GUIA PARA EL TRATAMIENTO DE DATOS PERSONALES EN EL AMBITO DE LA INVESTIGACION

La versión definitiva ha sido aprobada por el Comité de Ética de la Investigación de la Universidad Autónoma de Madrid (CEI-UAM), con fecha 3 de febrero de 2023

INDICE

1. INTRODUCCIÓN

Esta Guía tiene por objeto informar sobre los aspectos generales más relevantes que en materia de protección de datos inciden en el campo de la investigación con seres humanos, así como, sensibilizar y concienciar a los investigadores en un uso adecuado de los datos personales con la finalidad de contribuir a que los proyectos de investigación cumplan con la normativa y facilitar la preparación de la solicitud de su proyecto de investigación ante el Comité de Ética de la Investigación de la UAM (CEI-UAM) para su aprobación.

La normativa de referencia aplicable es:

- Reglamento (UE) 2016/679 General de Protección de Datos (RGPD)
- Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD)

En el caso de que los investigadores precisen de mayor asesoramiento podrán ponerse en contacto con el Delegado/a de Protección de Datos (DPD) de la UAM, 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.

Delegado/a de Protección de Datos (DPD)
Email: delegada.protecciondedatos@uam.es
Tlf. 91 497 6056

2. ¿QUÉ ES LA PROTECCIÓN DE DATOS PERSONALES?

El derecho a la privacidad e intimidad es un derecho fundamental reconocido en el art 8 de la Carta de los Derechos Fundamentales de la Unión Europea y en el art. 18 de la Constitución española por el que se reconoce el derecho de toda persona a la protección de los datos de carácter personal que la conciernan, a poder restringir el conocimiento de su vida personal, privada e íntima a otras personas así como a protegerse contra aquellas injerencias o intromisiones ilegítimas que la hagan pública.

La protección de datos personales es el conjunto de medidas legales, organizativas y técnicas encaminadas a garantizar los derechos y libertades de las personas en cuanto a su poder de disposición y control de sus datos personales, a decidir sobre el uso de estos, a conocer para qué se van a utilizar y quién accede a ellos, y a oponerse ante cualquier posesión, revelación o divulgación de su información personal.

Por tanto, la protección de datos plantea un equilibrio entre:

a) los derechos de protección de datos de las personas físicas, y,
b) la necesidad de que las organizaciones o entidades realicen un tratamiento de dichos datos de forma lícita, adecuada y razonable.

El objeto de la legislación en materia de protección de datos es salvaguardar los derechos y libertades inherentes a las personas por lo que el acceso, procesamiento y divulgación de sus datos por cualquier persona, entidad u organización requiere el compromiso previo de asumir ciertas obligaciones (legales, organizativas y técnicas) así como el respetar los principios generales (licitud, finalidad, minimización, plazo de conservación, seguridad de los datos, etc.) con el fin de no conculcar los derechos fundamentales de las personas afectadas.

3. LA IMPORTANCIA DEL DERECHO A LA PROTECCIÓN DE DATOS

La observancia y cumplimiento de lo establecido en la normativa de protección de datos no es opcional ni baladí porque forma parte de nuestro ordenamiento jurídico y es de obligado cumplimiento.

De hecho, su incumplimiento puede tener consecuencia para la Universidad, como responsable del tratamiento de los datos personales, porque la presentación de una reclamación ante la Agencia Española de Protección de Datos (AEPD) puede derivar en apercibimientos, apertura de expedientes sancionadores o en la obligación de resarcir los daños y perjuicios ocasionados.

Así pues, todo el personal de la UAM en el desempeño de sus funciones y tareas ha 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, porque no lo olvidemos la universidad cumple o incumple la normativa por medio de sus empleados.

El investigador principal (IP), como responsable interno con respecto al rol que ejerce la universidad, ha de observar y cumplir rigurosamente la normativa aplicable así como actuar de acuerdo con las instrucciones emanadas por la propia UAM en el caso de que realice algún tratamiento con datos personales.

En particular, el art. 15.1.l) de la Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación modificada por la Ley 17/2022 de 5 de septiembre, prevé entre los deberes del personal investigador que preste servicios en universidades públicas o en organismos de investigación precisamente el "*adoptar las medidas necesarias para el cumplimiento de la normativa aplicable en materia de protección de datos y de confidencialidad*".

4. ¿QUIÉN ES RESPONSABLE DE SU CUMPLIMIENTO?

Todo el personal que procese y trate datos de carácter personal está obligado al cumplimiento de la normativa aplicable. No obstante, su grado de responsabilidad es diferente según el rol o condición que tengan.

Según el RGPD, será «**responsable del tratamiento**» la persona, entidad u organización que, sola o conjuntamente con otras, determine los fines y el modo en que se tratan (o se van a tratar) los datos personales.

Es decir, básicamente el responsable es quien contesta a las siguientes preguntas: ¿qué datos se van a recabar?, ¿para qué se van a utilizar?, ¿cómo se van a tratar?, ¿dónde se van a almacenar?, ¿durante cuánto tiempo se van a conservar?, etc.

Con carácter general y en el marco de los proyectos de investigación, lo más probable es que sea el investigador principal (IP) por lo que será la UAM la que asuma la responsabilidad en tanto en cuanto el investigador actúa por cuenta y bajo la dependencia de la universidad como consecuencia del desempeño de las funciones investigadoras que les son propias en virtud de su relación laboral/estatutaria como personal docente e investigador.

El resto de los investigadores, colaboradores o miembros del equipo de investigación tendrán la consideración de «**usuario autorizado**» en la medida que realizan una actividad de tratamiento por cuenta del investigador principal (IP) y solo accederá a la información necesaria para el desarrollo de las tareas que tiene asignadas y no a otros datos o recursos aunque estén disponibles o accesibles.

No obstante, es frecuente que en la práctica, algunos proyectos de investigación se realicen en colaboración o coordinación con otras universidades, entidades, centros o instituciones. En tales casos, habrá que determinar quién lidera el equipo investigador, quién asigna los objetivos y los medios del tratamiento de datos, quién asume su coste, qué operaciones o tareas realiza cada miembro del equipo, etc.

En principio, en materia de protección de datos, cabrían las siguientes situaciones teóricas respecto a los proyectos coordinados:

1. Si no existe una entidad líder ya que las distintas universidades, centros o instituciones determinan conjuntamente los objetivos y los medios de la investigación, todas ellas serán «**corresponsables de tratamiento**» y, según prevé el art. 26 del RGPD, tendrán que firmar un acuerdo o convenio en el que se asignen y establezcan las respectivas obligaciones de cada parte en relación con el tratamiento de datos y frente a los interesados, en particular, en cuanto al suministro de información y al ejercicio de los derechos.
   Para ello, no es necesario que todos los corresponsables ejecuten todas y cada una de las tareas o trabajos en que se desarrolla la investigación, es decir, que pueden que interactúen o participen en algunas operaciones conjuntas del tratamiento y otras las realicen por sus propios medios y fines (subproyectos).

