines de mercadotecnia directa. Del mismo modo que se ha determinado esta finalidad como interés legítimo del responsable, sería interesante que las autoridades competentes pudieran hacer una guía o lista *nuperus apertus* que sirva de orientación para los responsables, dado que actualmente es un concepto que puede dar lugar a duda.

Igualmente, debido a la reciente aplicación del Reglamento 2016/679 y el LOPD, no contamos con numerosa jurisprudencia e interpretaciones judiciales de estos términos, y a medida que aparezcan conflictos derivados de la aplicación de la nueva norma, se podrá contar con jurisprudencia de los tribunales.

En segundo lugar, y como ya se ha anunciado, debemos destacar cuestiones relacionadas con la evaluación de impacto de protección de datos. En la lista elaborada por la AEPD se detalla con claridad los tratamientos que debido al alto riesgo en los derechos y libertades de los interesados, deben elaborar una evaluación del impacto sobre la protección de datos del tratamiento con anterioridad a la realización de la actividad.

Se establecen diversos supuestos en que se deberá realizar la evaluación, y estos se centran en diversos factores, tales como elaboración de perfiles, tratamiento a gran escala de datos especiales, observación sistemática de zonas públicas, toma de decisiones automatizadas etc.

Como hemos visto, el análisis de los datos personales a partir del método Big Data, en tanto que hace uso de nuevas tecnologías, o más bien dicho, que se hace un uso innovador de las tecnologías, tiene prevista la realización previa de la evaluación de impacto. Por el contrario, la simple comunicación de datos de una entidad a otra no se prevé como un tratamiento de alto riesgo. Este solo se vería

[85] Agencia Española de Protección de Datos (2016). *Informe jurídico 2016-0278. El interés legítimo.* Recuperado de https://www.aepd.es/sites/default/files/2019-09/informe-juridico-rgpd-interes-legitimo.pdf

afectado por la evaluación de impacto si comunicara datos de categorías especiales, datos a gran escala.

En consonancia con todo lo observado anteriormente, y teniendo en consideración que la comunicación de datos sistemática puede conllevar una sensación de pérdida de control del interesado, y una desinformación, debería considerarse la necesidad de evaluar el impacto que esta comunicación implicaría para la privacidad en los datos.

Distinta es la situación en que se comuniquen los datos para poder cumplir con las obligaciones contractuales o para prestar los servicios previamente contratados, en esta ocasión nos referimos a la comunicación con finalidades alternativas, de análisis por ejemplo.

Finalmente, cabe hacer mención de los sistemas de anonimización. Estos se presentan como una alternativa al tratamiento de datos personales. Como se ha visto, los datos anonimizados podrán ser tratados sin aplicación de la normativa establecida en el Reglamento 2016/679. Siempre que el proceso de anonimización sea efectivo e irreversible, se plantea como una opción que además de permitir obtener valor de los datos, respetara la privacidad e identidad se los sujetos que los cedieron.

VI. Referencias bibliográficas

Agencia Española de Protección de Datos (2016). *Informe jurídico 2016-0278. El interés legítimo.* Recuperado de https://www.aepd.es/sites/default/files/2019-09/informe-juridico-rgpd-interes-legitimo.pdf

Agencia Española de Protección de Datos (2016). *Orientaciones y garantías en los procedimientos de anonimización de datos personales.*

Agencia Española de Protección de Datos. (2019). *Lista orientativa de tipos de tratamiento que requieren Evaluación del Impacto Relativo a la Protección de Datos.*

Agencia Española de Protección de Datos. (2019). *Lista orientativa de tipos de tratamiento que no requieren Evaluación del Impacto Relativo a la Protección de Datos*.

Agencia Española de Protección de Datos. Resolución nº R/00657/2019 de 3 de febrero de 2020.

Amazon Europa (2019). *Aviso de privacidad de amazon.es*. Recuperado de https://www.amazon.es/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=200545460

Autoritat catalana de Protecció de Dades (2020). *Principals novetats del RGPD*. Recuperado de https://apdcat.gencat.cat/ca/documentacio/RGPD/novetats/

Castillo Jiménez, C. (2001). Derecho y conocimiento. *Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información*. Volumen 1, 35-48.

COMISIÓN EUROPEA (2014). *Hacia una economía de los datos próspera.* COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES.

Cristea Uivaru, L. (2018). *La protección de datos de carácter sensible: Historia Clínica Digital y Big Data en Salud.* J.M. Bosch Editor.

De Montalvo Jääskeläinen, F. (2019). *Una reflexión desde la teoría de los derechos fundamentales sobre el uso secundario de los datos de salud en el marco del Big Data.* Revista de derecho político nº 106, 43-75.

DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y 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 datos. Diario oficial de las Comunidades Europeas, L 281. (1995).

Facebook (2018). *Política de datos.* Recuperado de https://www.facebook.com/privacy/explanation

Fundación COTEC para la innovación (2017). *Generación de talento Big data en España.* Recuperado de https://www.ituser.es/big-data/2019/04/las-soluciones-de-big-data-y-analitica-creceran-un-12-en-2019

Garriga Domínguez, A. (2016). *Nuevos retos para la protección de Datos Personales. En la era del Big Data y de la computación ubicua.* Dykinson. Madrid.

Garriga Dominguez, A. (2018) *La elaboración de perfiles y su impacto en los derechos fundamentales. Una primera aproximación a su regulación en el reglamento general de protección de datos de la Unión Europea*.

Gil González, E. (2016). *Big data, privacidad y protección de datos.* Boletín Oficial del Estado. Madrid.

Goyzueta Rivera, S. (2015). *Big Data Marketing: una aproximación.* Perspectivas nº35, 147-158.

Grupo de Trabajo sobre protección de datos del artículo 29 (2014). *Dictamen 05/2014 sobre técnicas de anonimización.*

Grupo de Trabajo sobre protección de datos del artículo 29 (2016). *Directivas sobre delegados de protección de datos (DPD).*

Hernández-Pérez, T (2016) *En la era de la web de los datos abiertos, después los datos masivos*. Cita originaria IBM (2016) https://www-01.ibm.com/software/data/bigdata/what-isbig-data.html

INE. (2019). *Encuesta de uso de TIC y Comercio electrónico (CE) en las empresas 2017- 2018.* Recuperado de https://www.ine.es/jaxi/Datos.htm?path=/t09/e02/a2017-2018/l0/&file=02013.px

Iso 27000.es (2020) *SGSI: Información fundamental sobre el significado y sentido de implementación y mantenimiento de los sistemas de Gestión de la Seguridad de la Información*. Recuperado de http://www.iso27000.es/sgsi.html

Joyanes Aguilar, L. (2013). *Big Data: análisis de grandes volúmenes de datos en organizaciones.* Alfaomega Grupo Editor. México DF.

Kutxanet obtiene la ISO 27001 (2009). Banca Electrónica. Núm. 125, 19- 20.

Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación. Boletín Oficial del Estado, 89. (1998).

Ley Orgánica 3/2018, del 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Boletín Oficial del Estado, 294. (2018).

Mantelero, A. (2015). *Smart cities, movilidad inteligente y protección de los datos personales.* IDP. Revista de Internet, Derecho y Política nº 21, 37-49.

Miguel Asensio, P.A. (2017). *Competencia y derecho aplicable en el Reglamento General sobre Protección de datos de la Unión Europea*. Revista Española de Derecho Internacional, 75- 108. Recuperado de http://bibliotecaculturajuridica.com/EDIT/1665/competencia-y-derecho-aplicable-en-el-reglamento-general-sobre-proteccion-de-datos-de-la-union-europea.html/

Minero, G. (2019). *Nuevas tendencias en materia de protección de datos personales. La nueva Ley Orgánica y la jurisprudencia más reciente.* Anuario jurídico y económico. Núm. 52, 125- 148.

Ministerio de Economia y empresa, ONTRI & red.es (2019). *Esquema de indicadores de confianza digital en España. Abril 2019.*

Morente Parra, V. (2019). *Big Data o el arte de analizar datos masivos.* Derechos y libertades, 225-260.

Movistar (2019). *Política de privacidad.* Recuperado de http://www.movistar.es/particulares/centro-de-privacidad/#Quien

Perry, J.S. (2017). *What is big data? More than volume, velocity and variety*. Recuperado de https://developer.ibm.com/dwblog/2017/what-is-big-data-insight/

Pires, A. (2014). *Una gestión inteligente de la seguridad pública.* Revista de obras públicas nº 3550: Smart cities, 45-48.

Recurso 509/2017 de la Sección 1ª, sala de lo contencioso administrativo de la audiencia nacional.

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Diario Oficial de la Unión Europea, L 119. (2016).

Rosenberg, M. Condessore, N. Cadwalladr, C. (2018). How Trump Consultants Exploited the Facebook Data of Millions. *The New York Times*. Recuperado de https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

Sentencia del Tribunal de Justicia (Gran Sala) de 13 de mayo de 2014 (petición de decisión prejudicial planteada por la Audiencia Nacional — España) — Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos (AEPD),

Mario Costeja González. (Asunto C-131/12)

Silva Guerra, H. González Ortiz, J. Martínez Díaz, D. Giraldo Oliveros, M. Juliao Esparragoza, D. (2014) *Marketing: conceptos y aplicaciones.* Universidad del norte, Colombia

Todolí Signes, A. (2018). *La gobernanza colectiva de la protección de datos en las relaciones laborales: Big Data, creación de perfiles, decisiones empresariales automatizadas y los derechos colectivos*. Revista de Derecho Social, 69-88.

