PROTOCOLO INVESTIGACIÓN E INFORMACIÓN OBLIGATORIA INVESTIGADORES UNIVERSIDAD MIGUEL HERNÁNDEZ DE ELCHE

CONTROL DE EDICIÓN

FECHA	VERSIÓN	RESPONSABLE	DESCRIPCIÓN DE CAMBIOS
17/12/2020	01	Delegada Protección de datos UMH	Edición inicial.

ÍNDICE

1. INTRODUCCIÓN:

Esta Guía tiene por objetivo informar sobre los aspectos principales que en materia de protección de datos inciden en el campo de la investigación que se desarrolla en la UMH, así como, sensibilizar a la comunidad de personas investigadoras en esta materia y proporcionar una herramienta útil con el objeto de contribuir a que los proyectos de investigación cumplan con esta normativa de referencia.

Es importante que la persona investigadora estudie cuidadosamente las nociones, términos y explicaciones recogidas, así como, documentos externos (incluidos en la misma a través de enlaces), con el fin de facilitar la preparación de la solicitud de su proyecto de investigación ante el Comité Ético de la UMH para su aprobación.

La información contenida en este documento no responde a las circunstancias específicas de un proyecto de investigación o persona en concreto. Habida cuenta de lo anterior, su finalidad es informar de manera general sobre los aspectos más destacados e importantes que inciden en materia de protección de datos sobre los estudios, proyectos e investigaciones (en adelante investigaciones) con seres humanos, por lo tanto, en ningún caso, supone un asesoramiento jurídico vinculante.

La normativa de referencia aplicable es esencialmente, la siguiente:

- 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 y por el que se deroga la Directiva 95/46/CE (RGPD) Reglamento General de Protección de Datos (**en adelante, RGPD)**

- la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (**en adelante, LOPDGDD**)

Con respecto a la normativa en materia de salud e investigación:

- Ley 14/1986, de 25 de abril, General de Sanidad
- Ley 33/2011, de 4 de octubre, General de Salud Pública
- Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
- Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.
- Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias.
- La Ley 14/2007, de 3 de julio, de Investigación biomédica. Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios

En el caso, de que las personas investigadoras precisen de mayor

asesoramiento, podrán ponerse en contacto con la OIR, y en su caso con la Delegada de protección de datos, con el fin de realizar las consultas que consideren necesarias para proporcionar el adecuado tratamiento a los datos de carácter personal involucrados en su proyecto de investigación.

DATOS DE CONTACTO	
Oficina de Investigación Responsable (OIR)	**Delegación de Protección de datos (DPD)**
Tel. 965222687 oir@umh.es	Tel. 965222223 dpd@umh.es

2. ¿QUÉ ES LA PROTECCIÓN DE DATOS?

Desde un punto de vista legal, la protección de datos se plantea por objetivo establecer un equilibrio entre:

(a) los derechos de protección de datos de las personas físicas, y,
(b) la necesidad de que las organizaciones realicen un tratamiento de dichos datos de forma legal, justa y razonable.

Esto no implica en modo alguno que las personas investigadoras no puedan proceder al tratamiento de los datos personales en el curso de sus investigaciones, pero sí supone la asunción de obligaciones (legales, organizativas y técnicas) y el respeto de principios (seguridad, minimización, finalidad, plazo de conservación, etc.) al objeto de garantizar los derechos y libertades de las personas.

No debemos olvidar que el derecho de protección de datos es un derecho fundamental y en el contexto de las investigaciones podemos encontrar situaciones de hecho que podrían vulnerar el mismo, como por ejemplo la recopilación de datos de salud sin garantías, el uso de BIG DATA, inteligencia artificial, etc. Por ello, si bien es cierto que el RGPD apoya claramente la investigación científica, también nace para ser proteccionista y salvaguardar los derechos de las personas sujetas a investigación.

3. LA IMPORTANCIA DEL DERECHO A LA PROTECCIÓN DE DATOS

El cumplimiento de lo establecido en el RGPD y la LOPDGG no es opcional dado que es una normativa que forma parte de nuestro ordenamiento jurídico. Esto quiere decir, que ha de ser objeto de obligada observancia por parte de la UMH en general y del personal investigador en particular. De hecho, su incumplimiento puede traer como consecuencia que la UMH pueda recibir requerimientos de la Agencia Española de Protección de datos (en adelante, AEPD) u otra autoridad competente, que puedan derivar en expedientes sancionatorios, apercibimientos, publicidad adversa y responsabilidad civil o penal. Asimismo, la normativa de protección de datos abre la vía de amonestar al cargo responsable. (Art.77 LOPDgdd).

Así pues, la UMH, y por ende, su personal, han de tener una actitud comprometida y responsable con respecto a los tratamientos de datos de carácter personal que procesa, de entre los que se encuentran obviamente la

investigación. Por tanto, las personas investigadoras principales (en adelante IP), las investigadoras colaboradoras y terceras que están involucradas en los mismos han de observar y cumplir minuciosamente la normativa. -EL

4. ¿DEBE MI INVESTIGACIÓN CUMPLIR CON LA PROTECCIÓN DE DATOS?

El RGPD y la LOPDGDD sólo se aplica al "**tratamiento**" de "**datos personales**" de personas físicas. Por tanto, en el caso que la investigación no involucre el procesamiento de datos de humanos vivos, en principio, se excluiría de la aplicación de dicha normativa.

Si la investigación, en cambio, si supone dicho tratamiento, las personas investigadoras han de tener en cuenta las siguientes cuestiones:

I) ¿Estás "tratando" datos personales?

"Tratar" significa casi cualquier acción que un equipo de investigación pueda hacer con los datos personales, incluyendo: recolectarlos; guardarlos o almacenarlos; recuperarlos, consultarlos o usarlos; organizarlos o adaptarlos; publicarlos, divulgarlos o compartirlos; e incluso destruirlos.

Para mayor concreción, el RGPD define "tratamiento" como "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, efectuadas o no mediante procedimientos automatizados, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".

II) ¿Se incluyen datos personales en tu investigación?

Se define como "dato personal" cualquier información referida a una persona física y que le pueda identificar de manera directa o indirecta:

- Directa: nombre y apellidos, una imagen, etc.
- Indirecta: un identificador, un código seudonimizado, etc.

Esta definición se desarrolla con más profundidad en el Dictamen 4/2007 sobre el concepto de datos personales del Grupo del Artículo 29 (en adelante, WP29).

Así pues, podemos entender por "datos personales" un nombre, un número de identificación, datos de localización o un identificador en línea, como la dirección IP, o cookies. También hablamos de datos personales cuando nos referimos a características de un individuo, y la combinación de factores como los físicos, fisiológicos, genéticos, biométricos, culturales o sociales.

Con frecuencia, se cree erróneamente que en el marco de determinadas investigaciones no se "tratan" datos personales porque no se solicitan datos

"directamente identificables" como el nombre, los apellidos o una imagen de la persona. Sin embargo, en tanto en el proyecto haya una alta probabilidad de identificar a una persona determinada, (sin implicar un esfuerzo excesivo) entra en el ámbito del concepto de "dato personal" y se aplicaría la normativa de protección de datos.

En entornos en los que se recopilan grandes cantidades de datos, en los que se usan técnicas de OPEN DATA o tecnologías BIG DATA, en principio los datos podrían parecer a simple vista como no personales, sin embargo, hay una alta capacidad de agregarlos y re-identificarlos.

Un ejemplo sería la "combinación de identificadores". En este caso, a primera vista, la amplitud de los identificadores disponibles no permitiría, en principio, identificar a una persona determinada, pero, si dicha información se combina, habría una alta probabilidad de distinguir a una persona de entre una generalidad sin mucho esfuerzo.

Ejemplos:

> Ejemplo 1: Características singulares: "El rector de la UMH" o en una clase donde se recogen datos de los alumnos y se solicita como dato la edad. Si sólo hay una persona con 65 años, se le podría identificar de entre la generalidad.
>
> Ejemplo 2: Combinación de detalles combinados que identifican a una persona: en una encuesta "supuestamente" anónima, se pregunta por la categoría de edad +puesto de trabajo+ lugar de trabajo. (la probabilidad de identificar a una persona determinada es muy alta).