2. Si, por el contrario, hay una universidad, centro o institución que lidera o coordina la investigación y asigna los objetivos, trabajos y los medios entre los distintos miembros del equipo investigador entonces será ella la responsable del tratamiento de datos personales y el resto de las universidades u organizaciones participantes tendrán la consideración de «**encargado de tratamiento**» en la medida en que tratan los datos por cuenta de aquel responsable para realizar exclusivamente los servicios, trabajos o tratamientos encomendados (subproyectos).
   En tales casos y de acuerdo con el art. 28 del RGPD, se deberá firmar un acuerdo o contrato entre las partes en el que se establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento que se va a llevar a cabo con los datos.

Por último, puede haber ocasiones en los que una entidad pública o privada contrata al investigador para realizar determinados trabajos o estudios de carácter científico o técnico a cambio de una remuneración por la prestación de sus servicios (p. ej. aquellos que se formalizan en el marco del art. 83 de la Ley Orgánica de Universidades), en tales supuestos, la UAM actúa como encargado de tratamiento, en tanto en cuanto los trabajos del profesorado se desarrollan por cuenta y siguiendo las instrucciones de la empresa o entidad contratante.

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

Según establece el art. 40 de la Ley Orgánica de Universidades, la investigación es un derecho y un deber del personal docente e investigador de las Universidades pero siempre dentro de los límites establecidos por el ordenamiento jurídico, entre los cuales, el art. 15.1.l) de la Ley de la Ciencia, la Tecnología y la Innovación prevé expresamente que se deberán "*adoptar las medidas necesarias para el cumplimiento de la normativa aplicable en materia de protección de datos y de confidencialidad*".

Nos enfrentamos ante un posible conflicto de derechos. Por esta razón, el derecho a la creación científica y la libertad de investigar debe ponderarse con el derecho fundamental a la protección de datos de las personas.

La normativa de protección de datos (RGPD y LOPDGDD) sólo se aplica al tratamiento de datos personales de seres humanos vivos identificados o identificables (las personas jurídicas están excluidas).

Se considerará persona identificable toda persona física cuya identidad pueda determinarse, bien directa o bien indirectamente, empleando todos los medios que razonablemente puedan utilizarse para identificarla de manera inequívoca a través de uno o varios de sus rasgos fisiológicos, ideológicos, profesionales, económicos, culturales, sociales o genéticos.

Con frecuencia, se cree erróneamente que en el marco de determinadas investigaciones o estudios no se recaban ni tratan datos personales porque no se solicitan datos directamente identificativos a los participantes como pueden ser el nombre, el DNI o una imagen de la persona. Sin embargo, en tanto en cuanto en el proyecto de investigación haya una alta probabilidad de identificar a una persona determinada (sin implicar un esfuerzo excesivo o desproporcionado) se aplica la normativa de protección de datos.

Únicamente en el caso de que la investigación se centre en personas fallecidas o en personas no identificables (anónimas), en principio, se excluiría la aplicación de dicha normativa.

En definitiva, si la investigación implica el procesamiento o tratamiento de datos de personas físicas vivas se ha de tener en cuenta las siguientes cuestiones:

I. ¿Se incluyen datos personales en la investigación?

Se define como "dato personal" cualquier información referida a una persona física y que le pueda identificar de manera inequívoca, bien directa o indirectamente, a través de un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios

elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

A título de ejemplo categorías de datos personales pueden ser:

- Datos identificativos: nombre y apellidos, DNI/Pasaporte, dirección postal, correo electrónico, teléfono, imagen, firma manuscrita, fecha y lugar de nacimiento, matrícula del coche, número de Seguridad Social, IMEI del móvil, contraseñas;
- Datos de características personales: edad, sexo, altura, peso, talla, voz, etnia o raza, nacionalidad, idioma, fecha y lugar de nacimiento;
- Datos familiares y de filiación: estado civil, número de hijos, datos de progenitores
- Datos académicos y profesionales: estudios, calificaciones, becas, certificaciones, vida laboral, experiencia profesional, carrera administrativa, colegios profesionales;
- Datos económico-financieros: ingresos, datos bancarios, tarjeta de crédito, nóminas, ayudas y subsidios, impuestos, préstamos, bienes patrimoniales e inmuebles;
- Datos de geolocalización y navegación**:** GPS, ubicación, Direcciones IP, cookies;
- Datos relativos a la salud**:** datos relacionados con la salud física o mental, enfermedades, vacunas, pruebas diagnósticas, tratamientos, grado de discapacidad;
- Datos biométricos**:** huella dactilar, retina, imagen facial, reconocimiento de voz;
- Datos genéticos**:** ADN, muestras biológicas u otros datos relativos a las características genéticas heredadas o adquiridas;

También hablamos de datos personales cuando la combinación de varios factores tales como sus hábitos, aficiones, opiniones o conductas permiten distinguir a una persona específica de entre un colectivo sin mucho esfuerzo.

La existencia de encuestas, cuestionarios, vídeos y grabaciones de sonido de las personas (independientemente de si se revela voluntariamente alguna información personal o no) en una investigación suponen información sobre esa persona que les identifica y, por ende, su tratamiento debe cumplir con las obligaciones en materia de protección de datos.

Con frecuencia, algunos investigadores creen erróneamente que en el marco de sus investigaciones no tratan datos personales porque no se solicitan datos directamente identificables como pueden ser el nombre, los apellidos, el DNI, el email o teléfono de una persona. Sin embargo, en tanto en cuanto con la información recogida en el estudio haya una alta probabilidad de identificar a una persona determinada, 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 y tratan un gran volumen de datos, en los que se usan técnicas de Big Data o algoritmos de datos, a simple vista los datos podrían parecer como no personales porque no permitiría identificar a una persona en concreto, pero, si dicha información se combina, habría una alta probabilidad de reidentificarla sin mucho esfuerzo.

Por ejemplo, en una encuesta supuestamente anónima donde se recogen datos de los alumnos y se pregunta por el sexo + edad + titulación + lugar de residencia, la probabilidad de identificar a una persona determinada entre la población o muestra puede ser alta.

La capacidad de poder identificar a una persona es decisiva a la hora de establecer la existencia o no de un tratamiento de datos personales. Así pues, en cuanto no sea posible dicha identificación mediante el uso de técnicas de anonimización no se le aplicará la normativa de protección de datos.