Villarejo Galende, H. (2015). *Smart cities: una apuesta de la unión europea para mejorar los servicios públicos urbanos*. Revista de Estudios Europeos nº 66, 25-51.

VII. Anexos

Anexo I. Contrato encargado de tratamiento

En #POBLACION# a____de_____de 20____

REUNIDOS

De una parte, Don_____provisto de DNI nº _____actuando como representante legal de____con domicilio en_____y CIF nº _____en adelante RESPONSABLE DEL FICHERO.

De otra parte, Don_____provisto de DNI nº_____actuando como legal representante de NOMBRE DEL PROVEEDOR, con domicilio en _____y CIF nº _____en adelante ENCARGADO DEL TRATAMIENTO.

Ambas partes se reconocen mutuamente la capacidad legal suficiente para suscribir este contrato de encargo de tratamiento de datos personales y para quedar obligadas en la representación en que respectivamente actúan, en los términos convenidos en él. A tal fin,

MANIFIESTAN

1. Que ambas partes se encuentran vinculadas por una relación contractual de carácter mercantil para la prestación de_____ (en adelante SERVICIO).

2. Que para la prestación de dicho servicio es necesario que el ENCARGADO DEL TRATAMIENTO tenga acceso y realice tratamientos de datos de carácter personal de los _____ responsabilidad del RESPONSABLE DEL FICHERO, por lo que asume las funciones y obligaciones que el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, estipula para los Encargados de Tratamiento

3. Ambas partes reconocen cumplir con todas las obligaciones derivadas de la normativa

comunitaria y nacional en materia de protección de datos, en especial las relativas al derecho de información, consentimiento y deber de secreto, , y a la adopción de las medidas de seguridad técnicas y organizativas que garanticen la seguridad de los datos personales

4. Que, en cumplimiento del artículo 28 del RGPD, ambas partes de forma libre y espontánea voluntad acuerdan regular este acceso y tratamiento de datos de carácter personal de conformidad con las siguientes:

ESTIPULACIONES

PRIMERO: OBJETO DEL CONTRATO

Mediante las presentes cláusulas se habilita a la entidad ENCARGADA DE TRATAMIENTO, para tratar por cuenta del, RESPONSABLE DEL TRATAMIENTO, los datos de carácter personal necesarios para prestar el servicio anteriormente descrito.

SEGUNDO: IDENTIFICACIÓN DE LA INFORMACIÓN AFECTADA

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, el RESPONSABLE DEL TRATAMIENTO, pone a disposición del ENCARGADO DEL TRATAMIENTO, la
información que se describe a continuación:

- _____
- _____

TERCERO: DURACIÓN

El presente acuerdo tiene una duración de _____

Una vez finalice el presente contrato, el ENCARGADO DE TRATAMIENTO debe suprimir/devolver al RESPONSABLE, o devolver a otro encargado que designe el RESPONSABLE los datos personales y suprimir cualquier copia que esté en su poder.

CUARTO: OBLIGACIONES DEL ENCARGADO DE TRATAMIENTO

El ENCARGADO DEL TRATAMIENTO y todo su personal se obliga a:

1-. 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.

2-. 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 Reglamento (UE) 2016/679 o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el encargado informará inmediatamente al responsable.

3-. Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga[1]:

A. El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado y, en su caso, del representante del responsable o del encargado y del delegado de protección de datos.

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

C. En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49 apartado 1, párrafo segundo del Reglamento (UE) 2016/679 , la documentación de garantías adecuadas.

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

- La seudoanimización y el cifrado de datos personales.

- La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

- La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

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

[1] NOTA: Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, salvo que el tratamiento que realice pueda suponer un riesgo para los derechos y las libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1 del Reglamento (UE) 2016/679, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10 de dicho Reglamento.

tratamiento.

4-. 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 del mismo 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.

2. 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 72 horas, 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 72 horas.

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.

6-. El ENCARGADO DEL TRATAMIENTO deberá observar en todo momento, y en relación con los ficheros de datos de carácter personal a los que tuviera acceso o le pudieren ser entregados por el Responsable, para la realización en cada caso de los trabajos y servicios que pudieren acordarse, el deber de confidencialidad y secreto profesional que, de conformidad con lo dispuesto en la normativa de Protección de Datos, subsistirá aun después de finalizar la relación de los trabajos encargados en relación con cualquier fichero así como, en su caso, tras la finalización por cualquier causa del presente contrato.

7-. 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[2]

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

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

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

- Acceso, rectificación, supresión y oposición

- Limitación del tratamiento

[2] NOTA: Si existe una obligación de confidencialidad de naturaleza estatutaria o legal (por ejemplo, abogados) deberá quedar constancia expresa de la naturaleza y extensión de esta obligación.

- Portabilidad de datos

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

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.

11-. Derecho de información

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.

12-. 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 72 horas, y a través de correo electrónico con confirmación de lectura, 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:

- 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.

- 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.

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

- 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)[3]

Opción A

- Corresponde al RESPONSABLE DEL TRATAMIENTO comunicar las violaciones de la seguridad de los datos a la Autoridad de Protección de Datos y a los interesados.

La comunicación contendrá, como mínimo, la información siguiente:

- 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.

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

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

- 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:

- Explicar la naturaleza de la violación de datos.

- 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.

---

[3] NOTA: Pese a que la notificación de las violaciones de seguridad a la autoridad de control o a los interesados corresponde al responsable del tratamiento, en aquellos supuestos en que los datos se traten exclusivamente con los sistemas del encargado puede ser recomendable atribuir dichas funciones al encargado.

- Describir las posibles consecuencias de la violación de la seguridad de los datos personales.

- 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.

13-. Dar apoyo al RESPONSABLE DEL TRATAMIENTO en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

14-. Dar apoyo al RESPONSABLE DEL TRATAMIENTO en la realización de las consultas previas a la autoridad de control, cuando proceda.

15-. 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.

16-. Implantar las medidas de seguridad siguientes:

Todas aquellas necesarias para:

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

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

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

- Seudonimizar y cifrar los datos personales, en su caso.

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

18-. Destino de los datos:

(Escoger una de las 3 opciones siguientes)

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 comporta 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.

QUINTO: OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO

Corresponde al RESPONSABLE DEL TRATAMIENTO:

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

2-. Realizar una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el encargado.

3-. Realizar las consultas previas que corresponda.

4-. Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del Reglamento (UE) 2016/679 por parte del encargado.

5-. Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

SEXTO: RESPONSABILIDAD DEL ENCARGADO DE TRATAMIENTO

1-. El ENCARGADO DEL TRATAMIENTO será considerado responsable del tratamiento en el caso de que destine los datos a otra finalidad, los comunique o los utilice incumpliendo el presente contrato. En estos casos, el ENCARGADO DEL TRATAMIENTO responderá de las infracciones en que hubiera incurrido personalmente.

2.- El ENCARGADO DEL TRATAMIENTO indemnizará al RESPONSABLE DEL TRATAMIENTO por los daños y perjuicios, de cualquier naturaleza, que pudieran resultar del incumplimiento de las obligaciones contraídas en virtud del presente contrato.

3.- A título enunciativo, y no limitativo, dicha indemnización incluirá los daños morales e imagen, costes publicitarios o de cualquier otra índole que pudieran resultar para su reparación. El ENCARGADO DEL TRATAMIENTO, asimismo, deberá responder de cualquier indemnización que a resultas de su incumplimiento tuviera que satisfacer a terceros.

4.- La responsabilidad del ENCARGADO DEL TRATAMIENTO incluirá, además, el importe de cualquier sanción administrativa y/o resolución judicial condenatoria que pudiera resultar contra el RESPONSABLE DEL TRATAMIENTO, como resultado del incumplimiento del ENCARGADO DEL TRATAMIENTO de la normativa y de las obligaciones exigidas en el presente contrato. La indemnización comprenderá, además del importe de la sanción y/o resolución judicial, el de los intereses de demora, costas judiciales y el importe de la defensa del RESPONSABLE DEL TRATAMIENTO en cualquier proceso en el que pudiera resultar demandada por cualquiera de las causas anteriormente expuestas.

SÉPTIMO: CONTROLES Y AUDITORÍA

El RESPONSABLE DEL TRATAMIENTO, en su condición, se reserva el derecho de efectuar en cualquier momento los controles y auditorías que estime oportunos para comprobar el correcto cumplimiento por parte del ENCARGADO DEL TRATAMIENTO del presente contrato. Por su parte, el Encargado deberá facilitar al RESPONSABLE DEL TRATAMIENTO cuantos datos o documentos le requiera para el adecuado cumplimiento de dichos controles y auditorías.

OCHO: NOTIFICACIONES

1.- Cualquier notificación que se efectúe entre las partes se hará por escrito y será entregada personalmente o de cualquier otra forma que certifique la recepción por la parte notificada.

2.- Cualquier cambio de domicilio de una de las partes deberá ser notificado a la otra de forma inmediata y por un medio que garantice la recepción del mensaje.

NUEVE: CLÁUSULAS GENERALES

1.- La no exigencia por cualquiera de las partes de cualquiera de sus derechos, de conformidad con el presente Contrato, no se considerará que constituye una renuncia a dichos derechos en el futuro.