Por otro lado, hemos de tener en consideración **el formato o el medio que contiene la información pertinente**. Así pues, dentro del concepto de "datos personales" se incluye la información disponible en cualquier forma, ya sea alfabética, numérica, gráfica, fotográfica, acústica, etc. Incluyendo la información física (en papel), y/o, digital.

Los datos personales pueden proceder de cualquier tipo de actividad investigadora:

Estilo de vida
Salud
Historial genético
Educación
Registros de comportamiento
Muestras, tejidos, ADN
Localización y seguimiento (geolocalización, etc)
Características físicas
Características económicas
Etc.

- **Datos anónimos.**

Se ha concluido anteriormente que, la capacidad de poder identificar a una persona es decisiva a la hora de establecer la existencia de un tratamiento. Así pues, en cuanto no sea posible dicha identificación no se le aplicará la

normativa en materia de protección de datos.

Ejemplo: Las encuestas completamente anónimas (sin la recabación de ningún tipo de dato que pueda identificar a una persona directa o indirectamente) se consideran fuera del ámbito de la aplicación de la normativa de protección de datos.

- **Anonimización. Técnicas de anonimización.**

Como medida de salvaguardar la identidad de los sujetos de investigación se puede recurrir a las diversas herramientas de anonimización.

El artículo 3 de la Ley 14/2007 de Investigación Biomédica establece los siguientes conceptos:

- «Anonimización»: proceso por el cual deja de ser posible establecer por medios razonables el nexo entre un dato y el sujeto al que se refiere. Es aplicable también a la muestra biológica.

- «Dato anónimo»: dato registrado sin un nexo con una persona identificada o identificable.

- «Dato anonimizado o irreversiblemente disociado»: dato que no puede asociarse a una persona identificada o identificable por haberse destruido el nexo con toda información que identifique al sujeto, o porque dicha asociación exige un esfuerzo no razonable, entendiendo por tal el empleo de una cantidad de tiempo, gastos y trabajo desproporcionados.

La Agencia Española de Protección de Datos (en adelante, AEPD) entiende la "anonimización" como "la ruptura de la cadena de identificación de las personas" cuya finalidad es "eliminar o reducir los riesgos de reidentificación de los datos anonimizados". Es decir, la imposibilidad de que se asocien los datos anonimizados con una persona específica.

Así pues, en el caso que, en el marco de un proyecto de investigación, se considere el uso de técnicas de anonimización, se ha de proceder a la realización de un estudio sobre los riesgos de reidentificación, o la probabilidad que los datos puedan relacionarse con una persona física determinada, dado que, la misma podría darse, entre otras, por las siguientes circunstancias:

- pérdida de información,
- falta de protocolo adecuado en la anonimización
- falta de diligencia del personal involucrado.

Para ello, se ha de contar con varios equipos de trabajo independientes entre sí y en donde se procederá al desarrollo de las siguientes actividades, entre otras:

- Evaluación de riesgos que se pueden derivar de la anonimización.
- Determinación de las técnicas adecuadas.
- Cumplimiento y seguimiento de las medidas de seguridad necesarias para mantener la anonimización.
- Etc.

En este sentido, la AEPD ha publicado una guía[1] específica para proceder a la anonimización, una nota técnica sobre "k- anonimidad"[2] con pautas para las organizaciones que utilicen procesos de Big Data e inteligencia artificial para el tratamiento de datos y en donde ha indicado una serie de herramientas software[3], que permiten la anonimización de conjuntos de datos de forma eficaz.

No obstante lo anterior, y en el marco actual, las técnicas de anonimización están siendo cuestionadas[4] puesto que diversas investigaciones llegan a la conclusión sobre la inexistencia del riesgo cero, dado que existen técnicas (como la computación cuántica) que permiten revertir el proceso y averiguar la identidad de las personas que están detrás de estos datos y a las que se quiere proteger su privacidad.

- **Datos seudonimizados**

La seudonimización se define como la práctica de ocultar la identidad de las personas físicas a las que se refiere la investigación. Esto normalmente implica la eliminación de los datos que le identifican y el uso de un seudónimo (a menudo un número asignado aleatoriamente), de modo que se puedan recoger continuamente datos sobre la misma persona sin registrar su identidad. La finalidad perseguida es minimizar en la medida de lo posible que el interesado pueda ser identificado.

Elementos principales:

- La probabilidad de que los interesados sigan siendo identificados indirectamente es muy alta.
- Es una medida de seguridad muy útil, pero no es un método de anonimización.
- El tratamiento de los datos de forma seudonimizada no exime del cumplimiento de la normativa en materia de protección de datos.

Según el RGPD, es "aquella información que, sin incluir los datos denominativos de un sujeto, permiten identificarlo mediante información adicional, siempre que ésta figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.". **Así pues, los datos seudonimizados se consideran datos personales y su tratamiento implicaría el cumplimiento de la normativa.**

La seudonimización se puede realizar, entre otros, por algunos de estos procedimientos:

.

- A través de la codificación de la información. Esta codificación puede ser retornada con su clave de desencriptación.

[1] Ver Orientaciones y garantías en los procedimientos de anonimización de datos
[2] Ver https://www.aepd.es/sites/default/files/2019-09/nota-tecnica-kanonimidad.pdf
[3] ARX Data Anonymization Tool, Herramienta de anonimización UTD, Amnesia y Amnesia online
[4] https://www.nature.com/articles/s41467-019-10933-3

- Cuando la información se almacene bajo un número aleatorio que carezca de relación con la información original.
- La sustitución de cifras y códigos por palabras
- Intercambio de un número aleatorio por un conjunto de datos.

A este respecto la Agencia de Ciberseguridad de la UE (ENISA), ha publicado una guía con los principales escenarios y procedimientos en materia de seudonimización[5].

Existe la creencia errónea de utilizar, el número de DNI, como código. Este método en modo alguno se consideraría una técnica de seudonimización.

Por otro lado, cuando los datos seudonimizados se reciben de o se suministran a terceros sin los medios para identificar a los individuos, la eficacia de la seudonimización dependerá de una serie de factores (por ejemplo, la seguridad contra el rastreo inverso y el tamaño de la población en la que se oculta la persona).

La diferencia esencial entre anonimización y seudonimización es que, en la primera, los datos identificativos se disocian totalmente de los datos personales y de forma **IRREVERSIBLE.** En la seudonimización se desvinculan los datos identificativos, pero los datos seudonimizados mantienen datos adicionales que pueden reidentificar a los interesados siendo, por tanto, un proceso **REVERSIBLE**.

El artículo 89.2 del RGPD, viene a establecer que, en materia de tratamiento con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos deberá disponerse de medidas técnicas y organizativas para garantizar el principio de minimización de datos personales, de entre las que incluye la seudonimización **en la medida que ésa sea posible para alcanzar sus fines.**

- **Datos agregados o estadísticos**

Los datos agregados son parte del proceso de combinar la información sobre muchos interesados en clases, grupos o categorías amplias, de modo que no es posible distinguir la información relacionada con los mismos. De ello se deduce que estos datos no deben ser datos personales, pero su eficacia dependerá de factores tales como el tamaño de la población en la que se oculta la persona, o si la muestra original es suficientemente grande. Por tanto, el equipo de investigación deberá ir con cautela a la hora de calificarlos como "datos agregados", dado, que, en algunos casos, si se puede considerar datos personales de carácter identificable.

- **Datos biométricos, ADN y muestras de tejidos humanos**

El RGPD entiende por datos biométricos aquellos que se refieren a las características físicas, fisiológicas o conductuales de una persona que

[5] https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices/at_download/fullReport

posibilitan o aseguran su identificación única.