- La anonimización.

La anonimización es el proceso por el cual deja de ser posible establecer por medios razonables el nexo entre un dato registrado y el sujeto al que se refiere, rompiéndose la cadena de identificación de los datos con una persona específica.

Por tanto, se considera "dato anonimizado o irreversiblemente disociado" el dato que no puede asociarse a una persona identificada o identificable por haberse destruido el vínculo con toda la 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.

Así pues, en el caso de 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 previo sobre los riesgos o la probabilidad de reidentificación, es decir, que los datos puedan relacionarse o vincularse con una persona física específica, y la determinación de las técnicas más adecuadas. Sin embargo, hay que ser conscientes de que el riesgo cero no existe dado que existen técnicas (como la computación cuántica u otras) que permiten revertir el proceso y averiguar la identidad de las personas que están detrás de estos datos.

En el tratamiento de las imágenes y videos, se considera que son anónimas cuando se utilizan las técnicas adecuadas e irreversibles para el pixelado de las imágenes o la distorsión de la voz de modo que las personas que aparecen no sean reconocibles. También se recomienda transcribir a texto la grabación de la entrevista si es compatible con el objeto de la investigación.

En este sentido, la Agencia Española de Protección de Datos (AEPD) ha publicado unas guías específicas con pautas para las organizaciones para proceder a la anonimización de conjuntos de datos de forma eficaz tales como

- Guía básica de anonimización
- Guía orientaciones procedimientos anonimización
- La K-anonimidad como medida de la privacidad

- La seudonimización.

La seudonimización es la técnica que permite ocultar la identidad de las personas físicas a las que se refiere la investigación mediante el reemplazo de sus datos identificativos dentro de un registro o dataset por el uso de códigos, identificadores o un seudónimo, de modo que se puedan recoger continuamente datos y procesarlos sobre un sujeto específico sin registrar su identidad.

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.

Según el RGPD, «datos seudonimizados» 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.

La finalidad perseguida es minimizar en la medida de lo posible que el interesado pueda ser identificado pero no es un método de anonimización ni irreversible, por ello, la probabilidad de que los interesados puedan ser reidentificados indirectamente es muy alta aunque dependerá de múltiples factores (p.ej. la seguridad contra el rastreo inverso o el tamaño de la población y muestra) y su tratamiento no exime del cumplimiento de la normativa en materia de protección de datos.

El art. 89.2 del RGPD, viene a establecer que, en materia de tratamiento con 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.

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

- A través de la codificación de la información mediante una clave de encriptación
- 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 las principales técnicas y procedimientos en materia de seudonimización.

- Guía Técnicas de seudonimización y mejores prácticas

De acuerdo con la Disposición adicional 17ª de la LOPDGDD, 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. De modo que el dataset con los códigos reidentificativos de los participantes se almacene separadamente y en lugar seguro.

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.

- Datos agregados o estadísticos

Los datos agregados son parte del proceso de combinar la información sobre un conjunto de interesados agrupados en clases, conjuntos, grupos o categorías amplias, de modo que no es posible distinguir la información relacionada con cada individuo en concreto pero permite el análisis y procesamiento de datos. Se suele utilizar frecuentemente para el análisis matemático o estadístico de grupos de personas (suma, promedio, recuento, etc.)

De ello se deduce que estos datos agrupados o agregados no deben ser considerados datos personales en tanto en cuanto no conlleva datos personales de carácter identificativos pero su eficacia dependerá de factores tales como el tamaño del grupo o población en el que se oculta la persona, o si la muestra original es suficientemente grande.

II. ¿Qué son datos personales de categoría especial?

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

Dichos datos son los siguientes:

- los que revelen el origen étnico o racial,
- las opiniones políticas o ideológicas,
- las creencias religiosas o filosóficas,
- la afiliación sindical,
- la orientación o vida sexual
- los datos relativos a la salud física o mental
- los datos genéticos
- los datos biométricos

Con carácter general, se prohíbe recabar y tratar estos datos por su especial sensibilidad y transcendencia para la intimidad de los interesados, salvo las excepciones previstas con carácter exhaustivo en el art. 9 del RGPD.

En el ámbito de la investigación se suele aplicar el consentimiento explícito e informado del interesado (art. 9.2.a) o bien el tratamiento es necesario con fines de investigación científica (art. 9.2 j), de conformidad con el art. 89.1, respetando en lo esencial los intereses y derechos fundamentales de las personas.

Así pues, para utilizar datos personales de categoría especial se requiere que el equipo de investigación obtenga el consentimiento de manera particular y específico para el objeto de cada investigación, estudio o proyecto concreto o, al menos, para determinados ámbitos o áreas (si en ese momento no es posible delimitarse por el tipo de investigación), en especial, en investigaciones de salud.

Asimismo, se debe tratar con la debida diligencia y precaución la información que pueda revelar indirectamente datos personales de categoría especial sobre una persona, especialmente en las

entrevistas o en formularios con campos abiertos donde el participe puede revelar mucha información sin querer siendo intrascendente para la investigación.

Para garantizar la privacidad e intimidad de los participantes en el estudio, se deberán adoptar las medidas técnicas y organizativas necesarias para proteger la confidencialidad y seguridad de los datos evitando cualquier pérdida, difusión o acceso no autorizado, en particular, la seudonimización de los datos cuando sea compatible con el objeto de la investigación o estudio.

III. Datos de salud en estudios clínicos o biomédicos

El acceso y tratamiento de los datos de salud, incluida la historia clínica de un paciente o extracción de muestras biológicas, con fines de investigación científica o biomédica deberá hacerse con el previo consentimiento específico e inequívoco de todos los interesados (o de sus representantes legales) que participen en el proyecto de investigación o estudio clínico (incluidos familiares cuando se pudiera revelar información que les afecte) e informar de las consecuencias y los riesgos que pueda suponer para su salud, si los hubiera.

Dicho consentimiento expreso será también necesario para divulgar y publicar los resultados de la investigación, salvo que los datos a publicar estén disociados o anonimizados, de manera que queden separados los datos identificativos del paciente de los datos clínico-asistenciales.

Del mismo modo, en virtud de la Ley 14/2007 de investigación biomédica, se requerirá el consentimiento de los afectados para el depósito y conservación de las muestras biológicas en biobancos si las muestras se almacenen asociadas a los datos de los sujetos fuente con fines de investigación científica.