2.- La relación jurídica que se constituye entre las partes se rige por este único Contrato, siendo el único válido existente entre las partes y sustituye a cualquier tipo de acuerdo o compromiso anterior acerca del mismo objeto, ya sea escrito o verbal, y sólo podrá ser modificado por un acuerdo firmado por ambas partes.

3.- Si se llegara a demostrar que alguna de las estipulaciones contenidas en este Contrato es nula, ilegal o inexigible, la validez, legalidad y exigibilidad del resto de las estipulaciones no se verán afectadas o perjudicadas por aquélla.

4.- El presente Contrato y las relaciones entre el RESPONSABLE DEL TRATAMIENTO y el ENCARGADO DEL TRATAMIENTO no constituyen en ningún caso sociedad, empresa conjunta, agencia o contrato de trabajo entre las partes.

5.-Los encabezamientos de las distintas cláusulas son sólo a efectos informativos, y no afectarán, calificarán o ampliarán la interpretación de este Contrato.

En testimonio de lo cual formalizan el presente contrato, por duplicado, en el lugar y fecha indicados en el encabezamiento.

D:/Dña._____ D:/Dña. _____

En nombre de «EL RESPONSABLE» En nombre de «EL ENCARGADO»

Anexo II. Plantilla de evaluación de impacto de Protección de Datos.

Plantilla d'Avaluació d'Impacte relativa a la Protecció de Dades

Una avaluació d'impacte relativa a la protecció de dades (AIPD) és un procediment que busca identificar i controlar el riscos pels drets i les llibertats de les persones que resulten d'un tractament de dades personal.

Cal una descripció del tractament per determinar si es necessària una AIPD. Aquesta descripció ha de tenir un nivell de detall que permeti avaluar els supòsits i indicadors de risc que es detallen a continuació.

Descripció del tractament

No cal fer una AIPD si aplica algun dels supòsits següents:

Supòsit	**Aplica?**
El tractament té naturalesa, abast, context i finalitat semblant a un altre tractament pel qual ja s'ha fet una AIPD.	
El tractament té una base jurídica en el dret de la UE o d'un estat membre, i ja s'ha realitzat una AIPD en el moment d'adoptar aquesta base jurídica.	
Justificació	

Si cap dels supòsits anteriors aplica, cal fer una AIPD si el tractament pot comportar un risc greu pels drets i les llibertats de les persones. El Grup de Treball de l'Article 29 (GT29) dona la següent llista de característiques que poden ser indicatives de risc alt.

Indicador de potencial risc alt	**Aplica?**
Avaluació o puntuació, incloses l'elaboració de perfils i prediccions.	
Presa de decisions automatitzada amb efectes jurídics o que afecta de manera similar i significativa a la persona física.	
Observació sistemàtica d'un àrea d'accés públic.	
Dades sensibles	
Tractament de dades a gran escala	
Conjunts de dades que s'han enllaçat o combinat.	
Dades relacionades amb persones vulnerables	
Ús innovador de tecnologies.	
Tractament que en si mateix impedeix l'exercici d'un dret o l'ús d'un servei o contracte	

Segons el GT29, cal fer una AIPD quan el tractament en presenta dues o més, tot i que indica que pot ser convenient fer l'AIPD fins i tot en alguns casos en què només en presenta una. Si n'hi ha dues o més i es considera que no cal fer una AIPD, cal justificar-ho.

Cal fer l'AIPD? Per què?

Si s'ha nomenat un DPD, cal considerar la seva opinió respecte de la necessitat de fer una AIPD.

Opinió del DPD respecte de la necessitat de fer una AIPD

1. Descripció del Tractament

Cal fer una descripció del tractament que sigui el més detallada possible, ja que aquesta serà la base per avaluar la necessitat, la proporcionalitat i els riscos del tractament.

Descripció detallada del tractament

Finalitat del tractament

1.1 Dades personals tractades

Les característiques de les dades a tractar són rellevants a l'hora de determinar els riscos del tractament i el compliment d'algunes disposicions del reglament.

Tipus de dada	
Font	
Termini de conservació	
Dada especialment sensible?	
Ús amb propòsit diferent a de recol·lecció?	

Tipus de dada	
Font	
Termini de conservació	
Dada especialment sensible?	
Ús amb propòsit diferent a de recol·lecció?	

1.2 Actors que intervenen en el tractament

Els actors que intervenen en el tractament, la seva funció i les dades que tracten són importants a l'hora de determinar els riscos del tractament.

Nom	
Processos en que intervé	
Descripció	

Nom	
Processos en que intervé	
Descripció	

1.3 Processos de tractament

L'objectiu d'aquesta secció és dividir el tractament en parts més petites. De manera que siguin més coherents i més fàcils d'explicar.

Procés	
Descripció	
Dades tractades	
Resultat del procés	
Destinatari	
Lloc del tractament	

Procés	
Descripció	
Dades tractades	
Resultat del procés	
Destinatari	
Lloc del tractament	

1.4 Transferències de Dades

Compartir dades amb agents externs pot incrementar els riscos del tractament; especialment si es fan a tercers països on l'RGPD no aplica.

Es comparteixen dades? Descriu quines dades es comparteixen, el destinatari i la raó.

2. Necessitat i Proporcionalitat

L'avaluació de la necessitat i de la proporcionalitat del tractament es fa en relació a la finalitat del tractament, que s'ha descrit a la secció anterior.

2.1 Finalitat del tractament

En principi, les dades recollides s'utilitzen per assolir la finalitat del tractament que va motivar la recollida. Ara bé, en alguns casos, el Reglament permet el tractament de dades que han estat recollides amb una finalitat diferent.

S'utilitzen dades recollides amb una finalitat diferent a la d'aquest tractament?	Sí / No

En cas afirmatiu

Les següents condicions permeten el tractament de les dades amb una finalitat diferent a la de recollida.

S'ha obtingut el consentiment dels interessats pel tractament amb la nova finalitat.	
El tractament esta basat en el dret de la unió o dels estats membres que constitueix una mesura per salvaguardar	
• la seguretat nacional	
• la defensa	
• la seguretat pública	
• la prevenció, la investigació, la detecció i el processament de delictes penals	
• altres objectius importants d'interès públic	
• la protecció de la independència judicial i dels procediments judicials	
• la prevenció, la investigació, la detecció i el processament d'infraccions en normes deontològiques	
• la protecció de l'interessat o dels drets i llibertats d'altres	
• l'execució de demandes civils	

Si no aplica cap de les condicions anteriors, cal que la nova finalitat sigui compatible amb la finalitat que va motivar la recollida de les dades

Finalitat inicial	
Dades	
Nova finalitat	
Justificació de la compatibilitat	

Finalitat inicial	
Dades	
Nova finalitat	
Justificació de la compatibilitat	

2.2 Principis de licitud i la lleialtat

Base legal pel tractament

Un tractament és lícit si aplica alguna de les bases legals següents:

L'interessat ha donat el seu consentiment per al tractament de les seves dades personals, per una o diverses finalitats específiques.	
El tractament és necessari per executar un contracte en què l'interessat n'és part o per aplicar mesures precontractuals.	
El tractament és necessari per complir una obligació legal aplicable al responsable del tractament.	
El tractament és necessari per protegir interessos vitals de l'interessat o d'una altra persona física.	
El tractament és necessari per complir una missió feta en interès públic o en l'exercici de poders públics conferits al responsable del tractament.	
El tractament és necessari per satisfer els interessos legítims del responsable del tractament o d'un tercer, sempre que no hi prevalguin els interessos o els drets i les llibertats fonamentals de l'interessat (en particular, quan l'interessat és un menor).	
Justificació de la licitud del tractament	

A banda, cal que el tractament no incorri en cap il·lícit en un sentit més ampli. Per exemple, infringir el copyright o acords contractuals.

Confirma que el tractament no incorre en cap tipus d'il·lícit.

Tractament de dades de menors

Els menors necessiten una protecció especial en el tractament de les seves dades, perquè poden no ser conscients dels riscos que comporta.

El tractament ofereix serveis de la societat de la informació a nens i té com a base el consentiment?	Sí / No
En cas afirmatiu, s'ha tingut en compte l'edat mínima de consentiment?	Sí / No

Tractament de categories especials de dades

Es tracten dades de categories especials?	Sí / No

En cas afirmatiu
El tractament de categories especials de dades està prohibit, llevat que apliqui algun dels supòsits següents.

L'interessat ha donat el seu consentiment explícit per al tractament amb una finalitat específica, tret que el dret de la UE o de l'estat membre no ho permeti.	

El tractament és necessari per complir obligacions o per exercir drets en l'àmbit del dret laboral i de la seguretat i la protecció social.	
El tractament és necessari per protegir interessos vitals de l'interessat o d'una altra persona, i l'interessat no està capacitat per donar el consentiment.	
El tractament és necessari per protegir interessos vitals de l'interessat o d'una altra persona física.	
El tractament és legítim i amb garanties, fet per una associació sense ànim de lucre de caràcter polític, filosòfic, religiós o sindical, sempre que el tractament afecti persones amb qui mantenen contactes en relació amb aquestes finalitats i les dades no es comuniquin a tercers sense el consentiment dels interessats.	
El tractament fa referència a dades que l'interessat ha fet públiques.	
El tractament és necessari per formular, exercir o defensar reclamacions, o quan els tribunals actuen en la seva funció judicial.	
El tractament és necessari per raons d'interès públic essencial.	
El tractament és necessari per a finalitats de medecina preventiva o laboral, avaluació de la capacitat laboral del treballador, diagnòstic mèdic, prestació d'assistència o tractament de tipus sanitari o social.	
El tractament és necessari per raons d'interès públic en l'àmbit de la salut pública.	
El tractament és necessari amb la finalitat d'arxiu amb interès públic, investigació científica o històrica, o amb finalitat estadística.	
Justificació de la licitud del tractament de dades de categories especials.	