Los datos biométricos se caracterizan por tener tres elementos:

Son universales: existe en todas las personas sin distinción.
Únicos: distinguen a cada individuo.
Permanentes: se mantienen continuamente.

Se puede distinguir entre tres categorías principales de datos biométricos:

- Los datos que se refieren aspectos físicos y fisiológicos: huellas digitales, análisis de la imagen del dedo, iris, retina, reconocimiento facial, resultados de muestras de las manos, reconocimiento de la forma de la oreja, detección del olor corporal, reconocimiento de la voz, análisis de muestras del ADN y análisis de los poros de la piel, etc.

- Los datos basados en aspectos comportamentales, que miden el comportamiento de una persona e incluyen la comprobación de la firma manuscrita, el análisis de la pulsación sobre las teclas, el análisis de la forma de caminar, la forma de moverse, pautas que indiquen pensamiento subconsciente como mentir, etc.

- Los datos que se obtienen de técnicas basadas en elementos psicológicos, que incluyen la medición de la respuesta a situaciones concretas o pruebas específicas que se ajusten a un perfil psicológico.

Sin embargo, "las muestras de tejido humano", no se consideran en sí mismas como datos biométricos, sino como una fuente de la que se pueden extraer los mismos. es decir, la extracción de información de las muestras puede dar lugar a la recopilación de datos personales.

En opinión de la AEPD, en su Dictamen, 36/2020, "los datos biométricos solo constituirían una categoría especial de datos en el caso de que se sometan a un tratamiento técnico especifico dirigido a identificar de manera univoca a una persona física" y, en este sentido, igualmente se pronuncia el Considerando 51.

Así pues, y en referencia al Dictamen 3/2012 sobre la evolución de las tecnologías biométricas del WT29, distingue entre:

- Identificación biométrica: la identificación de un individuo por un sistema biométrico es normalmente el proceso de comparar sus datos biométricos (adquiridos en el momento de la identificación) con una serie de plantillas biométricas almacenadas en una base de datos (es decir, un proceso de búsqueda de correspondencias uno-a-varios)

- Verificación o autenticación biométrica: la verificación de un individuo por un sistema biométrico es normalmente el proceso de comparación entre sus datos biométricos (adquiridos en el momento de la verificación) con una única plantilla biométrica almacenada en un dispositivo (es decir, un proceso de búsqueda de correspondencias uno- a-uno)

La AEPD indica que, atendiendo a esta distinción, el concepto de dato biométrico incluiría ambos supuestos, tanto la identificación como la verificación o

autenticación. Sin embargo, y, con carácter general, únicamente tendrán la consideración de categoría especial los supuestos de identificación biomédica (uno-a varios).

- **Fotografías, videos y grabaciones de sonido**

Las personas investigadoras deben ser conscientes de que la existencia de fotografías, vídeos y grabaciones de sonido de las personas (independientemente de si esas personas revelan voluntariamente alguna información o no) en una investigación suponen información sobre esa persona que les identifica y por tanto, su tratamiento debe cumplir con las obligaciones en materia de protección de datos.

- **Datos personales de categoría especial**

El RGPD establece que son los datos personales que, "por su naturaleza, son particularmente sensibles y por ello, **merecen especial protección ya que, el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales.".**

Dichos datos son los siguientes:

- los que revelen el origen étnico o racial,
- las opiniones políticas,
- las convicciones religiosas o filosóficas,
- o la afiliación sindical,
- y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física,
- datos relativos a la salud
- o datos relativos a la vida sexual
- o la orientación sexual de una persona física.

En este sentido se debe prestar la debida atención a los datos tratados que puedan revelar indirectamente datos personales de categoría especial sobre una persona.

Ejemplo 1: Las fotografías y los nombres pueden dar una indicación de la raza o las creencias religiosas de una persona, no obstante lo anterior, esto no significa que se consideren siempre datos de categoría especial por dicha suposición. La cuestión se planteará si esa información se trata sobre la base de esos supuestos o no (por ejemplo, agrupar a las personas en función del color de la piel o del probable origen étnico de sus rasgos).

Ejemplo 2: Hay métodos que son muy propensos a la obtención de este tipo de datos, por ejemplo, en entrevistas en donde la persona puede revelar mucha información o por ejemplo en formularios con campos abiertos, y que permite a la persona escribir lo que estime oportuno.

- **Datos de menores**

En principio los datos relativos a menores, no se consideran datos de categorías especiales. No obstante, dada su vulnerabilidad por su juventud e inexperiencia, la normativa establece una especial protección, por su

desconocimiento de las repercusiones del tratamiento de sus datos.
En función de las características de la investigación, se deberá tener especial atención a la intervención de los representantes legales.

Así pues, a rasgos generales, en caso de investigaciones invasivas de datos, se deberá obtener el consentimiento de los representantes legales junto con el consentimiento del menor si es mayor de 12 años.

En el caso de investigaciones no invasivas, los mayores de 14 años podrán dar su consentimiento para participar en las mismas, relegando el consentimiento de los representantes legales a los menores de 14 (junto con el consentimiento del menor que es mayor de 12 años).

- **Datos relativos a condenas e infracciones penales**

El RGPD establece que el tratamiento de este tipo de datos sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados.

En consecuencia, dichos datos únicamente pueden ser tratados por la Administración incluso, aunque los mismos pudieran haber sido obtenidos de fuentes accesibles al público.

La LOPDGDD, aparte, añade los siguientes extremos:

- ·El registro completo de datos personales referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas, podrá realizarse conforme con lo establecido en la regulación del Sistema de registros administrativos de apoyo a la Administración de Justicia, y,

- Fuera de los supuestos señalados, solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones."

III) ¿Quién es responsable del cumplimiento del RGPD? ¿La persona IP? Otras figuras: Encargado del tratamiento, Corresponsable, Destinatario de datos.

Responsable de tratamiento (RT)

En materia de protección de datos, se define como la persona u organización que, (sola o conjuntamente con otras) determina los fines y el modo en que se tratan (o se van a tratar) los datos personales.

Esencialmente es quien contesta a la pregunta: ¿controlas y defines el uso de la información de carácter personal?

Encargado de tratamiento (ET)

Es la persona u organización que realiza el tratamiento de datos personales en nombre del responsable del tratamiento. En este caso, los datos tratados pertenecen al RT y su acceso a ellos está exclusivamente delimitado por el servicio, trabajo o tratamiento a realizar y demandado por el RT.

Contestaría a la siguiente cuestión: ¿Estás actuando de acuerdo con las instrucciones de otra persona u organización?

Si lo situamos en el marco de la Universidad, y en concreto en el marco de los proyectos de investigación, lo más probable es que la UMH sea la RT y que se puedan contar con terceras organizaciones (o personas) para encomendar determinados trabajos para llevar a cabo la investigación, como, por ejemplo, la contratación de un "data center" que aloje los datos de la investigación, que serían los encargados del tratamiento.

Asimismo, también pueden darse casos en los que la UMH actúe como ET, cuando una persona investigadora pueda colaborar en investigaciones cuya iniciativa y control sea de terceros y a la que se le encomienden determinadas funciones o trabajos, pero sin ser parte de la investigación. (Por ejemplo, aquellos que se formalizan en el marco del artículo 83 de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.

Corresponsable de tratamiento (CoRT)

Este supuesto se da en la práctica, cuando existen dos (o más) organizaciones que deciden y colaboran determinando conjuntamente los fines y el modo de tratamiento (la investigación), en este caso, dichas organizaciones asumirán el rol de corresponsables de Tratamiento.

En este caso, se dan varios elementos, la existencia de un nivel general de complementariedad y la unidad de propósito. Para ello, en principio no es necesario que todos los corresponsables ejecuten todas las operaciones en que se constituye la investigación, es decir, que puede que interactúen en diversas operaciones del tratamiento, y en otras las realicen por sus propios medios y fines.

En caso que se de esta situación, se ha de establecer una asignación clara de responsabilidades de cada uno de los corresponsables en relación con la investigación y frente a los interesados.