Únicamente se tratarán aquellos datos de la historia clínica o muestras biológicas que sean estrictamente necesarios, pertinentes y adecuados para la finalidad legítima que se persigue, no utilizándolos para otros fines incompatibles, y se deberán adoptar medidas técnicas y organizativas específicas para garantizar la confidencialidad e integridad de los datos, protegiéndolos de cualquier revelación o acceso de terceras personas no autorizadas así como para evitar la reidentificación de los datos personales seudonimizados.

IV. Datos de menores y personas con discapacidad

El tratamiento de datos relativos a menores de edad (entendiendo por tal los menores de 14 años según el art. 7 de LOPDGDD) o de personas con discapacidad, dada su especial vulnerabilidad y desconocimiento de los posibles riesgos o consecuencias, requieren de una protección específica al exigir la intervención y consentimiento expreso de los titulares de la patria potestad, tutores o representantes legales.

Así pues, con carácter general, los niños mayores de 14 años y personas con discapacidad no incapacitadas legalmente pueden otorgar libremente su consentimiento para el tratamiento de sus datos personales en investigaciones no invasivas que supongan una grave intromisión en su privacidad, por ejemplo, encuestas y estudios, sin necesidad de la autorización de sus progenitores, tutores o representantes, siempre que la información proporcionada resulte sencilla, de fácil comprensión y se la facilite en formatos adecuados de acuerdo a sus

circunstancias personales, salvo en aquellos supuestos en que la ley exija expresamente la asistencia del titular de la patria potestad o tutela.

En el ámbito de los ensayos clínicos o investigaciones con muestras biológicas con menores, el RD 1090/2015, de 4 de diciembre que regulan los ensayos clínicos con medicamentos, establece en el art. 5 que, siendo menor de doce años, solo podrá realizarse con el consentimiento informado previo de los padres y, si es mayor de 12 años, se requerirá también el consentimiento expreso del menor para participar en el ensayo clínico.

Puedes consultar la guía publicada Recomendaciones sobre el uso de grabación audiovisuales de menores en investigación

V. Datos relativos a condenas e infracciones penales

El RGPD establece que el tratamiento de datos personales relativos a delitos y condenas penales, así como a procedimientos y medidas cautelares y de seguridad conexas, solo podrá llevarse a cabo bajo la supervisión de las autoridades o cuando se encuentre amparado en una norma de rango legal.

En consecuencia, estos datos de naturaleza penal únicamente pueden ser tratados y registrados por la Administración de Justicia y los investigadores, de acuerdo con el art. 89 del RGPD, solo pueden tratar dichos datos si se ha realizado previamente la pseudonimización de manera que no se pueda identificar a la persona afectada, aunque los mismos pudieran haber sido obtenidos de fuentes accesibles al público.

VI. Datos personales para la elaboración de perfiles

La elaboración de perfiles tiene como objeto la recopilación de datos personales con el fin de evaluar, estudiar o analizar determinados aspectos relacionados con una persona física y así poder hacer predicciones automatizadas sobre su posible comportamiento, modo de vida, rendimiento profesional, estado de salud, solvencia económica, intereses y preferencias, localización y movimientos, etc. permitiendo la toma de ciertas decisiones respecto a ella basada en el resultado de operaciones algorítmicas o en inteligencia artificial.

La elaboración de perfiles es una práctica habitual en el sector financiero, de seguros, de recursos humanos, de la salud o el marketing y busca dotar de valor a los datos recopilados por las empresas. También en el ámbito de la investigación, es frecuente en los estudios de psicología y de educación.

En principio, está permitido el tratamiento de datos personales con la finalidad de perfilar, segmentar o evaluar determinados aspectos de las personas siempre que se cumplan los requisitos exigidos por la normativa, a saber: que se trate de un tratamiento leal y lícito, se informe adecuadamente a los interesados de su finalidad para poder obtener su consentimiento, se recaben los datos que sean mínimos y necesarios, se facilite el ejercicio de sus derechos, etc. No obstante, el responsable del tratamiento deberá adoptar las medidas apropiadas para salvaguardar el derecho del interesado a expresar su punto de vista y a impugnar la decisión adoptada.

Dado el mayor riesgo que supone el tratamiento automatizado de datos personales para la elaboración de perfiles, en tanto en cuanto pueden tener efectos jurídicos u otros impactos negativos sobre los interesados, el RGPD y la LOPDGDD obligan a realizar una evaluación de impacto (EIPD) antes de iniciar cualquier tipo de perfilado.

VII. Tratamiento de imágenes y videos

La captación y grabación de imágenes y videos en el ámbito de la investigación para su posterior reproducción o divulgación requiere el consentimiento/autorización previa y expresa de las personas afectadas si pueden identificarse porque, además de la normativa de protección de datos, debe tenerse en cuenta el derecho y protección a la propia imagen (LO 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen).

Las sesiones de grabación deberán realizarse en un entorno en el que el participante se sienta cómodo y seguro, respetando en todo momento la imagen respetuosa de su persona y su derecho al honor. En el caso de que muestre claros indicios de estrés, malestar o bien exprese su deseo de abandonar la sesión, se deberá inmediatamente finalizar la grabación o realizar los descansos necesarios.

Durante las grabaciones se respetará el principio de minimización de datos personales por el que tan solo se recabarán y tratarán aquellas imágenes, sonidos y datos que sean exclusivamente pertinentes, necesarios y proporcionales para el objetivo de la investigación.

La captación y grabación de imágenes o videos de una persona se considera un dato sensible y especialmente protegido al poder identificar unívocamente a una persona mediante el uso de técnicas biométricas lo que exige el cumplimiento de garantías adicionales.

Por ello, se deberán adoptar las medidas apropiadas para garantizar la confidencialidad y seguridad de las grabaciones para evitar en lo posible que se produzcan daños, pérdidas o usos inadecuados de las mismas. En la medida en que sea acorde con el objeto de la investigación, se utilizaran técnicas para el pixelado de las imágenes, la distorsión de la voz o la transcripción a texto, se deberán archivar seudonimizadas mediante códigos de modo que no permita identificar al participante o se almacenarán cifradas o protegidas con una clave alfanumérica para acceder.

6. 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.

Antes de iniciar la investigación o estudio, los investigadores que lleven a cabo actividades de investigación con seres humanos o que utilicen muestras biológicas de origen humano deberían preguntarse si es necesario utilizar datos de carácter personal en su proyecto de

investigación o si podrían cumplir sus objetivos empleando solo datos agregados, disociados o seudonimizados.

También desde el diseño y por defecto debemos tener en consideración el tratamiento de datos que vayamos a hacer al desarrollar una actividad de investigación, los riesgos de diversa probabilidad y gravedad que entraña dicho tratamiento para los derechos y libertades de los participantes y establecer las medidas apropiadas al respecto porque es difícil subsanar completamente a posteriori una investigación que se ha planteado sin respetar la normativa sobre protección de datos. Por tanto, es importante al diseñar el proyecto de investigación, tener en cuenta los aspectos de la privacidad y cumplimiento de la normativa aplicable desde sus inicios.