Tractament de dades penals

Es tracten dades relatives a condemnes o infraccions penals?	Sí / No

En cas afirmatiu

Tot i que les dades relatives a condemnes o infraccions penals no són categories especials de dades, hi ha un requisit addicional per tractar-les: el tractament només és pot portar a terme sota la supervisió de les autoritats públiques o quan ho autoritzi el dret de la unió o de l'estat membre.

Justificació de la licitud del tractament de dades penals.

Validesa del consentiment

Si un tractament té com a base legal el consentiment, cal que es compleixin les següents condicions perquè aquest sigui vàlid:

El responsable ha de poder demostrar que l'ha recollit.	
La sol·licitud de consentiment és intel·ligible, de fàcil accés i en un llenguatge clar.	

L'execució d'un contracte no es pot supeditar a rebre el consentiment respecte de dades personals no necessàries per executar el contracte.	
S'ha informat els interessats de la possibilitat de retirar el consentiment en qualsevol moment.	

Transferències de dades

Per evitar que els interessats vegin reduïts els seus drets, el RGPD és especialment restrictiu amb les transferències de dades amb països on el RGPD no aplica.

És fan transferències a tercers països o a organitzacions internacionals?	Sí / No

En cas afirmatiu

Aquestes transferències estan permeses si la Comissió Europea considera que el país o organització ofereix un nivell adequat de protecció, si s'han establert les garanties suficients segons l'article 46 o si aplica alguna de les excepcions de l'article 49.

Dades transferides	
País	
Condició que permet la transferència	

Dades transferides	
País	
Condició que permet la transferència	

Lleialtat del tractament

Un tractament és lleial si fa un ús de les dades previsible per part dels interessats, i del tractament no se'n deriven conseqüències adverses pels interessats que no siguin justificables.

Justificació de tractament lleial

2.3 Principi de minimització

Les dades han de ser adequades, rellevants i limitades a l'estrictament necessari per acomplir la finalitat del tractament.

Tipus de dades	
Justificació de l'adequació, la rellevància i la necessitat	

Tipus de dades	

Justificació de l'adequació, la rellevància i la necessitat

2.4 Principi de limitació del termini de conservació

Les dades personals no s'han de conservar més temps de l'estrictament necessari per complir amb la finalitat del tractament. A la descripció del tractament, es va especificar el termini de conservació de les dades. Cal justificar que els terminis donats compleixen el principi de limitació del termini de conservació.

Justificació que els terminis de conservació donats compleixen amb la limitació del termini de conservació.

Cal que els mecanismes establerts per esborrar les dades siguin efectius (és automàtic o s'ha d'activar manualment? romanen les dades a les còpies de seguretat del sistema un cop esborrades? quant de temps i com es garanteix que no es tracten? etc.).

Descriu els mecanismes establerts per esborrar les dades.

Les dades es poden conservar indefinidament amb finalitat d'arxiu en interès públic, amb finalitat d'investigació científica o històrica, o amb finalitat estadística.

Es conserven dades amb finalitat d'arxiu en interès públic, amb finalitat d'investigació científica o històrica, o amb finalitat estadística.	
En cas afirmatiu, quines mesures s'han implantat per garantir el principi de minimització.	

2.5 Principi d'exactitud

El tractament de dades inexactes pot afectar negativament les persones. El principi d'exactitud demana que les dades siguin exactes i que es prenguin les mesures adequades per garantir que les que siguin inexactes s'actualitzin o s'esborrin sense dilació.

Controls de la qualitat de les dades

Mesures per corregir les dades

2.6 Riscos per les persones

L'objectiu d'aquest punt és identificar els possibles efectes negatius sobre les persones, quantificar-los i si és necessari proposar mesures per mitigar-los.

En aquesta secció avaluarem el tractament tal i com està dissenyat. És a dir, no considerem els casos en que falla la seguretat del sistema (sigui aquesta fallada accidental o intencionada).

En la identificació dels potencials efectes negatius del tractament sobre les persones convé tenir en compte el punt de vista dels interessats i del delegat de protecció de dades.

Potencials efectes negatius del tractament sobre les persones

Per cadascun dels efectes negatius identificats, cal estimar el nivell de risc associat. El risc depèn de dos factors: l'impacte que té sobre les persones (baix, mitjà, alt o molt alt) i la probabilitat que es materialitzi (baixa, mitjana, alta). L'impacte s'estima directament dels potencials efectes. Per determinar la probabilitat, cal analitzar en quines circumstancies fan que els efectes negatius és materialitzin (les amenaces) i estimar la probabilitat d'aquestes.

El risc es determina, en funció de l'impacte i de la probabilitat, seguint la taula següent:

Probabilitat	Alta	Risc Mitjà	Risc Alt	Risc Alt	Risc Alt
	Mitjana	Risc Baix	Risc Mitjà	Risc Alt	Risc Alt
	Baixa	Risc Baix	Risc Baix	Risc Mitjà	Risc Alt
		Baix	Mitjà	Alt	Molt Alt
		Impacte			

Primer s'estimarà el risc associat a cada amenaça. El risc global serà el màxim dels riscos de les amenaces.

Efecte sobre les persones:

Impacte:

Amenaça	Probabilitat	Risc

Risc estimat:

Efecte sobre les persones:

Impacte:

Amenaça	Probabilitat	Risc

Risc estimat:

Llevat que el risc sigui baix, cal buscar mesures per reduir-lo. Això és especialment necessari en els casos de risc alt o molt alt. Si no és possible reduir un risc alt, abans de començar el tractament cal consultar l'autoritat de protecció de dades competent sobre la idoneïtat del tractament.

En cas que s'hagi alterat el tractament inicial per fer-lo menys lesiu per les persones, caldrà revisar i actualitzar les seccions anteriors de l'AIPD.

2.7 Necessitat i Proporcionalitat del Tractament

Amb la informació recollida en aquesta secció, cal justificar que el tractament és necessari (propòsit buscat no es pot atènyer amb cap altre mesura més moderada) i proporcional (no provoca més danys que beneficis).

Justificació de l'eficàcia del tractament pel propòsit que és busca.

Justificació de la necessitat del tractament.

Justificació de que el tractament és proporcional

2.8 Opinió dels interessats

L'RGPD estableix que, si és possible, cal recollir l'opinió dels interessats sobre el tractament.

Opinió dels interessats sobre la necessitat i la proporcionalitat del tractament.

En cas que no es considera apropiat recollir l'opinió dels interessats, cal justificar-ho.

Per què no s'ha recollit l'opinió dels interessats?

Si l'opinió dels interessats respecte al tractament difereix de la visió que el responsable ha donat a l'apartat 2.7 i es pretén portar endavant el tractament, cal justificar el perquè.

Per què es porta endavant el tractament tot i les discrepàncies dels interessats?

3. Controls per Garantir els Drets de les Persones

3.1 Controls pel dret a tenir informació transparent

La transparència és transversal i ha de ser present en totes les comunicacions amb els interessats.

Tota comunicació amb els interessats ha de ser concisa, intel·ligible, de fàcil accés i ha de fer ús d'un llenguatge clar i senzill.	✓ ✗

El reglament regula com s'ha de fer aquesta comunicació

La informació es donarà per escrit (incloent mitjans electrònics).	✓ ✗
Pel cas de peticions fetes amb mitjans electrònics, la informació es donarà preferentment de forma electrònica.	✓ ✗
Si l'interessat ho demana, la informació es donarà oralment.	✓ ✗

El responsable ha de respondre les peticions d'exercici de drets d'un interessat dins uns terminis establerts:

Sense demora indeguda i no més enllà d'un mes.	✓ ✗
Si la complexitat o el número de peticions ho justifica, es pot estendre el període en dos mesos. En aquest cas cal informar de les raons dins el primer mes.	✓ ✗

Si el responsable no ha de respondre a la petició d'exercici de drets d'un interessat, cal:

Avisar l'interessat d'aquest fet sense demora indeguda i com a màxim en un mes.	✓ ✗
Explicar les raons per no portar a terme la petició (per exemple, la petició és repetitiva o el responsable no pot identificar l'interessat).	✓ ✗
Informar de la possibilitat de recorre la decisió davant una autoritat supervisora o un jutjat	✓ ✗

Només si la petició és excessiva (per exemple, per repetitiva), es podrà cobrar un càrrec per cobrir els costos de tramitar-la.	✓ ✗

3.2 Controls pel dret d'informació

A l'hora de recollir dades personals, el responsable del tractament ha d'informar els interessats de diferents aspectes del tractament.