Según la Guía de la CRUE sobre la protección de datos personales en el ámbito universitario en tiempos del COVID-19:

> "En principio, cabrían dos situaciones teóricas:
> • por un lado, si hay una entidad líder, entonces ella será la responsable del tratamiento de datos personales y el resto tendrán que firmar un contrato de encargado de tratamiento (en la medida en que tratan datos por cuenta de aquel responsable);
>
> •por otro lado, si no existe tal líder único ya que las entidades determinan

conjuntamente los objetivos y los medios del tratamiento de datos, en ese supuesto todas ellas serán corresponsables de tratamiento y tendrán que firmar un acuerdo de esa naturaleza"

Destinatario de datos (DT)

En determinadas ocasiones, es preciso proceder a la comunicación de los datos a otra organización (persona física, jurídica o entidad). Por ejemplo, entre otros, cuando una ley establezca la comunicación. En este caso se debe informar expresamente al interesado de dicha comunicación.

En cualquier caso, si en el curso de un proyecto de investigación se requiriera de la colaboración de un tercero, la persona IP debe dirigirse a la OIR para obtener orientación, dado que se deben formalizar las relaciones con otras organizaciones o personas a través de acuerdos o contratos concretos.

Así pues, ya sea la Universidad RT, o se constituya como ET o CoRT, **la persona IP es responsable interno** con respecto al rol que ejerce la Universidad, dado que existe una relación vinculante laboral/estatutaria entre esta y la UMH. Por ello, deberá actuar de acuerdo con las instrucciones en materia de protección de datos contempladas en la normativa de protección de datos aplicable, este documento, y cualesquiera otras normativas o documentos que fuesen aplicables en el seno de la UMH.

5. DEBERES Y OBLIGACIONES

I) Principios de la Protección de datos

Este apartado es uno de los más importantes de la normativa en materia de protección de datos (art. 5 RGPD), dado que viene a establecer qué criterios se deben seguir en el tratamiento de datos personales:

i.- Han de ser tratados de forma **lícita, leal y transparente**.

ii.- Se recogerán únicamente para fines **determinados, explícitos y legítimos,** y no se tratarán de manera incompatible con dichos fines (No obstante, el tratamiento ulterior con fines de investigación científica o histórica no se considerará incompatible con los fines iniciales).

iii.- Serán **adecuados, pertinentes y limitados** a lo necesario en relación con los fines para los que son tratados.

iv.- Serán **exactos** y, cuando sea necesario, **mantenerse actualizados.**

v.- **No se conservarán** como datos identificados durante más tiempo del necesario para los fines en cuestión.

vi.- Tratados con garantía de **seguridad**, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida,

destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas

i.-Tratamiento licito, leal y transparente

Tratamiento Lícito: Este principio supone que las personas investigadoras, ante un proyecto de investigación, deben considerar de forma previa a su inicio, cómo éste podría afectar a los derechos y libertades de las personas objeto de investigación. Habida cuenta de lo anterior, deberán ponderar entre el uso de los datos personales y el interés del proyecto en sí, sobre todo, si dicho proyecto puede causar algún perjuicio en el derecho de protección de datos de los interesados. En este caso, la persona investigadora debería de estar en condiciones de demostrar que dicho perjuicio está justificado.

La licitud está naturalmente ligada también a la transparencia y a la capacidad de la persona a negarse al tratamiento de sus datos.

Tratamiento Leal: El tratamiento de datos personales debe tener una base legítima (un motivo legalmente aceptable para el tratamiento de los datos), que debe ser documentado por la RT, y realizado fácticamente por la persona IP.

Base legítima para datos personales

Según el artículo 8 de la Carta de Derechos Fundamentales de la UE, «estos datos se tratarán de modo leal, para fines concretos y **sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley**.

En el RGPD establece seis posibles fundamentos jurídicos sobre los que basar jurídicamente el tratamiento:

a) Consentimiento – esta base jurídica implica obtener de forma fehaciente el consentimiento del interesado bien directa o indirectamente a través de un tercero que contribuya en el proyecto de investigación.

En este sentido, el Comité Europeo de Protección de datos (en adelante, EDPB) ha indicado que, en determinados supuestos en el marco de una investigación (sobre todo en materia de ensayos clínicos) puede darse un desequilibrio entre las partes, y no cumplirse los requisitos que el RGPD establece para que éste se considere válido ("manifestación de voluntad libre, específica, informada e inequívoca por la cual el interesado acepta, mediante una clara acción afirmativa, el tratamiento de sus datos personales).

Por ello, el equipo de investigación, deberá valorar la existencia o no de dicho desequilibrio.

b) el tratamiento es necesario para la **ejecución de un contrato** en el que el interesado es parte.

c) **Interés vital del interesado** – El Tratamiento será lícito cuando sea necesario para proteger intereses vitales del interesado o de otra persona física.

e) Interés público – Una investigación realizada en el seno de la universidad puede considerarse como un tratamiento necesario para el cumplimiento de una misión realizada en interés público en conexión al artículo 1. de Ley Orgánica 6/2001, de 21 de diciembre, de Universidades [6].

f) El tratamiento es necesario para la **satisfacción de intereses legítimos**. (no aplica a administraciones)

Las bases jurídicas aplicables preferentemente en el marco de una investigación en el seno de la Universidad como organismo público son:

a) consentimiento,

e) interés público.

En el caso de datos de categorías especiales (datos sensibles)

En el ámbito de una universidad, es muy habitual que se produzcan investigaciones en los que se traten, no sólo datos de salud, sino de otra tipología muy sensible como colectivos vulnerables, de víctimas de violencia de género, datos genéticos, biométricos, etc.

Tal como se ha comentado con anterioridad, los datos de categorías especiales se regulan en el artículo 9 del RGDP, en donde se establecen que son los siguientes:

- Datos que revelen el origen étnico o racial,
- Las opiniones políticas,
- Las convicciones religiosas o filosóficas,
- La afiliación sindical,
- Datos genéticos,
- Datos biométricos
- Datos relativos a la salud
- Datos relativos a la vida sexual
- La orientación sexual

El RGPD establece **una prohibición en general** para el tratamiento de estos datos tan sensibles, a salvo de las excepciones que, se enmarcan en el artículo 9 del RGPD y que, son aplicables a las investigaciones.

Por tanto, para utilizar los datos sensibles en una investigación, además de identificar una base legal para el tratamiento de

[6] Art. 1.1 de la L.O.U . "La Universidad realiza el servicio público de la educación superior mediante la investigación, la docencia y el estudio".

investigación (como se ha comentado en el punto anterior, consentimiento o interés público) se ha de "levantar" la prohibición del tratamiento de los datos sensibles a través de alguna de las siguientes excepciones:

Consentimiento explícito – Además de las características atribuidas por el RGPD al consentimiento[7], en el caso del tratamiento de datos sensibles, se exige que el mismo sea EXPLICITO, es decir, que el consentimiento e información previa deberán ser prestados de manera particular para cada investigación, estudio o proyecto concreto o al menos para determinados ámbitos o áreas[8] (si en ese momento no es posible delimitarse por el tipo de investigación), en especial, en investigaciones de salud[9].

Así pues, para utilizar datos personales de categoría especial requiere que el equipo de investigación obtenga ese consentimiento explícitamente. Esto significa que el mismo debe darse en forma de una declaración expresa a tal efecto ("Doy mi consentimiento para que mis datos sean tratados para...) o a través de mecanismos "doble opt in" en tratamientos digitales. (artículo 9.2.a RGPD).

Al igual que se ha comentado anteriormente, se ha de comprobar que la persona participante en la investigación **no concurre en una situación de desequilibrio** con respecto a la misma (que no se encuentre en buenas condiciones de salud, o pertenezca a grupos económicos o socialmente débiles, o encontrarse en situaciones de jerarquía institucional, etc.) en cuyo caso, convendría acudir a otras bases jurídicas alternativas.