Toda investigación que trate datos de carácter personal deberá basarse en el «*principio de proporcionalidad, en su doble versión de idoneidad y de intervención mínima*». La idoneidad determina que sólo se podrán utilizar aquellos procedimientos o técnicas científicas que resulten adecuadas e idóneas para el propósito de la investigación. La intervención mínima exige la ponderación, en cada caso, entre la finalidad pretendida y la posible afectación a la intimidad de las personas eligiendo siempre las técnicas o métodos que sean menos intrusivos para la privacidad de los participantes.

I. Lealtad, Licitud y Transparencia

- Tratamiento Leal: Este principio supone que los investigadores, de forma previa al inicio de su proyecto de investigación, deben considerar 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 de grave o difícil reparación para los interesados en caso de vulneración de la confidencialidad y seguridad de los datos.

Asimismo, en función de la finalidad perseguida y del nivel de perjuicio que se pueda derivar para los participantes en el estudio, se deberá llevar a cabo un análisis previo de los riesgos o, en caso de ser necesaria, una evaluación de impacto de protección de datos relativa al tratamiento.

- Tratamiento Lícito: El tratamiento de datos personales debe tener una base legítima o habilitadora de las establecidas en el art. 6.1 del RGPD que fundamente la recogida y tratamiento de los datos.

En el ámbito de la investigación las bases jurídicas son:

a) **Consentimiento**: manifestación de voluntad libre, específica, informada e inequívoca por la cual el participe en la investigación acepta el tratamiento de sus datos personales.

   Las condiciones que se deben cumplir para que el consentimiento sea válido y no esté viciado son las siguientes:

   - Libre y voluntario: No se puede obligar ni condicionar al interesado a otorgar su consentimiento.
     Para que el consentimiento sea libre, debe poder ser retirado por el interesado en cualquier momento y etapa de la investigación sin sufrir perjuicio alguno o represalia

por ello. Esto obliga al investigador a planificar su proyecto de modo que pueda suprimir inmediatamente los datos personales de los sujetos participantes en la investigación en caso de solicitud de revocación.
Se considera que no se ha prestado voluntariamente el consentimiento cuando haya un desequilibrio claro entre las partes, en particular, cuando exista alguna relación, contrato o prestación de servicio entre ellas (p.ej. profesor con sus alumnos o médico con sus pacientes)

- Informado: Se debe informar de manera clara y sencilla al interesado del tratamiento que se va a realizar con sus datos, los beneficios que se esperan, los riesgos o molestias previstos, la metodología y la duración del proyecto.
  En particular, en el ámbito de la protección de los datos, el interesado debe conocer como mínimo la identidad y datos de contacto del investigador principal (IP), los fines y base jurídica para recabar y tratar sus datos personales, durante cuánto tiempo y dónde se van a almacenar, los destinatarios a los que se comuniquen datos así como del ejercicio de sus derechos.

- Determinado y específico: Cuando el tratamiento tenga varias finalidades, debe darse el consentimiento para cada una de ellas, no siendo válido un consentimiento general e indeterminado para todas.

- Inequívoco y explícito: se requiere una declaración por escrito o clara acción afirmativa para la prestación del mismo, no admitiéndose el silencio, las casillas premarcadas o la inacción.
  El modelo de declaración de consentimiento deber ser comprensible y emplear un lenguaje claro y sencillo evitando en lo posible tecnicismos.

- Demostrable: El investigador debe ser capaz de demostrar que el interesado ha dado su consentimiento a la operación de tratamiento en caso de reclamación por lo que deberá conservarlo o guardarlo mientras sea necesario.

b) **Interés público o en el ejercicio de poderes públicos** – 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 o en beneficio del interés general en conexión con el art. 1 de Ley Orgánica de Universidades que establece "*La Universidad realiza el servicio público de la educación superior mediante la investigación, la docencia y el estudio*"

   Tendrá la consideración que la investigación se realiza en interés público cuando se trate de un proyecto institucional a realizar en el marco de programas y convocatorias de proyectos de investigación competitivos a nivel nacional, europeo o internacional.

c) **Interés legítimo** – En último caso, el tratamiento puede ser necesario para la satisfacción de intereses legítimos perseguidos por el investigador, siempre que sobre dichos intereses no prevalezcan los derechos a la intimidad y a la protección de datos del interesado.

   Para ello, se deberá realizar un juicio de ponderación, teniendo en cuenta la idoneidad, necesidad y proporcionalidad, para determinar, en función de las circunstancias

concurrentes en cada supuesto, si el interés legítimo del investigador debe prevalecer o no sobre el derecho de los afectados.

- Tratamiento Transparente: Se ha de informar al interesado o a sus progenitores, de manera comprensible, transparente y con un lenguaje fácil y sencillo de entender, evitando cualquier jerga profesional, del tratamiento que se va a realizar con sus datos personales así como de sus posibles riesgos o consecuencias en el mismo momento o con anterioridad a la recogida de los datos.

En particular, de acuerdo con el art 13 del RGPD y art 11 de LOPDGDD, el interesado debe conocer como mínimo la identidad y datos de contacto del investigador principal (IP), los datos que se van a recabar y tratar, lo que se quiere hacer con los datos, los posibles destinatarios a los que se comuniquen o con quienes se compartan los datos, durante cuánto tiempo se van a conservar, dónde se van a guardar o almacenar, así como el ejercicio de sus derechos de acceso, rectificación y supresión.

Los investigadores deben asegurarse de que todos los participantes reciban y conocen la información prescrita ya sea en formato papel o electrónico y deben poder demostrar que dicha información se ha proporcionado correctamente ante posibles quejas o reclamaciones.

Asimismo, en el marco de algunas investigaciones es frecuente que los datos personales no se hayan recabado directamente de los participantes sino que se hayan obtenido a través de otros proyectos de investigación o de organizaciones externas. En estos casos, la obligación de transparencia persiste y se debería proporcionar igualmente a cada uno de los sujetos participantes la información descrita con indicación de la categoría de datos que se van a tratar y de la fuente de donde se han obtenido. Sin embargo, no es necesario proporcionar dicha información si ya se la hubiera facilitado con anterioridad a los participantes; o hacerlo implicaría un esfuerzo desproporcionado; o bien impediría seriamente el logro de los objetivos de la investigación. Obviamente, estos casos concretos deben ser justificados.