Els articles 13 i 14, especifiquen que cal informar els interessats dels punts a la taula següent:

La identitat i les dades de contacte del responsable	✓ ✗

Les dades de contacte del delegat de protecció de dades (si n'hi ha)	✓ ✗
La finalitat del tractament	✓ ✗
La base legal del tractament	✓ ✗
L'interès legítim del responsable, si aquesta és la base legal del tractament	✓ ✗
Els destinataris o categories de destinataris de les dades	✓ ✗
El termini de conservació de les dades o el criteri emprat per determinar-lo	✓ ✗
La intenció de transmetre les dades fora de la UE, si escau	✓ ✗
La decisió de la Comissió Europea respecte de la suficiència de la seguretat que ofereix el país o organització destinatària	✓ ✗
L'existència del dret d'accés a les dades	✓ ✗
L'existència del dret de rectificació i supressió	✓ ✗
L'existència del dret de limitació del tractament	✓ ✗
L'existència del dret d'oposició al tractament	✓ ✗
L'existència del dret de portabilitat de dades	✓ ✗
L'existència del dret a revocar el consentiment (si aquesta és la base legal del tractament)	✓ ✗
L'existència del dret a presentar una reclamació davant una autoritat de control	✓ ✗
Que la comunicació de les dades és un requisit legal o contractual, si escau	✓ ✗
L'existència de decisions automatitzades	✓ ✗
El propòsit de fer servir dades amb una finalitat diferent a la que va motivar la recollida, si s'escau.	✓ ✗
La procedència de les dades, si no s'han obtingut directament de la persona interessada.	✓ ✗

Hi ha algunes exempcions a l'obligatorietat d'informar, que depenen de la forma en que s'han recollit les dades.

- Si les dades s'han obtingut directament de l'interessat, no hi ha l'obligació d'informar-lo si ja disposa de la informació.
- Si les dades no s'han obtingut directament de l'interessat, no cal informar-lo si es dona alguna de les següents condicions[1]: l'interessat ja disposa d'aquesta informació, la comunicació és impossible o suposa un esforç desproporcionat, així està regulat per una norma de la UE o dels estats membres o la informació té caràcter confidencial sobre la base del secret professional.

Si no s'informa, cal justificar-ho.

S'aplica el dret d'informació a totes les dades tractades?	
Si aplica alguna exempció al dret d'informació, cal dir quina, a quines dades i justificar el perquè.	

[1] RGPD, article 14.5.

Si s'informa els interessats, el Reglament determina quan cal fer-ho[1].

Si les dades es recullen directament dels interessats, en el moment de recollir-les.	✓ ✗
Si les dades es recullen indirectament, cal complir les condicions següents:	
• En un període raonable de temps i no superior a un mes.	✓ ✗
• Si ens comuniquem amb els interessats, com a molt tard en el moment de la primera comunicació.	✓ ✗
• Si es volen comunicar les dades a tercers, abans de comunicar-les.	✓ ✗

3.3 Controls per garantir el dret d'accés

L'interessat té el dret d'obtenir del responsable del tractament la confirmació que s'estan tractant les seves dades i, en aquest cas, el dret d'accés a les dades personals i a la informació següent:

La finalitat del tractament	✓ ✗
Les categories de dades tractades	✓ ✗
Els destinataris de les dades	✓ ✗
El termini de conservació de les dades	✓ ✗
Els drets a rectificar i suprimir les dades	✓ ✗
Els drets a limitar i oposar-se al tractament	✓ ✗
El dret a reclamar davant una autoritat de control	✓ ✗
Si les dades no s'han obtingut de l'interessat, l'origen de les dades	✓ ✗
L'existència de decisions automatitzades, si escau	✓ ✗
Garanties en la transferència de dades fora de la UE, si escau	✓ ✗

A banda de conèixer quina informació s'ha de transmetre als interessats, cal assegurar-se que es donen les condicions per fer efectiu el dret d'accés.

S'ha establert un procediment estàndard per la gestió de sol·licituds d'accés?	✓ ✗
El personal que tracta amb les persones interessades té la formació necessària per reconèixer les sol·licituds d'accés?	✓ ✗

3.4 Controls per garantir el dret de rectificació

Les persones tenen el dret a que és rectifiquin les seves dades, si aquestes no són exactes.

S'ha establert un procediment per la gestió de sol·licituds de rectificació?	✓ ✗
El personal que tracta amb les persones interessades té la formació necessària per reconèixer les sol·licituds de rectificació?	✓ ✗

[1] GDPR art 13(1) i 14(3),

Si el responsable ha compartit les dades, cal que informi els destinataris sobre la rectificació.

S'ha establert un procediment per notificar la rectificació als destinataris?	✓ ✗

3.5 Dret de supressió

Les persones tenen el dret a que s'esborri la seva informació quan es dona algun dels següents casos:

- Les dades ja no són necessàries en relació amb la finalitat per què es van recollir.
- L'interessat treu el seu consentiment i no hi ha cap altra base legal pel tractament.
- L'interessat s'oposa al tractament i no hi ha cap altre factor superior que el legitimi.
- Les dades s'han tractat sense una base legal.
- Les dades s'han d'esborrar d'acord amb una obligació legal que afecta el responsable.
- Les dades s'utilitzen per oferir serveis de la societat de la informació a nens.

En canvi, el dret de supressió no aplica en els següents casos:

- Per exercir el dret a la llibertat d'expressió i d'informació.
- Per complir una obligació legal o en l'interès públic.
- Amb la finalitat d'arxiu en interès públic, amb finalitat d'investigació científica o històrica, i amb finalitat estadística (si el compliment d'aquestes finalitats es veiés afectat per la supressió de les dades).
- Per presentar, exercir o defensar reclamacions legals.

El personal té capacitat per decidir si aplica el dret a supressió?	✓ ✗

Es recomanable establir un canal estàndard perquè els interessats puguin demanar de fer efectiu el dret de supressió. Ara bé, cal assegurar-se que el personal està capacitat per detectar les sol·licituds que es facin per altres mitjans.

S'ha establert un procediment per la gestió de sol·licituds de supressió?	✓ ✗
El personal que tracta amb les persones interessades té la formació necessària per reconèixer les sol·licituds de supressió?	✓ ✗

Si el responsable del tractament comparteix les dades, ha de prendre les mesures apropiades (tenint en compte els costos i la tecnologia disponible) per notificar els destinataris sobre la petició de supressió.

S'ha establert un procediment per notificar la petició de supressió als destinataris?	✓ ✗

3.6 Dret a limitar el tractament

L'article 18 dona a les persones el dret a limitar el tractament de les seves dades, en els casos següents:

- L'interessat ha demanat la rectificació de les seves dades i el responsable està verificant si són exactes.
- Les dades s'han tractat sense una base legal.
- L'interessat necessita que el responsable guardi les dades per iniciar, exercir o defensar una reclamació.
- L'interessat s'ha oposat al tractament i el responsable està avaluant si els motius legítims del responsable prevalen sobre els de l'interessat.

El personal està capacitat per decidir si aplica el dret a limitar el tractament?	✓ ✗

Cal assegurar-se que el personal està capacitat per detectar les sol·licituds de limitació del tractament.

S'ha establert un procediment per la gestió de sol·licituds de limitació del tractament?	✓ ✗
El personal que tracta amb les persones interessades té la formació necessària per reconèixer les sol·licituds de limitació del tractament?	✓ ✗

A l'hora de limitar el tractament, cal tenir en compte les diferents formes que aquest pot tenir: recollida de dades, anàlisi de dades, disseminació de resultats, etc.

Es tenen en compte totes les possibles formes de tractament a l'hora de limitar-lo?	✓ ✗

Si s'han compartit dades, cal informar els destinataris de les peticions de limitació del tractament.

S'ha establert un procediment per notificar la petició de limitació del tractament als destinataris?	✓ ✗

3.7 Dret a la portabilitat de les dades

Les persones tenen el dret a demanar les dades que han facilitat al responsable del tractament en els següents cassos:

- Si el tractament està basat en el consentiment, o és necessari per executar un contracte o per aplicar mesures precontractuals.
- El tractament es fa amb mitjans automatitzats.

El dret a la portabilitat de dades no es limita a les dades que les persones han donat de forma explicita; també afecta les dades que s'han recollit de l'observació de les persones.

El personal està capacitat per decidir si aplica el dret a la portabilitat de dades?	✓ ✗

El dret a la portabilitat de dades no ha d'afectar negativament a altres persones. En particular:

- Si les dades personals contenen informació d'una tercera persona, cal avaluar si aquesta darrera pot veure afectats els seus drets i llibertats.

- Si les dades estan associades a diverses persones (per exemple, un compte bancari compartit), cal buscar el consens de tots els interessats.

El procediment per fer efectiu el dret a la portabilitat de dades té en compte l'efecte sobre els drets i les llibertats de les altres persones?	✓ ✗

Cal assegurar-se que el personal està capacitat per detectar les sol·licituds de portabilitat de dades.

S'ha establert un procediment per la gestió de sol·licituds de portabilitat de dades?	✓ ✗
El personal que tracta amb les persones interessades té la formació necessària per reconèixer les sol·licituds de portabilitat de dades?	✓ ✗

El reglament determina la forma en la que s'ha de fer la portabilitat.

S'usa un format estructurat, d'ús comú i que sigui de fàcil lectura mecànica?	✓ ✗

3.8 Dret d'oposició

Les persones tenen el dret a oposar-se al tractament de la seva informació quan aquest tractament es fa sobre la base de:

- L'interès públic o l'exercici de poders públics conferits al responsable del tractament.
- L'interès legítim del responsable del tractament.