Aparte de lo anterior, los participantes de la investigación, en este caso, disponen del derecho a retirar su consentimiento en cualquier momento, esto implicaría que el IP principal debería suprimir inmediatamente los datos personales del proyecto, estudio o investigación en caso de solicitud de revocación por su parte.

Interés público esencial: tratamiento sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser

[7] Art.4.11 RGPD 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".

[8] Considerando 33 RGPD: "Con frecuencia no es posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida. Por consiguiente, debe permitirse a los interesados dar su consentimiento para determinados ámbitos de investigación científica que respeten las normas éticas reconocidas para la investigación científica. Los interesados deben tener la oportunidad de dar su consentimiento solamente para determinadas áreas de investigación o partes de proyectos de investigación, en la medida en que lo permita la finalidad perseguida".

[9] Disposición adicional décimo séptima, apartado 2d: El tratamiento de datos en la investigación en salud se regirá por los siguientes criterios: El interesado o, en su caso, su representante legal podrá otorgar el consentimiento para el uso de sus datos con fines de investigación en salud, y, en particular, la biométrica. Tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora.

proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado; (9.2.g RGPD). (Según la LOPDgdd ha de estar amparado en una norma con rango de Ley).

Fines médicos - en este contexto, se entienden los fines de la medicina preventiva o laboral, la evaluación de la capacidad de trabajo de un empleado, el diagnóstico médico, la prestación de asistencia sanitaria y tratamiento, y la gestión de los servicios sanitarios. La condición se aplica cuando el tratamiento se realiza **en virtud de un contrato con un profesional de la salud**. (Los investigadores deben tener en cuenta que la definición de profesional de la salud es muy restrictiva); Esta excepción se aplicará siempre y cuando se apliquen al tratamiento las garantías adecuadas. (artículo 9.2.h RGPD). (Según la LOPDgdd ha de estar amparado en una norma con rango de Ley).

Interés Público: el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional (art. 9.2.i) (Según la LOPDgdd ha de estar amparado en una norma con rango de Ley).

Fines de archivo en el interés público, **o fines de investigación científica e histórica** o fines estadísticos – esta excepción se aplicará siempre y cuando se apliquen al tratamiento las garantías adecuadas del artículo 89.1[10] RGPD sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado. (9.2.j)

En el marco de proyectos, estudios e investigaciones realizadas en el seno de la Universidad, suele aplicarse

[10] Art.89.1 RGPD: El tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo.

preferentemente el 9.2.a o el 9.2.j. (consentimiento explícito y/o fines de investigación científica).

Datos sensibles, en especial los relativos a salud

Cuando en el marco de una investigación se traten datos de salud o biomédicos, para poder aplicar la excepción 9.2.j. debemos acudir a la disposición adicional decimoséptima de la LOPDGDD, dado que en ella se prevén las normas estatales que habilitan el tratamiento:

- La Ley 14/1986, de 25 de abril, General de Sanidad.
- La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.
- La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
- La Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.
- La Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias.
- La Ley 14/2007, de 3 de julio, de Investigación biomédica.
- La Ley 33/2011, de 4 de octubre, General de Salud Pública.
- La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.
- El texto refundido de la Ley de garantías y uso racional de los 105 medicamentos y productos sanitarios, aprobado por Real Decreto Legislativo 1/2015, de 24 de julio.
- El texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado por Real Decreto Legislativo 1/2013 de 29 de noviembre.

Investigaciones con datos seudonimizados

Es posible la realización de proyectos, estudios e investigaciones a través del acceso a datos seudoanimizados.

Dicha habilitación, se basa en la DA17 de la LOPDgdd, fundamentada en el artículo 9.2.j del RGPD en conexión con el artículo 89.1, al respecto de cuando el tratamiento es necesario para el cumplimiento de una misión realizada en interés público (art. 6.1. e RGPD).

Para poder utilizar los datos seudonimizados en una determinada investigación, debemos dar cumplimiento a determinadas garantías:

1. Una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la identificación.

2. Que los datos seudonimizados únicamente sean accesibles al equipo de investigación cuando:
    a. Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.
    b. Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados.

Asimismo, en el apartado f, establece que conforme a lo previsto por el artículo 89 se procederá a:

1.-Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 35 del RGPD.

2.-Someter a investigación científica a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica.

3.- Adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados.

4.º Designar un representante legal establecido en la Unión Europea, conforme al artículo 74 del Reglamento (UE) 536/2014, si el promotor de un ensayo clínico no está establecido en la Unión Europea. Dicho representante legal podrá coincidir con el previsto en el artículo 27.1 del Reglamento (UE) 2016/679.

Por otro lado, el apartado g) establece la obligación de ser sometida la investigación con tratamiento de datos seudonimizados al informe previo del comité de ética de la investigación.

Esquema principio licitud:

En resumen, la licitud del tratamiento en una investigación, dependería de los siguientes supuestos:

- Si se tratan datos generales (sin categorías especiales de datos)

- Si se tratan datos generales + Datos de categorías especiales de datos (No datos salud y/ biomédicos)

- Si se tratan datos generales + Datos de categorías especiales de salud y biomédicos

- Si se realizan investigaciones con datos seudonimizados.

1.- Datos GENERALES

DATOS	BASE LEGITIMA	REQUISITO	EXCEPCIÓN	LEY	GARANTIA
DATOS PERSONALES	CONSENTIMIENTO ART. 6.1.a RGPD	EVIDENCIA de ser una manifestación libre, específica, informada e inequívoca mediante declaración o una clara acción afirmativa.	N/A	N/A	**EVIDENCIA** del consentimiento otorgado por el partipante Si es posible por tipo de investigación: Seudonimización datos identificativos (cumplimiento principcio minimización de datos)
	INTERÉS PÚBLICO. ART. 6.1.e RGPD	LEY APLICABLE: L.O.U. Artl1 Finalidad de investigación	N/A	N/A	Si es posible por tipo de investigación: Seudonimización datos identificativos (cumplimiento principcio minimización de datos)

2.- Datos Categoría Especial NO SALUD NI BIOMÉDICOS

DATOS	BASE LEGITIMA	REQUISITO	EXCEPCIÓN	LEY	GARANTIA
CATEGORIA ESPECIAL DE DATOS: NO SALUD Y NO BIOMÉDICOS: - ORIGEN ETNICO O RACIAL -OPINIONES POLITICAS -CONVICCIONES RELIGIOSAS O FILOSOFICAS -AFILIACIÓN SINDICAL -DATOS BIOMETRICOS NO DE SALUD -VIDA SEXUAL -ORIENTACION SEXUAL -DATOS SENSIBLES:VIOLENCIA DE GÉNERO, MINUSVALIAS, ETC.	CONSENTIMIENTO ART. 6.1.a RGPD	EVIDENCIA de ser una manifestación libre, específica, informada e inequívoca mediante declaración o una clara acción afirmativa	CONSENTIMIENTO EXPLÍCITO Art. 9.2.a	L.O.U. Art.1 Finalidad de investigación	. EVIDENCIA del consentimiento explíctio otorgado por el partipante. Si es posible por tipo de investigación: Seudonimización datos identificativos (cumplimiento principcio minimización de datos)

3.- Datos Categoría Especial SALUD NI BIOMÉDICOS

DATOS	BASE LEGITIMA	REQUISITO	EXCEPCIÓN	LEY	GARANTIA
CATEGORIA ESPECIAL DE DATOS: SALUD Y BIOMÉDICOS	CONSENTIMIENTO ART. 6.1.a RGPD	EVIDENCIA de ser una manifestación libre, específica, informada e inequívoca mediante declaración o una clara acción afirmativa	CONSENTIMIENTO EXPLÍCITO Art. 9.2.a	N/A	Si es posible por tipo de investigación: Seudonimización datos identificativos (cumplimiento principcio minimización de datos)
	INTERÉS PÚBLICO	LEY APLICABLE: L.O.U. Finalidad de investigación	FINES DE INVESTIGACIÓN Art. 9.2.j	DA17 LOPDGDD: siempre que le sea aplicable alguna de las siguientes normas: - LEY 41/2002 - LEY 16/2003 - LEY 44/2003 - LEY 14/2007 - LEY 33/2011 - LEY 20/2015 - RD 1/2015 - RD LEGISLATIVO 1/2013	**Disposición Adicional 17** apartado f en relación al artículo 89.1 - Realización Evaluación Impacto - Someter la investigación a las normas de calidad y, en su caso, a las directrices internacionales de buena práctica clínica. - Adoptar, en su caso, medidas a garantizar que los investigadores no accedan a datos de investigación. - En Transferencias Internacionales, desisgnar a un representante legal establecido en la UE. Seudonimización datos.