II. Limitación de finalidad

Los datos se recogerán únicamente para fines determinados, explícitos y concretos, y no serán tratados para otros usos o finalidades posteriores que sean incompatibles con ese fin original. Por ello, los investigadores deberán adquirir el compromiso explícito de no traspasar datos o muestras biológicas a otros proyectos u otros investigadores sin la previa autorización o consentimiento de los sujetos participantes en el estudio o investigación.

Si las finalidades fueran varias, el interesado deberá ser informado oportunamente para otorgar su consentimiento para cada una de las finalidades previstas de modo independiente e inequívoco.

No obstante, el tratamiento ulterior de los datos con fines de investigación científica, histórica o estadística no se considerará incompatible con los fines iniciales o principales para los que se recabaron los datos. En consecuencia, se podrán utilizar, por ejemplo, los datos demográficos obtenidos de la matrícula de los alumnos para estudios científicos, históricos o estadísticos.

En el caso de las investigaciones en materia de salud y biomédica, se podrán utilizar los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial para el que se obtuvo el consentimiento.

III. Minimización

Exclusivamente se recabarán y tratarán aquellos datos personales que sean adecuados, idóneos y pertinentes para el objeto de la investigación, eliminando aquellos otros datos que sean considerados innecesarios, accesorios o intrascendentes.

Por esta razón, se deberá tener especial cuidado en el proceso de toma y recogida de datos, sobre todo en grabaciones, cuestionarios y entrevistas, en no recabar ni tratar datos personales que sean superfluos o innecesarios para el objeto del estudio o investigación. En el caso de que, accidental o incidentalmente, se hayan recabado datos personales considerados intrascendentes o superfluos, éstos deberán eliminarse inmediatamente y no ser objeto de tratamiento.

IV. Limitación del plazo de conservación

Los datos personales no se conservarán durante más tiempo del imprescindible para los fines del tratamiento y, en consecuencia, deberán ser destruidos o anonimizados cuando hayan dejado de ser necesarios o pertinentes para la finalidad de la investigación para la cual hubieren sido recabados o registrados.

Sin embargo, la actividad de investigación científica, por su propia naturaleza, implica el transcurso de un período de tiempo indeterminado, a la vez que la conservación de los datos resulta imprescindible para poder contrastar la veracidad de los resultados. Por ello, los datos se conservarán de manera seudonimizada o disociada, de modo que no resulte posible reidentificar a las personas, garantizándose que la confidencialidad quedará preservada.

No obstante, hay que tener en cuenta que en algunos casos las leyes establecen un plazo mínimo de conservación, p.ej. el art 17.1 de la Ley 41/2002 de autonomía del paciente prevé que la documentación clínica (historia clínica) debe conservarse 5 años como mínimo desde la fecha del alta de cada proceso asistencial, la Ley 14/2007 de Investigación biomédica exige que los datos deben conservarse durante al menos 30 años cuando sea preciso asegurar la trazabilidad de células y tejidos que se hayan aplicado en humanos con fines de investigación (art 8) o el RD 1090/2015, que regulan los ensayos clínicos con medicamentos, establece que el investigador conservará el contenido del archivo maestro de cada ensayo clínico durante al menos 25 años tras la finalización del ensayo (art 43).

Por ello, los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables y una vez transcurrido dicho plazo deberán eliminarse, cifrarse o anonimizarse de modo que no se pueda identificar a las personas afectadas en aras de proteger sus derechos.

V. Seguridad y confidencialidad

Tal y como establece el punto 10 del Código de Buenas prácticas en investigación de la UAM, los investigadores así como todas las personas que intervengan en cualquier fase del estudio o investigación estarán sujetas al deber de confidencialidad y guardarán la debida discreción sobre los datos de las personas participantes en el proyecto que conozcan en el desempeño de sus tareas, tanto en los procesos de su obtención, tratamiento y conservación como en la posterior publicación de los resultados, no comunicándoselos o traspasándoselos a otros investigadores ni los utilizaran para otros proyectos de investigación sin el previo consentimiento o autorización de los afectados.

En consecuencia, el investigador deberá comprometerse a implementar las medidas técnicas u organizativas apropiadas para garantizar la confidencialidad y seguridad de los datos con el objeto de impedir cualquier acceso o tratamiento no autorizado o ilícito así como contra su alteración, pérdida, destrucción accidental o divulgación, de acuerdo con el estado de la técnica, los costes de aplicación, la naturaleza del tratamiento o los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas participantes en la investigación.

Con el objeto de minimizar los riesgos, el acceso a los datos personales debe estar siempre restringido y limitado a aquellas personas o colaboradores que tengan necesidad de conocerlos. Por tanto, en el caso de que no esté justificado el acceso y tratamiento generalizado de los datos por parte de todos los miembros del equipo investigador, colaboradores o personal de apoyo, es preciso determinar quiénes deben tener acceso, a qué datos y por cuanto tiempo.

Entre las medidas de seguridad a adoptar se recomienda, entre otras, las siguientes:

- la seudonimización, la disociación y el cifrado de datos personales;
- el almacenamiento de los archivos que contengan datos personales se realizará en sistemas o servidores ubicados en lugares seguros preferiblemente en los espacios de red y aplicaciones corporativas habilitadas para ello por la UAM y no se realizará en dispositivos externos como pendrive, CD, discos externos, etc. para evitar su posible deterioro, extravío o robo;
- establecer procedimientos de autenticación y control de acceso a los ficheros, preferiblemente utilizando el doble factor de autenticación (2FA);
- realizar copias de seguridad para garantizar la integridad y disponibilidad de forma rápida en caso de incidente físico o técnico;
- utilizar antivirus, antimalware o firewall actualizados como medios de resiliencia permanentes de los sistemas y servicios de tratamiento;
- los archivos que contengan datos, una vez que ya no sean necesarios para los fines de la investigación, serán destruidos de tal forma que la información no pueda ser recuperada por terceros.

Todos los usuarios de la UAM, incluido los investigadores, deben ser conscientes de la necesidad de garantizar la seguridad e integridad de los sistemas de información que utilicen y la confidencialidad de los datos personales que traten. Por ello, tienen la obligación de conocer y cumplir todas las medidas de seguridad conforme a las instrucciones y procedimientos establecidos por la Universidad.

- Real Decreto 311/2022, de 3 de mayo, Esquema Nacional de Seguridad (ENS)

- Acuerdo 18/CG de 17-06-22 por el que se aprueba la Normativa sobre el equipamiento informático de uso individual gestionado por la Unidad de Tecnologías de la Información
- Acuerdo 5/CG de 14-07-16 por el que se aprueba la Normativa general de uso de recursos TIC y sistemas de información de la Universidad Autónoma de Madrid

El RGPD define «*brecha de seguridad o incidente de seguridad*» como cualquier violación de la seguridad de los datos personales que ocasionen su destrucción, pérdida o alteración accidental o ilícita de los datos transmitidos, conservados o tratados, o bien la comunicación o acceso no autorizados a dichos datos.