En aquest cas, el responsable ha de cessar en el tractament, llevat que acrediti motius legítims que prevalguin sobre els drets de l'interessat.

El personal està capacitat per decidir si aplica el dret a d'oposició?	✓ ✗

Cal assegurar-se que el personal està capacitat per detectar les sol·licituds d'oposició.

S'ha establert un procediment per la gestió de sol·licituds d'oposició al tractament?	✓ ✗
El personal que tracta amb les persones interessades té la formació necessària per reconèixer les sol·licituds d'oposició al tractament?	✓ ✗

El reglament especifica com s'ha d'actuar en rebre una petició d'oposició al tractament en diversos casos.

Si la petició s'oposa al tractament amb finalitats de màrqueting, aquesta ha de ser acceptada sense excepció.	✓ ✗
Si la petició s'oposa al tractament amb finalitat d'investigació científica o històrica, o amb finalitat estadística, ha de ser acceptada llevat que el tractament es faci en l'interès públic.	✓ ✗

3.9 Dret a no ser objecte de decisions automatitzades

Es fa un tractament automatitzat que té efectes jurídics o altres efectes significatius per les persones?	SÍ / No

En cas afirmatiu, quina base legal que ho permet?	
• És necessari per l'execució d'un contracte entre l'interessat i el responsable	
• Està autoritzat pel dret de la unió o d'un estat membre	
• L'interessat ha donat el seu consentiment explícit	

L'interessat sempre té dret a obtenir intervenció humana, a expressar el seu punt de vista i a impugnar la decisió.

Existeix un procediment perquè les persones puguin demanar intervenció humana, expressar el seu punt de vista i impugnar la decisió?	✓ ✘
Hi ha personal a l'organització amb la capacitat de revisar les decisions i canviar-les?	✓ ✘

Les decisions automatitzades només poden fer ús de categories especials de dades si hi ha el consentiment explícit de l'interessat, o si el tractament es fa per protegir els interessos vitals de l'interessat o d'una altra persona.

Es fa ús de categories especials de dades en el tractament automàtic?	Sí / No
En cas afirmatiu, quina base legal que ho permet?	
• L'interessat ha donat el seu consentiment explícit	
• El tractament es fa per protegir els interessos vitals de l'interessat o d'una altra persona	

4. Riscos en la Seguretat de les Dades

D'acord amb l'RGPD, les mesures emprades per protegir la informació han de ser apropiades al risc per als drets i les llibertats de les persones. En aquesta secció seguim una metodologia senzilla per analitzar els riscos relacionats amb la seguretat de les dades. És a dir, els riscos associats a la pèrdua de la confidencialitat, de la integritat i de la disponibilitat de les dades.

4.1 Impacte

Avaluem l'impacte que la pèrdua de la confidencialitat, de la integritat i de la disponibilitat de les dades personal tenen sobre la persona interessada.

Per fixar l'impacte sobre les persones de la pèrdua de la seguretat de les dades, cal tenir en compte les característiques del tractament. Entre d'altres:

- El tractament dades de categories especials o altres dades especialment sensibles (informació financera, localitzacions, etc.).
- La monitorització de persones.
- El tractament de dades de grups amb necessitats especials (menors, autoritats, etc.).
- El tractament de gran quantitat de dades de cada persona.

Amb l'objectiu de contextualitzar el càlcul de l'impacte, es plantegen diferents d'escenaris en que es perd alguna d'aquestes propietats.

Impacte que la pèrdua de la confidencialitat de les dades (és a dir, d'un accés no autoritzat a les dades) té sobre les persones. Exemples de casos de pèrdua de confidencialitat: • Pèrdua o robatori d'un ordinador que conté dades personals. • Enviament per error de dades personals a persones no autoritzades. • Possibilitat d'accedir de forma no autoritzada al compte d'una persona. • Un error de configuració en una web exposa les dades personals dels seus usuaris. • Robatori d'informació de les instal·lacions del responsable o de l'encarregat del tractament. • Un empleat d'un centre mèdic consulta de forma no autoritzada l'expedient d'un pacient.
Impacte ☐Baix ☐Mitjà ☐Alt ☐Molt alt
Justificació

Impacte que la pèrdua de la integritat de les dades (és a dir, de la modificació no autoritzada de les dades) té sobre les persones. Exemples de casos de pèrdua de la integritat: • Un empleat modifica per error les dades d'un client. • Un error en la xarxa de comunicacions altera les dades mentre estan en trànsit. • Per motius operacionals, una empresa manté diverses còpies de les dades, però un canvi en alguna de les còpies no és propaga a les altres. • Pèrdua de part d'un expedient, com a conseqüència d'una fallada en el sistema de tractament.
Impacte ☐Baix ☐Mitjà ☐Alt ☐Molt alt
Justificació

Impacte que la pèrdua de la disponibilitat de les dades té sobre les persones. Exemples de casos de pèrdua de la disponibilitat: • Un fitxer és corromp o s'esborra i no hi ha una còpia de seguretat. • Es perd un expedient del qual només hi havia una còpia en paper. • Un servei de consulta de dades deixa d'estar disponible (per exemple, el servei per accedir al registres electrònics de salut).
Impacte ☐Baix ☐Mitjà ☐Alt ☐Molt alt
Justificació

L'impacte del sistema serà el màxim dels tres.

Impacte ☐Baix ☐Mitjà ☐Alt ☐Molt alt

4.2 Probabilitat inicial

La taula següent mostra característiques del tractament que incrementen els riscos de seguretat de les dades. Estimarem la probabilitat de fallada en la seguretat en funció del número de característiques es compleixen.

Maquinari i programari	
P1. El sistema de tractament està connectat a sistemes externs a l'organització? La connexió amb sistemes externs a l'organització incrementa l'exposició a amenaces. Per exemple, la informació pot ser capturada o modificada maliciosament mentre està en trànsit. Exemples: • El sistema de tractament d'un hospital està connectat amb els sistema públic de seguretat social i amb els sistemes de d'asseguradores privades. • Les estacions de treball que formen part del sistema de tractament tenen accés a internet.	☐Sí ☐No
Q2. Alguna part del tractament es fa a través d'internet? La interacció amb els interessats a través d'internet exposa el sistema de tractament a amenaces externes, com ara *phishing*, SQL *injection*, *man-in-the-middle attacks*, DoS i XSS. Aquestes amenaces poden comprometre el sistema de tractament i afectar les propietats de seguretat de les dades (confidencialitat, integritat i disponibilitat). Permetre que els treballadors accedeixin al sistema de tractament a través d'internet també incrementa l'exposició a atacs externs i, a banda, incrementa la possibilitat que els treballadors facin un mal ús de la informació (accidental o intencionat). Exemples: • Botiga en línia, banca en línia, etc. • S'utilitza el correu electrònic en el tractament. • Els administradors del sistema de tractament poden fer tasques de manteniment o supervisió a través d'internet. L'accés al sistema de tractament des d'un espai públic pot facilitar que persones alienes a l'organització puguin observar-les	☐Sí ☐No

P3. Manca de seguiment d'un document de bones pràctiques rellevant en el disseny o la configuració del sistema de tractament? Si el sistema de tractament no està ben dissenyat o els elements que el componen no estan configurats adequadament, els riscos per a la seguretat de les dades s'incrementen. Hi ha multitud de guies de bones pràctiques en seguretat amb diferent temàtica (xarxa, equips, etc.). Exemples: • Cal dissenyar la xarxa seguint un document de bones pràctiques que inclogui elements com ara tallafocs, segmentació de la xarxa i ús de VPN. • Cal fer ús d'un document de bones pràctiques, a l'hora de configurar el sistema operatiu. Això implica mesures com ara l'ús d'antivirus i no permetre l'ús de paraules de pas insegures. • Cal dimensionar el sistema de tractament pensant en les necessitats computacionals, de comunicació i d'emmagatzematge que s'anticipen. També cal dotar-lo del personal suficient. • Cal fer ús d'un document de bones pràctiques, a l'hora de configurar el programari. Per exemple, com configurar un servidor web per fer-lo més segur. • Cal usar una metodologia de desenvolupament que tingui en compte la seguretat de les dades durant tot el cicle de vida de l'aplicació.	☐Sí ☐No
P4. Manca de seguiment d'un document de bones pràctiques rellevant en el manteniment, la monitorització i la resposta a incidents del sistema de tractament? És essencial fer un manteniment i una monitorització adequada del sistema. El manteniment s'ha de fer tant dels dispositius com del programari. Monitoritzar el sistema no només permet analitzar un incident un cop s'ha produït, sinó que també ajuda a detectar comportaments sospitosos a fi d'evitar que l'incident tingui lloc, o per reduir-ne l'impacte. Exemples: • No aplicar les actualitzacions de seguretat del sistema operatiu pot donar lloc a nous vectors d'atac. • La manca de còpies de seguretat regulars pot donar lloc a la pèrdua d'informació en cas d'incident.	☐Sí ☐No

P5. Hi ha una manca de seguretat física a les instal·lacions on té lloc el tractament? La seguretat física de les instal·lacions de tractament és essencial. Sense això, no es pot garantir la seguretat del sistema de tractament (ja sigui electrònic o no). Exemples: • El CPD no està degudament protegit amb un sistema que impedeix l'accés a les persones no autoritzades. • Les limitacions d'espai han fet que part de l'arxiu en paper s'hagi distribuït en diferents àrees, que no en garanteixen la seguretat. • El CPD no està protegit contra accidents naturals i industrials (per exemple, fallades elèctriques, inundacions). • És fa ús d'un servei al núvol sense tenir garanties que les instal·lacions proveïdor estan prou protegides.	☐Sí ☐No