4.-Datos Categoría Especial DATOS SEUDONIMIZADOS

DATOS	BASE LEGITIMA	REQUISITO	EXCEPCIÓN	LEY	GARANTIA
CATEGORIA ESPECIAL DE DATOS: SALUD Y BIOMÉDICOS: **DATOS SEUDONIMIZADOS**	INTERÉS PÚBLICO: ART. 6.1.e	LEY APLICABLE: L.O.U. Finalidad de investigación	Art. 9.2.j	DA17 LOPDGDD: siempre que le sea aplicable alguna de las siguientes normas: - LEY 41/2002 - LEY 16/2003 - LEY 44/2003 - LEY 14/2007 - LEY 33/2011 - LEY 20/2015 - RD 1/2015 - RD LEGISLATIVO 1/2013	**Disposición Adicional 17** **apartado d S**e considera lícito el uso de datos personales seudonimizados con fines de investigación en salud y, en particular, biomédica. -separación técnica y funcional - datos seudonimizados sólo accesible a investigaroes cuando exista compromiso de confidencialidad y de no proceder a la reidentificación y - se adopten medidas de seguridad para evitar reidentificación **apartado f** en relación al artículo 89.1 - Realización Evaluación Impacto - Someter la investigación a las normas de calidad y, en su caso, a las directrices internacionales de buena práctica clínica. - Adoptar, en su caso, medidas a garantizar que los investigadores no accedan a datos de investigación. - En Transferencias Internacionales, desisgnar a un representante legal establecido en la UE. **apartado g:** Informe previo Comité ética.

Los investigadores deben tener en cuenta que cada una de las condiciones descritas anteriormente es adicional a cualquier condición que pueda ser establecida por el organismo aplicable para la revisión y aprobación ética.

Tratamiento Transparente:

Datos obtenidos directamente de los participantes:

Cuando se recogen datos personales debe utilizarse un lenguaje claro, abierto y transparente con las personas, exponiendo lo que se pretende hacer con sus datos.

Específicamente, el RGPD requiere que se les proporcione la siguiente información:

- el nombre del responsable o responsables del tratamiento (es decir, la Universidad y los eventuales cotitulares o responsables conjuntos de los datos (Corresponsables),si procede, y la delegación de protección de datos;
- los fines para los que se pretende tratar los datos,
- la base legal para el tratamiento;
- los destinatarios o categorías de destinatarios con los que se van a compartir los datos, o se pueden compartir.

- en su caso, el hecho de que los datos se transferirán fuera del Espacio Económico Europeo (el "**EEE**") y las salvaguardias que se aplicarán a dicha transferencia;

- el período durante el cual se almacenarán los datos o, si esto no es posible, los criterios que se utilizarán para determinar el período de retención;

- si el tratamiento se basa en el consentimiento, el derecho del interesado a retirar su consentimiento en cualquier momento; y

- los derechos de los interesados en virtud del RGPD (derecho de acceso a sus datos, rectificación, supresión de sus datos, derecho a oponerse al tratamiento, derecho a presentar una reclamación ante la AEPD).

Para la investigación, esta información se proporciona a menudo en forma de un aviso de privacidad o información del participante.

Los investigadores deben asegurarse de que *todos* los participantes (o en su caso, padres/madres o tutores/ras de los niños y niñas participantes) reciban la información correcta prescrita

El hecho de que dicha información se proporcione por escrito, o se ponga a disposición de los participantes de alguna otra manera dependerá de la naturaleza del proyecto y de la utilidad de ese formato para los participantes.

En cualquier caso, la información debe proporcionarse de una manera fácil, que evite una jerga innecesaria, y siempre debe documentarse que se ha proporcionado, especialmente si la información prescrita se lee en voz alta a los interesados.

Datos no obtenidos directamente de los participantes:

En el marco de las investigaciones es habitual la captación de datos personales de los participantes a través de otros proyectos de investigación o de organizaciones externas.

En estos casos, la obligación de transparencia persiste y se debe proporcionar igualmente a cada uno de los participantes la información descrita, como se detalla anteriormente, añadiendo la siguiente información adicional:

- las categorías de datos personales que se van a tratar; y
- la fuente de los datos personales, y, si proceden de fuentes públicas.

Sin embargo, no es necesario proporcionar la información si los participantes ya tienen la información; o si hacerlo

resultara imposible, o implicara un esfuerzo desproporcionado; o impediría o perjudicaría seriamente el logro de los objetivos de la investigación. Obviamente, estos casos concretos deben ser justificados documentados adecuadamente y ser aprobados por el Comité ético.

En el caso de que traten datos de categorías especiales de datos, en particular biomédicos o de salud, la LOPDGDD establece en la DA17 que, en caso de reutilización de los datos en una investigación "los responsables deberán publicar la información en un lugar fácilmente accesible de la página web corporativa del centro donde se realice la investigación o estudio clínico, y, en su caso. en la del promotor, y notificar la existencia de esta información por medios electrónicos a los afectados. Cuando estos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato". Para este tratamiento, se requiere el informe previo favorable del comité de ética de investigación.

ii.-Obtenidos para fines específicos, explícitos y legítimos

Este principio de protección de datos está directamente relacionado con la transparencia y al requisito de proporcionar a las personas la información prescrita.

Cuando el investigador obtiene datos personales para un fin determinado, en principio no debería permitirse su uso para otros fines (es decir, "tratamiento posterior") que sean incompatibles con ese fin original. No obstante, el RGPD establece que el tratamiento ulterior de los datos **con fines de investigación** se considerará compatible con el propósito original para el que se recogieron los datos.

Tal como se ha comentado anteriormente, la LOPDGDD establece en la DA17 que "se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial".

En este caso, los responsables deberán publicar la información en un lugar accesible de la página web corporativa del centro donde realice la investigación o estudio clínico, y, en su caso en la del promotor y notificar la existencia de esta información por medios electrónicos (u otros formatos en su ausencia) a los afectados.

iii.-Adecuado, pertinente y limitado a lo que es necesario para los fines en cuestión (minimización de datos)

Este principio tiene por objeto evitar la recopilación de datos personales innecesarios.

Si tenemos a la vista la sensibilidad que se asocia a los datos personales, se deduce que ninguna organización debe tener en su poder datos personales que no necesite. Así como, establece la obligación de garantizar que dichos datos sean adecuados para los fines de la investigación.

Este principio de minimización de datos es considerado por el RGPD como uno de los más importantes y se aplica no sólo en la captación de estos, sino a todo su ciclo de vida (forma en la que podrá acceder, procesar, compartir, razón para su uso, destrucción, conservación, etc.). Por ejemplo, puede que no sea necesario que todos los miembros del equipo de investigación o los colaboradores tengan acceso a todo el conjunto de datos y que sea posible proporcionar información a esas personas de forma anónima o seudonimizada.

El acceso a los datos personales debe estar siempre restringido a aquellas personas con una necesidad legítima para conocerlos. Los investigadores deberían preguntarse si es necesario utilizar datos personales en su investigación o si podrían cumplir sus objetivos con datos anónimos, agregados o seudonimizados.

iv. Exacto y, cuando sea necesario, actualizado

Este principio tiene conexión directa con el anterior dado que los datos que no se mantienen actualizados pueden dejar de ser adecuados y pertinentes para los fines para los que se van a tratar.