La UAM, como responsable del tratamiento, tiene la obligación de notificar a la Agencia Española de Protección de Datos (AEPD) cualquier brecha que atañe a 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 Delegado/a de Protección de Datos (DPD) de la UAM a fin de poder cumplir con esta obligación.

7. EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS (EIPD)

De acuerdo con el art. 35 del RGPD, aquellas actividades o tratamiento de datos personales en los que es probable que entrañen un alto riesgo para los derechos y libertades de las personas a las que se refieren los datos deben someterse previamente a un análisis de riesgo y evaluación de impacto (EIPD) con la finalidad de poder identificar, evaluar y gestionar, de forma previa y anticipada, los riesgos y establecer las medidas técnicas y organizativas más adecuadas para reducirlos hasta un nivel considerado aceptable.

Por consiguiente, no todas las actividades o tratamientos con datos personales requieren realizar una evaluación de impacto, solamente aquellas que puedan suponer con cierta probabilidad un alto riesgo para los derechos y libertades de los interesados y, en particular, cuando se lleve a cabo:

- procesamiento a gran escala de datos utilizando las nuevas tecnologías de Big Data
- tratamiento de datos con el objeto de realizar, a través de una evaluación sistemática y exhaustiva de aspectos personales, el perfilado, valoración y seguimiento de individuos
- tratamiento de datos de categoría especial (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 o vida sexual de una persona física)
- tratamiento de datos de sujetos vulnerables o en riesgo de exclusión social, incluyendo datos de menores de 14 años, mayores con algún grado de discapacidad, personas que acceden a servicios sociales y víctimas de violencia de género

En cualquier caso, la AEPD ha publicado con carácter orientativo un listado no exhaustivo con los tratamientos que requieren la realización previa de una EIPD. Cuantos más criterios reúna el tratamiento en cuestión, mayor será el riesgo que entrañe dicho tratamiento y mayor será la certeza de la necesidad de realizar una EIPD

Listado orientativo de tipos de tratamientos de datos que requieren EIPD

Al respecto, y como probablemente muchos proyectos de investigación pueden realizar estos tratamientos, se puede solicitar el asesoramiento del Delegado/a de Protección de Datos (DPD) al objeto de ayudar en la realización de la EIPD y dar cumplimiento a esta obligación.

8. CESIÓN O COMUNICACIÓN DE DATOS

Se produce una comunicación de datos cuando el responsable del tratamiento o el personal autorizado para tratar los datos facilitan el acceso, consulta, comunicación por transmisión, interconexión, transferencia, difusión o divulgación de los datos personales a un tercero o destinatario, entendiendo por tal una persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado o del encargado del tratamiento.

No siempre la transferencia o comunicación de datos entre los diferentes miembros de un grupo investigador o colaboradores supone una cesión de datos a efectos del RGPD, si es que estos sujetos no son considerados terceros, y en la medida en que solo accederán a la información necesaria para el desarrollo de las tareas asignadas por cuenta del investigador responsable (IP). Ahora bien, puede ser conveniente que las actividades y sus condiciones se reflejen en un acuerdo que garantice que el tratamiento se lleva a cabo en las condiciones adecuadas.

La comunicación o cesión de los datos debe estar sustentada en una base legitimadora explícita y específica del art 6 del RGPD, p. ej. una obligación legal, celebración de un contrato o en el consentimiento explícito de los afectados. Si no existe dicha habilitación, no se pueden comunicar los datos personales a otros investigadores o terceras personas porque se infringiría el deber de confidencialidad.

Asimismo, se debe informar previamente al titular de los datos de los posibles destinatarios o terceros a los que se les va a comunicar o compartir sus datos y con qué finalidad para que, si lo consideran conveniente, pueda oponerse en cualquier momento a dicho tratamiento si está basado en el consentimiento.

La publicación y difusión de los resultados de la investigación si se realiza con datos agregados, disociados o seudomizados, de manera que no se puedan identificar inequívocamente a las personas participantes en el estudio o investigación, no tendrán la consideración de cesión o comunicación de datos. No sería el caso, y se requiere el consentimiento explícito de los afectados, cuando se comunican datos de carácter personal a repositorios o biobancos con fines de investigación científica si las muestras se almacenan asociadas a los datos de los sujetos.

9. TRANSFERENCIA INTERNACIONAL DE DATOS

Se entiende por transferencia internacional de datos, el acceso, tratamiento, almacenamiento, transmisión, comunicación o flujo de datos personales, sea cual sea el

medio que se utilice, desde el territorio español a un destinatario, organización o entidad que se encuentra en un país fuera de las fronteras del Espacio Económico Europeo (EEE).

Por ejemplo, esta situación podría darse cuando los datos personales se han recabado en España pero un colaborador accede a ellos desde Chile, o bien los datos se almacenan en un prestador de servicios "cloud" o en la nube cuyos servidores están ubicados en Estados Unidos.

El RGPD contempla la posibilidad de que se pueda realizar una transferencia internacional de datos a entidades u organismos situados en un tercer país cuando éste pueda garantizar un nivel de protección adecuado y los interesados disfruten de derechos equivalentes o similares que en la Unión Europea (UE).

Supuestos previstos:

1. Países que han sido declarados que tienen un nivel de protección adecuado por la Comisión Europea.
   Hasta la fecha, la lista de los países son: Andorra, Argentina, Canadá, Corea del Sur, Guernsey, Isla de Man, Islas Feroe, Israel, Japón, Jersey, Nueva Zelanda, Reino Unido, Suiza y Uruguay.

2. Si la entidad receptora de los datos ofrece garantías adecuadas, que podrán ser aportadas a través de:
   a. Normas corporativas vinculantes o "Binding Corporate Rules" (BCR) que son políticas de protección de datos personales o códigos de conducta jurídicamente vinculantes dentro de un grupo de empresas.
   b. Cláusulas contractuales tipo o "Standard Contractual Clauses" (SCC) adoptadas por la Decisión (UE) 2021/914 de la Comisión de 4 de junio de 2021 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.
   c. Códigos de conducta aprobados o certificaciones en materia de protección de datos

3. A falta de garantías adecuadas, se requerirá que el interesado haya dado explícitamente su consentimiento informado a la transferencia propuesta.