Ús del sistema de tractament	
P6. Hi ha una manca de claredat en la definició dels rols i les responsabilitats dels treballadors? Una manca de claredat en la definició dels rols i les responsabilitats pot donar lloc a un ús descontrolat de les dades (ja sigui accidental o intencionat). Exemples: • Un treballador d'una oficina bancària només hauria de consultar les dades dels seus clients. • Els treballadors són responsables de destruir la informació (digital o no) de forma segura, quan deixa de ser necessària. • Els treballadors són responsables de mantenir la seguretat de les dades, quan les comuniquen a alguna altra persona o organització.	☐Sí ☐No
P7. Hi ha manca de claredat en la definició dels usos acceptables dels sistemes de tractament? Quan els usos acceptables dels sistemes de tractament no estan definits clarament, s'incrementa el risc de fer-ne un mal ús i d'introduir vulnerabilitats al sistema. Exemples: • La instal·lació de programari de compartició de fitxers pot donar lloc a la compartició involuntària de fitxers. • La instal·lació de programari per part d'usuaris no administradors pot donar lloc a un manteniment deficient. • Visitar pàgines web malicioses pot set una font d'entrada de programari maliciós i de robatori de dades.	☐Sí ☐No

P8. Pot el personal connectar dispositius externs al sistema? La connexió de dispositius externs al sistema de tractament és una porta a l'entrada de programari maliciós, d'introducció de vulnerabilitats, etc. A banda, també facilita l'extracció d'informació. Exemples: • El personal connecta el seu telèfon o el seu llapis de memòria als ports USB de l'ordinador. • El personal pot emprar els seus dispositius per efectuar tasques relacionades amb el tractament (BYOD).	☐Sí ☐No
P9. Manca un procediment adequat de registre i supervisió de les activitats relacionades amb el tractament? La manca d'un registre de les activitats (*log file*) pot incrementar les males pràctiques del personal i, alhora, dificulta la investigació dels incidents un cop s'han produït. Exemples: • Es poden consultar els expedients de clients/pacients sense que en quedi un registre. • Tot i que es genera un registre d'activitats, no es monitoritza. • No hi ha constància de les persones que entren al CPD.	☐Sí ☐No

Persones que intervenen en el tractament	
P10. El personal rep permisos que no són necessaris per complir les tasques que té encomanades? Com més gran sigui la base de persones que tenen accés a unes dades, més gran és la probabilitat que es produeixi un abús. Per evitar això, és essencial que el sistema controli l'accés al sistema del personal i autoritzi només els accessos que són estrictament necessaris per complir les tasques que té encomanades. Exemples: • L'accés a l'historial clínic d'un pacient hauria d'estar limitat als professionals que el tracten.	☐Sí ☐No
P11. S'ha externalitat alguna part del tractament a un encarregat? L'externalització del tractament o part del tractament a un encarregat suposa una pèrdua de control sobre les dades. Cal escollir un encarregat que pugui oferir un nivell alt de seguretat i definir clarament les seves responsabilitats. Exemples: • S'utilitza un núvol per realitzar part del tractament. • Es contracten uns serveis especialitzats per analitzar unes dades.	☐Sí ☐No

P12. Hi ha una manca de coneixement del personal respecte de l'ús adequat del sistema, d'aspectes de seguretat de les dades o de les limitacions d'ús que imposa l'RGPD? Una manca de coneixements sobre l'ús que s'espera del sistema, sobre seguretat de la informació o sobre les obligacions i limitacions que imposa l'RGPD pot donar lloc a males pràctiques. Exemples: • La manca de coneixements en seguretat pot fer que el personal que tracta les dades sigui més propens a seguir les instruccions d'un correu de *phishing*. • El personal ha de recordar la necessitat de desar els document físics sota les condicions de seguretat adequades.	☐Sí ☐No

Altres característiques	
P13. Ha patit l'empresa o altres empreses del sector atacs darrerament? L'existència d'atacs anteriors s'ha de prendre com una advertència de potencials atacs futurs. Convé prendre les mesures necessàries per evitar que atacs similars tinguin èxit.	☐Sí ☐No
P14. S'han rebut queixes d'alguna persona respecte de l'estabilitat o la seguretat del sistema de tractament darrerament? La presència d'errors en el sistema de tractament incrementa la probabilitat de patir un atac. De la mateixa manera, les advertències respecte de potencials fallades en la seguretat del sistema també poden indicar una probabilitat més alta de patir atacs. Exemples: • En entrar dades incorrectes en un formulari, l'aplicació de tractament mostra un error i finalitza de forma inesperada. • S'ha rebut la notificació d'un usuari que el sistema és vulnerable a algun atac específic.	☐Sí ☐No
P15. Es tracten dades d'especial interès o dades d'un nombre molt gran d'usuaris? La presència massiva de dades i la presència de dades d'especial interès són una motivació extra per als possibles atacants. Exemple: • Una gran empresa que emmagatzema dades personals i financeres dels seus clients (per exemple, número de targeta de crèdit).	☐Sí ☐No

Calculem la probabilitat inicial de en funció del nombre de respostes afirmatives d'acord amb la taula següent:

Respostes Afirmatives	Probabilitat inicial
0 - 4	Baixa
5 – 9	Mitjana
10 - 15	Alta

Nombre de respostes afirmatives:	
Probabilitat inicial estimada:	

4.3 Risc inicial

Un cop estimat l'impacte i la probabilitat inicial, aplicaquem la taula de la Secció 2.6 per calcular el risc inicial (sense els controls de seguretat).

Impacte sobre la confidencialitat Impacte sobre la integritat Impacte sobre la disponibilitat	
Màxim dels impactes Probabilitat	
Risc inicial	

4.4 Controls de seguretat

Un cop calculat el risc inicial, cal determinar quins controls (mesures per millorar la seguretat) s'han d'aplicar.

Hi ha moltes llistes de controls. Aquí fem ús dels controls que l'ENS (Esquema Nacional de Seguretat). A la guia sobre AIPD es més detalls sobre els controls i indicacions per determinar quins aplicar.

Baix	Mitjà	Alt	Control	Aplicat
Marc organitzatiu				
Sí	Sí	Sí	Política de seguretat [org.1] (sistema)	
Sí	Sí	Sí	Normativa de seguretat [org.2] (sistema)	
Sí	Sí	Sí	Procediments de seguretat [org.3] (sistema)	
Sí	Sí	Sí	Procés d'autorització [org.4] (sistema)	
Marc Operacional				
				Planificació
Sí	Sí	Sí	Arquitectura de seguretat [op.pl.2] (sistema)	
Sí	Sí	Sí	Adquisició de noves components [op.pl.3] (sistema)	
No	Sí	Sí	Dimensionament [op.pl.4] (D)	
No	No	Sí	Components certificats [op.pl.5] (sistema)	
				Control d'accés
Sí	Sí	Sí	Identificació [op.acc.1] (sistema)	
Sí	Sí	Sí	Requeriments d'accés [op.acc.2] (ICAT)	
No	Sí	Sí	Segregació de funcions i tasques [op.acc.3] (ICAT)	
Sí	Sí	Sí	Procés de gestió de drets d'accés [op.acc.4] (ICAT)	
Sí	Sí	Sí	Mecanisme d'autenticació [op.acc.5] (ICAT)	
Sí	Sí	Sí	Accés local [op.acc.6] (ICAT)	
Sí	Sí	Sí	Accés remot [op.acc.7] (ICAT)	
				Explotació
Sí	Sí	Sí	Inventari d'actius [op.exp.1] (sistema)	
Sí	Sí	Sí	Configuració de seguretat [op.exp.2] (sistema)	
No	Sí	Sí	Gestió de la configuració [op.exp.3] (sistema)	
Sí	Sí	Sí	Manteniment [op.exp.4] (sistema)	
No	Sí	Sí	Gestió de canvis [op.exp.5] (sistema)	
Sí	Sí	Sí	Protecció contra codi maliciós [op.exp.6] (sistema)	
No	Sí	Sí	Gestió d'incidències [op.exp.7] (sistema)	
No	No	Sí	Registre de l'activitat dels usuaris [op.exp.8] (sistema)	