Se deben adoptar todas las medidas razonables para garantizar que los datos inexactos, habida cuenta de los fines para los que se tratan, se supriman o rectifiquen sin demora.

No obstante lo anterior, nos encontramos en muchos casos con proyectos de investigación con archivos estáticos, cuya actualización frustraría el propósito para el cual se inició el mismo. En estos casos, se puede interpretar que los investigadores no necesitarían mantener actualizados los datos personales. Esta situación, deberá documentarse y justificarse.

v. No se conservarán como datos identificables durante más tiempo del necesario para los fines en cuestión

Al igual que el anterior principio, el de conservación de los datos también guarda conexión directa con el principio de pertinencia y adecuación en función de los fines[11]. En el caso de proceder a la conservación de los datos personales de forma identificable durante más tiempo del necesario los mismos podrían no ser pertinentes y adecuados.

En cuanto a cómo debería de conservarse los datos personales en la investigación durante este tiempo, en algún soporte, a ser posible,

electrónico, que permita mantener bloqueados los datos (íntegro y sin alteraciones).

vi. Garantía de seguridad.

El RGPD instaura un sistema de seguridad basado en la responsabilidad proactiva determinando que serán los responsables y/o encargados de tratamiento quienes establecerán las medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales.

Esto trae como consecuencia que el IP y los investigadores/ colaboradores adopten medidas técnicas y organizativas adecuadas para proteger los datos personales contra el tratamiento no autorizado o ilegal de los mismos y contra la pérdida, destrucción o daño accidental de los mismos.

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

- la seudonimización 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;
- un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento"

"En cualquier caso, resulta fundamental que, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el equipo de investigación aplique las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo detectado, medidas que, en el ámbito de las universidades públicas, deberán ser conformes con las que contiene el ENS (disp. adic. 1ª LOPDGDD).

Asimismo, en materia de seguridad, "todo investigador debe saber que más importante que las medidas generales de seguridad, son las medidas de seguridad individuales y específicas que se deben adoptar por parte de todos los investigadores para proteger los datos

personales”[12]

II) Otros principios y obligaciones.

i. Principio de responsabilidad activa

Este principio (accountability), viene recogido en el artículo 5.2 del RGPD. constituye un concepto esencial del mismo.

Se define como la necesidad (obligatoriedad) de que el RT aplique medidas técnicas y organizativas apropiadas a fin de garantizar y **poder demostrar** que el tratamiento de datos personales es conforme con el Reglamento.

Esencialmente implica que no basta con proceder a dar cumplimiento de la normativa de protección de datos, sino que, además, se ha de poder demostrar frente a terceros que se está cumpliendo con la misma.

A fin de poder proceder al cumplimiento del principio de responsabilidad proactiva, el RGPD desarrolla una serie de medidas de obligado cumplimiento para el RT mediante las cuales se puede demostrar este cumplimiento de normativa, y que, en el marco específico de la investigación en el seno de la UMH son las que se reflejan en el presente documento. (medidas de protección de datos desde el diseño y por defecto, registro de actividades de tratamiento, evaluación de impacto en la protección de datos, notificación de quiebras por seguridad, etc.).

ii. Privacidad por defecto y desde el diseño.

El RGPD incluye estos principios en el artículo 25 del RGPD.

En lo referente a los proyectos de investigación, se han de aplicar medidas técnicas y organizativas en las primeras fases de las operaciones del tratamiento que los constituyen de tal manera que se garantice la intimidad y lo principios de protección de datos desde el primer momento (**protección de datos desde el diseño**).

Principios privacidad desde el diseño[13]

Principios Fundacionales de la Privacidad desde el Diseño
1. Proactivo, no reactivo; Preventivo, no correctivo
2. La privacidad como configuración predeterminada
3. Privacidad incorporada en la fase de diseño
4. Funcionalidad total: pensamiento “todos ganan”
5. Aseguramiento de la privacidad en todo el ciclo de vida.
6. Visibilidad y transparencia
7. Enfoque centrado en el sujeto de los datos

[12] Guía sobre la protección de datos personales en el ámbito universitario en tiempos del COVID-19.
[13] Guia de privacidad desde el diseño de la AEPD. Tabla 1. Página 5

El uso de técnicas de seudonimización y de cifrado son ejemplos de medidas a aplicar bajo este principio.

Por otro, lado y desde el punto de vista de la **privacidad por defecto**, se ha de garantizar que los datos personales se tratan con la máxima protección de la intimidad, es decir, bajo el prisma del principio de minimización de datos, y teniendo en cuenta los criterios de adecuación, pertinencia y necesidad con relación a los fines en el diseño de las distintas fases del tratamiento. (medidas a tomar en cuenta sobre la cantidad de datos personales recogidos, la extensión del tratamiento, el periodo de conservación o la accesibilidad de los datos).

La AEPD ha elaborado una "Guía de Privacidad desde el Diseño"14, y otra "Guia de privacidad por Defecto"15 en donde se detallan y se explican concienzudamente estos principios.

iii. Brechas de seguridad:

El RGPD define, las "violaciones de seguridad de los datos personales" como "todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos"

Cuando hablamos del término "violación" se entiende algo más que un simple incidente en la seguridad, es decir, que debe de comprometer al RT en el cumplimiento de los principios del RGPD y debe, además entrañar riesgos para los derechos y libertades de las personas participantes en la investigación.

El RGPD impone la obligación al RT de notificar a la AEPD cualquier brecha de la seguridad de los datos personales en un plazo máximo de 72 horas. esto implica que, tan pronto como el investigador tenga conocimiento de la misma debe efectuar la correspondiente notificación al RT o a la DPD de la UMH a fin de poder cumplir con esta obligación.

Así pues, en caso que exista en el seno de un proyecto de investigación, una brecha de seguridad que implique un riesgo para los derechos y libertades de las personas físicas, se deberá notificar inmediatamente a la Universidad como Responsable del Tratamiento a fin de poder notificar, en su caso, en plazo y en forma la misma a la AEPD y/ o a los interesados (si procede).

La AEPD, ha publicado una herramienta específica[16] que puede ser de ayuda a conocer cuando un determinado suceso puede entrañar un alto riesgo en cuanto a los derechos y libertades de las personas físicas y por tanto, puede constituir una brecha de seguridad.

iv. Evaluación de impacto:

El Reglamento General de Protección de Datos (RGPD) introduce el concepto de Evaluación de Impacto relativa a la Protección de Datos (EIPD) en su artículo 35[17]

---

[14] https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf
[15] https://www.aepd.es/sites/default/files/2020-10/guia-proteccion-datos-por-defecto.pdf

[16] https://www.aepd.es/es/guias-y-herramientas/herramientas/comunica-brecha-rgpd
17 Art. 35.1 RGPD: . Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y

Una EIPD viene a ser un proceso para analizar[18]. y describir de forma previa y anticipada un tratamiento de datos personales que puedan calificarse de alto riesgo para los derechos y libertades de las personas físicas, evaluándose, en particular, el origen, la naturaleza, la particularidad y la gravedad del riesgo.

¿Cuándo mi investigación puede involucrar tratamientos de datos personales que puedan calificarse de alto riesgo para los derechos y libertades de las personas físicas?

Se considera que el tratamiento de datos supone un alto riesgo para los derechos y las libertades de los participantes en la investigación cuando se llevan a cabo perfilados, seguimiento sistemático de individuos o procesamiento a gran escala de categorías especiales de datos o cuando se utilizan métodos intrusivos de tratamiento de datos (como seguimiento, vigilancia, grabación de audio y vídeo, seguimiento de geolocalización, etc.).

En cualquier caso, la AEPD ha publicado un listado[19] con los tratamientos que requieren la realización de una EIPD. Según su criterio, y teniendo a la vista los supuestos definidos, en el caso que se den dos o más, se ha de proceder a realizar una EIPD. Dicho lo anterior, y por las características que suelen darse en los proyectos de investigación existe una alta probabilidad que sea necesaria la realización de la misma, en particular para datos de salud.