Si no resultase aplicable ninguna de estas excepciones, solo y exclusivamente se podrá llevar a cabo una transferencia internacional de datos si es con carácter ocasional, afecta solo a un número limitado de personas, es necesaria a los fines de intereses legítimos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos de los interesados, y se ofrezcan garantías apropiadas con respecto a la protección de datos personales.

A este respecto, y en caso de que colaboren en el proyecto de investigación miembros de otros países, se puede consultar con el Delegado/a de Protección de Datos (DPD) al objeto de asesoramiento para dar cumplimiento a esta obligación

10. DERECHOS DE LOS INTERESADOS

Cualquier persona que participe en el proyecto o estudio de investigación podrá ejercer ante el investigador principal (IP) o ante el Delegado/a de Protección de Datos (DPD), conforme a lo establecido en los artículos 15 a 22 del RGPD, sus derechos relacionados con el tratamiento de sus datos personales.

Tan solo se podrán limitar excepcionalmente los derechos de acceso, rectificación, limitación y oposición, según el apartado 2 del art. 89 RGPD, si el ejercicio de tales derechos imposibilitan u obstaculizan gravemente el logro de los fines científicos de la investigación. Obviamente deberá justificarse y motivarse razonadamente.

I. Derecho de acceso

Cualquier persona tiene el derecho a obtener confirmación de si está realizando algún tratamiento o no con sus datos personales y, en caso afirmativo, a conocer qué datos se están tratado, el uso que se haya hecho con ellos, a quién se les ha comunicado, cuánto tiempo se van a conservar y a obtener una copia de los mismos.

Si se tratan una gran cantidad de datos, el investigador podrá solicitar al interesado que especifique los datos personales a los que se refiere en su solicitud, concretando si se refiere a todos o solo a una parte de ellos.

Este derecho subsiste durante todo el periodo de archivo y custodia de los datos como información personal, es decir, hasta su supresión o anonimización.

II. Derecho de rectificación

El sujeto participe en la investigación tiene derecho a rectificar, modificar y actualizar en cualquier momento sus datos personales que sean inexactos, obsoletos o incompletos.

Al ejercer este derecho el afectado deberá indicar en su solicitud a qué datos en concreto se refiere y la corrección que haya de realizarse, acompañando la documentación justificativa de la inexactitud o carácter incompleto de los datos, cuando ello sea preciso.

Este derecho no tiene una gran trascendencia en el campo de la investigación científica pues la metodología y el rigor de la propia investigación exige la exactitud y fiabilidad de la información que se maneja para obtener conclusiones sólidas y rigurosas.

III. Derecho de limitación del tratamiento

El participante en el estudio o investigación tiene el derecho a limitar el uso que se haga de sus datos personales bien por un determinado tiempo (p.ej. mientras se hacen las verificaciones correspondientes cuando se haya opuesto al tratamiento o bien mientras presenta una reclamación) bien para determinados usos o finalidades en el caso de ser varios los fines del tratamiento.

La revocación del consentimiento para determinados usos o finalidades no afectará a las actividades de tratamiento realizadas con anterioridad a su retirada pero una vez ejercido la limitación del tratamiento los datos no serán objeto de tratamiento ulterior.

IV. Derecho de oposición al tratamiento

El interesado puede oponerse en cualquier momento al tratamiento de sus datos de carácter personal por motivos o circunstancias particulares y, en su caso, solicitar el cese inmediato de los mismos salvo que la investigación científica sea necesaria para el cumplimiento de un interés público o el investigador acredite intereses legítimos que deban prevalecer sobre los derechos y las libertades de la persona interesada.

V. Derecho de supresión o cancelación

Cualquier persona que participe en el estudio tiene el derecho a solicitar al investigador que sus datos personales sean suprimidos, borrados o cancelados cuando resulten inadecuados, excesivos o ya no sean necesarios para la finalidad para la que fueron recogidos, cuando se haya retirado el consentimiento en que se basa su tratamiento o cuando hayan sido recabado de forma ilícita.

Por tanto, existe la obligación de suprimir, cancelar o borrar los datos si lo solicita expresamente la persona afectada. No obstante, este derecho no es absoluto y puede verse limitado en algunos casos cuando la legislación aplicable exige unos plazos mínimos de conservación de los datos como se prevé en la ley 14/2007 de Investigación biomédica o en el RD 1090/2015, que regulan los ensayos clínicos con medicamentos.

La revocación del consentimiento no afectará a la licitud del tratamiento realizado antes de su retirada, en consecuencia, los efectos del ejercicio de este derecho no se extenderán a los datos resultantes de las investigaciones que se hubiesen realizado con carácter previo o a las actividades llevadas a cabo en base a su consentimiento antes de haberlo retirado.

VI. Derecho a no ser objeto de decisiones individuales automatizadas

En el supuesto de que se realice un tratamiento automatizado de sus datos con la finalidad de evaluar, estudiar o analizar determinados aspectos relacionados con su persona, incluida la elaboración de perfiles, que puedan producir efectos jurídicos en él o le afecte significativamente, el interesado podrá oponerse al mismo y a no ser objeto de decisiones que sean tomadas exclusivamente por medios automatizados sin intervención humana.

11. DIFUSIÓN Y PUBLICACIÓN DE LOS RESULTADOS DE LA INVESTIGACIÓN

La difusión de los resultados es uno de los principales objetivos de la investigación científica en la universidad. La publicación de los resultados fruto de la investigación o estudio clínico

en revistas u otros medios con revisión por pares es considerada como uno de los mejores modos de difundir y transferir el conocimiento a la sociedad.

Con carácter general, deberá tenderse a la anonimización o disociación de los datos publicados para que no pueda identificarse a las personas que han participado en la investigación, excepto cuando las características del estudio, su metodología o el interés público debidamente justificado requieran otro procedimiento. Es evidente, que cuando la identificabilidad del dataset no resulte relevante para validar la verificación y reproducibilidad de los resultados obtenidos hay que anonimizar los datos personales para facilitar su reutilización en repositorios institucionales de acceso abierto.

No obstante, si fuera estrictamente imprescindible facilitar o publicar los datos brutos registrados durante el ciclo de vida del proyecto y asociados a los sujetos participantes en la investigación para contrastar la calidad y veracidad de los resultados obtenidos o bien por las exigencias referentes a los datos utilizados específicamente para un artículo que las editoriales científicas puedan requerir a los investigadores, será necesario recabar previamente el consentimiento explícito de los afectados para poder difundir sus datos personales en concordancia con la normativa de protección de datos porque, en caso contrario, se trataría de una comunicación o cesión ilícita de datos a terceros no autorizados, infringiendo el deber de confidencialidad.