No	Sí	Sí	Registre de la gestió d'incidències [op.exp.9] (sistema)	
No	No	Sí	Protecció dels registres d'activitat [op.exp.10] (sistema)	
No	No	Sí	Protecció de les claus criptogràfiques [op.exp.11] (sistema	
				Serveis externs
No	Sí	Sí	Contractació i acords de nivell de servei [op.ext.1] (sistema)	
No	Sí	Sí	Gestió diària [op.ext.2] (sistema)	
No	Sí	Sí	Mitjans alternatius [op.ext.3] (D)	
				Continuïtat del servei
No	Sí	Sí	Continuïtat del servei [op.cont.1] (D)	
No	No	Sí	Pla de continuïtat [op.cont.2] (D)	
No	No	Sí	Proves periòdiques [op.cont.3] (D)	
				Monitorització del sistema
No	No	Sí	Detecció d'intrusions [op.mon.1] (sistema)	
No	No	Sí	Sistema de mètriques [op.mon.2] (sistema)	
Mesures de protecció				
				Protecció de les instal·lacions i les infraestructures
Sí	Sí	Sí	Àrees separades i control d'accés [mp.if.1] (sistema)	
Sí	Sí	Sí	Identificació de les persones [mp.if.2] (sistema)	
Sí	Sí	Sí	Condicionament dels locals [mp.if.3] (sistema)	
No	Sí	Sí	Energia elèctrica [mp.if.4] (D)	
Sí	Sí	Sí	Protecció contra incendis [mp.if.5] (D)	
No	Sí	Sí	Protecció contra inundacions [mp.if.6] (D)	
Sí	Sí	Sí	Registre d'entrada i de sortida d'equipament [mp.if.7] (sistema)	
No	No	Sí	Instal·lacions alternatives [mp.if.8] (D)	
				Gestió del personal
No	No	Sí	Caracterització del lloc de treball [mp.per.1] (sistema)	
Sí	Sí	Sí	Deures i obligacions [mp.per.2] (sistema)	
Sí	Sí	Sí	Conscienciació [mp.per.3] (sistema)	
Sí	Sí	Sí	Formació [mp.per.4] (sistema)	
No	No	Sí	Personal alternatiu [mp.per.5] (D)	
Protecció dels equips				
No	Sí	Sí	Lloc de treball buidat [mp.eq.1] (sistema)	
No	Sí	Sí	Bloqueig del lloc de treball [mp.eq.2] (sistema)	
No	Sí	Sí	Protecció de portàtils [mp.eq.3] (sistema)	
No	Sí	Sí	Mitjans alternatius [mp.eq.4] (D)	
				Protecció de les comunicacions
Sí	Sí	Sí	Perímetre segur [mp.com.1] (sistema)	
No	Sí	Sí	Protecció de la confidencialitat [mp.com.2] (C)	
Sí	Sí	Sí	Protecció de l'autenticitat i de la integritat [mp.com.3] (IA)	
No	No	Sí	Segregació de xarxes [mp.com.4] (sistema)	
No	No	Sí	Mitjans alternatius [mp.com.5] (D)	
				Protecció dels suports de la informació
Sí	Sí	Sí	Etiquetat [mp.si.1] (C)	
No	Sí	Sí	Criptografia [mp.si.2] (IC)	
Sí	Sí	Sí	Custodia [mp.si.3] (sistema)	
Sí	Sí	Sí	Transport [mp.si.4] (sistema)	
No	Sí	Sí	Esborrat i destrucció [mp.si.5] (C)	
				Protecció de les aplicacions informàtiques
No	Sí	Sí	Desenvolupament d'aplicacions [mp.sw.1] (sistema)	

Sí	Sí	Sí	Acceptació i posada en servei [mp.sw.1] (sistema)	
				Protecció de la informació
Sí	Sí	Sí	Qualificació de la informació [mp.info.2] (C)	
No	No	Sí	Xifrat de la informació [mp.info.3] (C)	
Sí	Sí	Sí	Signatura electrònica [mp.info.4] (IA)	
No	No	Sí	Segells temporals [mp.info.5] (T)	
Sí	Sí	Sí	Neteja de documents [mp.info.6] (C)	
No	Sí	Sí	Còpies de seguretat [mp.info.7] (D)	
				Protecció dels serveis
Sí	Sí	Sí	Protecció del correu electrònic [mp.s.1] (sistema)	
Sí	Sí	Sí	Protecció de serveis i aplicacions web [mp.s.2] (sistema)	
No	Sí	Sí	Protecció contra la denegació de servei [mp.s.3] (D) (impacte, probabilitat)	
No	No	Sí	Mitjans alternatius [mp.s.9] (D) (impacte)	

4.5 Impacte residual

Els controls de seguretat poden reduir l'impacte d'un incident de seguretat. Per exemple, el xifratge de certa informació pot limitar l'extensió d'una pèrdua de confidencialitat, una còpia de seguretat pot limitar l'impacte d'una pèrdua de la disponibilitat de la informació i l'ús de signatura electrònica pot permetre la detecció, i per tant la reducció de l'impacte, d'una pèrdua de la integritat.

Impacte que la pèrdua de la confidencialitat de les dades (és a dir, d'un accés no autoritzat a les dades) té sobre les persones.				
Impacte	☐Baix	☐Mitjà	☐Alt	☐Molt alt
Impacte residual	☐Baix	☐Mitjà	☐Alt	☐Molt alt
Justificació				

Impacte que la pèrdua de la integritat de les dades (és a dir, de la modificació no autoritzada de les dades) té sobre les persones.				
Impacte	☐Baix	☐Mitjà	☐Alt	☐Molt alt
Impacte residual	☐Baix	☐Mitjà	☐Alt	☐Molt alt
Justificació				

Impacte que la pèrdua de la disponibilitat de les dades té sobre les persones.				
Impacte	☐Baix	☐Mitjà	☐Alt	☐Molt alt
Impacte residual				

☐Baix	☐Mitjà	☐Alt	☐Molt alt
Justificació			

L'impacte residual del sistema serà el màxim dels tres anteriors.

Impacte residual del sistema			
☐Baix	☐Mitjà	☐Alt	☐Molt alt

4.6 Probabilitat residual

Per reduir la probabilitat cal eliminar la casuística que fa que les preguntes de la secció 4.2 tinguin resposta afirmativa. Per exemple, si permetre el tractament a través d'internet no és essencial, podem desactivar-ho per fer negativa la resposta a la pregunta P2.

Moltes vegades no es factible eliminar la casuística associada a les preguntes de la secció 4.2. En aquest cas, per canviar una resposta afirmativa a negativa, cal justificar que, en el context del sistema de tractament, els controls implementats fan que l'objecte de la pregunta tingui un pes negligible en l'aparició d'incidents de seguretat.

Cal revisar les respostes donades en el càlcul de la probabilitat inicial tenint en compte els controls implementats..

Maquinari i programari		
Q1	**Està el sistema de tractament connectat a sistemes externs a l'organització?** Controls implementats i justificació	☐Sí ☐No
Q2	**Alguna part del tractament es fa a través d'internet?** Controls implementats i justificació	☐Sí ☐No
Q3	**Manca de seguiment d'un document de bones pràctiques rellevant en el disseny o la configuració del sistema de tractament?** Controls implementats i justificació	☐Sí ☐No
Q4	**Manca de seguiment d'un document de bones pràctiques rellevant en el manteniment, la monitorització i la resposta a incidents del sistema de tractament?** Controls implementats i justificació	☐Sí ☐No
Q5	**Hi ha una manca de seguretat física a les instal·lacions on té lloc el tractament?** Controls implementats i justificació	☐Sí ☐No

Procediments relacionats amb el tractament		
Q6	**Hi ha una manca de claredat en la definició dels rols i les responsabilitats dels treballadors?** Controls implementats i justificació	☐Sí ☐No
Q7	**Hi ha manca de claredat en la definició dels usos acceptables dels sistemes de tractament?** Controls implementats i justificació	☐Sí ☐No
Q8	**Pot el personal connectar dispositius externs al sistema?** Controls implementats i justificació	☐Sí ☐No
Q9	**Manca un procediment adequat de registre i supervisió de les activitats relacionades amb el tractament?** Controls implementats i justificació	☐Sí ☐No

Persones que intervenen en el tractament		
Q10	**El personal rep permisos que no són necessaris per complir les tasques que té encomanades?** Controls implementats i justificació	☐Sí ☐No
Q11	**S'ha externalitat alguna part del tractament a un encarregat?** Controls implementats i justificació	☐Sí ☐No
Q12	**Hi ha una manca de coneixement del personal respecte de l'ús adequat del sistema, d'aspectes de seguretat de les dades o de les limitacions d'ús que imposa l'RGPD?** Controls implementats i justificació	☐Sí ☐No

Altres característiques		
Q13	**Ha patit l'empresa o altres empreses del sector atacs darrerament?**	☐Sí ☐No
Q14	**S'han rebut queixes d'alguna persona respecte de l'estabilitat o la seguretat del sistema de tractament darrerament?**	☐Sí ☐No
Q15	**Es tracten dades d'especial interès o dades d'un nombre molt gran d'usuaris?**	☐Sí ☐No

La probabilitat residual es calcula comptant el número de respostes afirmatives.

Respostes Afirmatives	Probabilitat inicial
0 - 4	Baixa
5 – 9	Mitjana
10 - 14	Alta

4.7 Estimació del risc residual

Un cop estimat l'impacte residual i la probabilitat residual, calculem el risc residual seguint la taula de la Secció 2.6.

Probabilitat					
	Alta	Risc Mitja	Risc Alt	Risc Alt	Risc Alt
	Mitjana	Risc Baix	Risc Mitja	Risc Alt	Risc Alt
	Baixa	Risc Baix	Risc Baix	Risc Mitja	Risc Alt
		Baixa	Mitjana	Alta	Molt Alta
		Severitat			

Impacte residual sobre la confidencialitat Impacte residual sobre la integritat Impacte residual sobre la disponibilitat	
Màxim dels impactes residual Probabilitat residual	
Risc residual	

Si el risc residual és alt, cal proposar nous controls per reduir-lo. Si no és possible reduir-lo, abans d'iniciar el tractament cal consultar l'autoritat de protecció de dades competent sobre la seva idoneïtat..