Para ayudar a la realización de la EIPD, la AEPD ha desarrollado una herramienta para la realización de evaluaciones de impacto en la protección de datos.:

https://gestiona.aepd.es – Evaluación de impacto.

Con el objeto de dar mayor información al respecto de las EIPD, se ha de tener en cuenta otros documentos de interés.

Modelo de informe de Evaluación de Impacto en la protección de datos para Administraciones Públicas

Guía para la Evaluación de Impacto de la AEPD

Documentos del Comité Europeo de Protección de Datos sobre EIPD

Mas información

Al respecto de este caso, se puede solicitar el asesoramiento de la Delegación de

---

libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares

18 Art. 35.3 RGPD La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:
a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;
b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o
c) observación sistemática a gran escala de una zona de acceso público

19 https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf

Protección de datos al objeto de dar cumplimiento a esta obligación.

v. Registro de Actividades del tratamiento (RAT)

El art. 30 del RGPD establece la obligación del Responsable del tratamiento de llevar un registro , de las actividades de tratamiento efectuadas bajo su responsabilidad, así como, del Encargado del tratamiento, cuando actúe bajo este rol.

La UMH, ha incluido como actividad del tratamiento los proyectos de investigación en su Registro a nivel general, no obstante lo anterior, y en aras al cumplimiento del principio de responsabilidad pro activa, cada IP procederá a inventariar el proyecto de investigación para catalogarlo como accesorio al general. Dentro del protocolo para la autorización del proyecto de investigación por parte del Comité ético, se facilitará un modelo de RAT a la personal IP para su cumplimentación.

vi. Transferencias Internacionales de Datos

En el caso que la investigación requiera la realización de transferencias internacionales de datos a países que estén fuera del Espacio Económico Europeo deberán cumplirse y aportar garantías de cumplimiento del régimen jurídico establecido en la normativa de protección de datos. (artículos 44 a 50).

Así pues, se entiende que existen garantías para la realización de transferencias internacionales, cuando:

- Se realicen a un país, sector específico u organización internacional que haya sido declarado de nivel de protección adecuado por la comisión europea.

- Se realicen entre empresas del mismo grupo y se hayan aprobado normas corporativas vinculantes de acuerdo con el art. 47 RGPD. En este caso, se adjuntará dichas normas o la dirección electrónica desde la que sean accesibles.

- Se haya firmado cláusulas contractuales tipo de protección de datos adoptadas por la Comisión Europea. Se adjuntará copia de las cláusulas firmadas.

- Las entidades que realicen la transferencia de datos y que estén adheridas a un código de conducta o mecanismo de certificación, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de los interesados. Se aportará copia del código de conducta o certificación o dirección electrónica desde la que sea accesible.

Al respecto de este caso, se puede solicitar el asesoramiento de la Delegación de Protección de datos al objeto de dar cumplimiento a esta obligación.

vii. Las decisiones individuales automatizadas y la elaboración de perfiles (Profiling)

La elaboración de un perfil y las decisiones individuales automatizadas de una persona física suponen tratamientos de datos personales relevantes que pueden darse de forma habitual en el marco de un proyecto de investigación.

El RGPD introduce disposiciones para garantizar que su uso no produzcan un impacto no justificado en los derechos de las personas, como por ejemplo[20]:

- "requisitos específicos de transparencia y equidad;
- mayores obligaciones de responsabilidad proactiva;
- bases jurídicas específicas para el tratamiento;
- derechos individuales para oponerse a la elaboración de perfiles y específicamente a la elaboración de perfiles para mercadotecnia; y
- si se cumplen ciertas condiciones, la necesidad de llevar a cabo una evaluación de impacto relativa a la protección de datos".

El artículo 22 de la RGPD establece el derecho de toda persona a no ser objeto de una decisión basada en el tratamiento automatizado, incluida la elaboración de perfiles, cuando dicha decisión traiga consigo efectos jurídicos o bien le afecte significativamente de modo similar: Ejemplo: denegación de subvenciones públicas, cancelación de un contrato, imposición de una multa, etc.).

Así pues, se ha de entender ambos conceptos de forma separada y conjunta.

La elaboración de perfiles[21] es un procedimiento que implica un tratamiento automatizado de datos personales para evaluar aspectos personales, en particular para analizar o hacer predicciones de personas. (Es decir, implica un tipo de evaluación o juicio sobre una persona).

Este término, va más allá que una simple clasificación de personas (como su edad, sexo y altura).

Por ejemplo, en una clasificación de personas participantes por su edad o género con motivos estadísticos con la finalidad de obtener una visión global de estos (SIN hacer predicciones ni sacar conclusiones sobre una persona no es una "elaboración de perfil" dado que no es su objetivo evaluar las características individuales.

Así pues, éste concepto legal implica la recogida de información sobre una persona (o grupo de personas) y la evaluación de sus características o patrones de comportamiento con el fin de asignarla a una determinada categoría o grupo, en particular para analizar o hacer predicciones sobre, por ejemplo:

- su capacidad para realizar una tarea;

[20] Ejemplos dados en las Directrices sobre decisiones automatizas y elaboraciones de perfiles del grupo de trabajo del art. 29

[21] "toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar, predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación, o movimientos de dicha persona física. (art. 4.4 RGPD).

- sus intereses; o
- su comportamiento probable

Las decisiones automatizadas son aquellas que se toman por medios tecnológicos sin participación humana.

El RGPD aborda estos conceptos bajo tres posibles formas:

1.- Decisiones basadas únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que producen efectos jurídicos en el interesado o le afecten significativamente de modo similar

La clave está en el concepto es la "toma de decisión automatizada", basada exclusivamente en medios tecnológicos sin intervención humana. Este caso es el definido en el artículo 22.1 del RGPD, lo que implicaría una prohibición en general de este tipo de actuaciones. No obstante, existen excepciones [22], que en caso de aplicarse, deberán existir unas medidas para garantizar los derechos y libertades del interesado.

2.- Elaboración de perfiles general
3.- Decisiones basadas en la elaboración de perfiles

En estos dos últimos casos, se ha de aplicar, entre otras obligaciones, los principios del artículo 5 (finalidad, conservación, minimización, etc.), las bases legitimadoras del artículo 6 (preferentemente consentimiento, interés público), transparencia (informar al interesado) y en su caso, la realización de una Evaluación de impacto del artículo 35. El WP29 publicó unas directrices[23] a fin de garantizar el cumplimiento del Reglamento cuando se dé la concurrencia de estos tratamientos.

viii. Derechos de los interesados

Los participantes en los proyectos de investigación pueden solicitar el ejercicio de los derechos de acceso, rectificación, supresión, limitación del tratamiento, oposición y a no ser objeto de decisiones individualizadas automatizadas).

En caso de que las personas investigadoras tengan conocimiento de alguno de los

---

[22] Articulo 22. Decisiones individuales automatizadas, incluida la elaboración de perfiles
1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.
2. El apartado 1 no se aplicará si la decisión:
a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;
b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o c) se basa en el consentimiento explícito del interesado.
3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.
4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

[23] Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679

citados derechos, deberán notificarlo a la Delegación de Protección de datos de la UMH en el menor plazo de tiempo posible a fin de que, junto con ellos, se proceda a resolver dicha solicitud.

ix. La persona delegada de protección de datos de la UMH.

La persona Delegada de Protección de datos (la DPD) es un órgano consultivo e independiente, que, entre otras funciones, ha de proceder a supervisar el cumplimiento de la normativa en materia de protección de datos personales, reportar informes, y, en su caso, gestionar las consultas de las personas que se pongan en contacto con el mismo en relación con el tratamiento de sus datos personales en la Universidad.

Asimismo, es la persona encargada de informar a la alta dirección sus obligaciones legales en materia de protección de datos, cooperar con la autoridad de control y actuar como punto de contacto entre ésta y la entidad responsable del tratamiento de los datos (artículo 39 del RGPD).