Crue-Secretarías Generales

Comision Delegada del grupo de Trabajo de Delegadas y Delegados de Protección de Datos

Guía para delegados de protección de datos.

Guía sobre la protección de datos en los proyectos de investigación.

*Como citar este informe:

Guía sobre la protección de datos en los proyectos de investigación

Este documento de trabajo responde exclusivamente a las opiniones de sus autores

FECHA: Febrero 2024

Grupo de Trabajo Delegadas y Delegados de Protección de Datos.

Universidades participantes:

Universidad de Barcelona	Ruben Ortiz
Universidad Carlos III	José Furones
Universidad de la Coruña	Luz María Puente
Universidad Miguel Hernández	Esther Botella
Universidad de Murcia	Ignacio Fontán
Universidad de la Rioja	Pilar Ovejas
Universidad de Sevilla	Margarita Martínez-Pais

Índice

Alcance de la presente Guía

La Guía está dirigida a delegados de protección de datos de Universidades, los cuales, dentro de las funciones atribuidas por el artículo 39 del Reglamento (UE) 2016/679 General de Protección de Datos (en adelante, RGPD), lleven a cabo funciones de asesoramiento, supervisión y control de tesis doctorales, trabajos fin de titulación u otros trabajos académicos (en adelante, la actividad o actividades). Por tanto, se omitirá información y explicaciones que, atendiendo a su ámbito de conocimiento, se entienden como adquiridas.

Como documento complementario a esta Guía, se aporta un manual o documento destinado a aquellas personas que realicen este tipo de actividades, cuyo fin es pedagógico y de concienciación, evitando utilizar en exceso terminología jurídico-técnica que pueda confundir al lector, tratando de apoyar cada uno de los apartados en ejemplos prácticos.

AVISO

Este documento se trata de una guía sobre cómo cumplir la normativa de protección de datos personales en los tratamientos de datos personales que se originen en proyectos y actividades de investigación científica. Su contenido no vincula a los delegados de protección de datos de las universidades, los cuales tienen independencia en el ejercicio de las funciones de asesoramiento y supervisión que les establece la normativa de protección de datos personales.

1. Definiciones

1.1. Dato personal (art. 4.1 del RGPD)

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 (en adelante RGPD), en su artículo 4 apartado 1 define **dato personal** como "toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo 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".

Algunos ejemplos de datos personales pueden ser: Datos identificativos: Nombre y apellidos, DNI/CIF/Documento identificativo, dirección (postal y electrónica), firma, teléfono; imagen; voz; Datos de características personales: Sexo, estado civil, nacionalidad, edad, fecha y lugar de nacimiento y datos de circunstancias familiares, datos relacionados con la salud. Datos de circunstancias laborales: Fecha de alta y baja, licencias, permisos y autorizaciones; Datos académicos y profesionales: Titulaciones, formación y experiencia profesional; Datos de localización; Direcciones IP: si es estática, siempre; si es

dinámica, solo cuando pueda vincularse indirectamente a una persona concreta.

1.2. Datos personales seudonimizados (Considerando 26 del RGPD)

Según el RGPD la información personal seudonimizada sigue siendo información personal y, por lo tanto, son objeto de la normativa de protección de datos personales. Según el artículo 4 del RGPD datos personales seudonimizados son aquellos datos personales que ya no pueden atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyen a una persona física identificada o identificable.

Por lo tanto, los datos personales seudonimizados, son aquellos que cabría atribuir a una persona física mediante la utilización de información adicional, y deben considerarse información sobre una persona física identificable. La seudonimización es una medida de seguridad.

Por ejemplo, si se hace una entrevista a una persona y se remite el contenido de la misma a otro colaborador indicando que se trata del entrevistado 2859artz. Pero la relación entre la persona entrevistada y el identificador 2859artz se mantiene aparte por otra persona y no está accesible al investigador a quien se le remite el contenido de la entrevista para que trabaje con esa información.

1.3. Datos anónimos y datos anonimizados (Considerando 26 del RGPD)

Datos anónimos o anonimizados se refieren a aquella información que no guarda relación con una persona física identificada o identificable. La información (los datos) convertida en anónima es aquella en la que el interesado no sea identificable, o deje de serlo. Dato anónimo es aquel que se ha obtenido sin que exista ninguna relación con una persona identificable. Dato anonimizado es aquel dato que con anterioridad se podía relacionar con una persona identificable pero, después de aplicarle determinadas técnicas, ha perdido dicha relación con la persona física.

La normativa y los principios de protección de datos no resultan de aplicación a la información anónima.

En relación con la consideración de una información como anónima hay que tener en cuenta lo siguiente:

- Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física.
- Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos.

  Por ejemplo, si yo hago una encuesta en la que solicito información que no identifica directamente a una persona: género, población de nacimiento y titulación universitaria, esta información podría hacer identificable a una persona, en los casos en los que se hubiera nacido en una población con pocos habitantes donde hay pocas personas con estudios universitarios y

son, por tanto, identificables. En estos casos deberíamos adoptar medidas técnicas para anonimizar esa información como pudiera ser la eliminación de la información de estos casos en los que hay pocas personas en un campo de información determinado. Este proceso técnico se denomina K anonimización.

En el siguiente enlace se puede consultar el Dictamen del Grupo de trabajo GT29 5/2014 sobre técnicas de anonimización: https://www.aepd.es/sites/default/files/2019-12/wp216-es.pdf

En el siguiente enlace se puede consultar la guía de la AEPD sobre procedimientos de anonimización: https://www.aepd.es/es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf

En el siguiente enlace se puede consultar la guía de la AEPD sobre posibles malentendidos sobre procedimientos de anonimización: https://www.aepd.es/es/node/46262

En el siguiente enlace se puede consultar la Guía básica de Anonimización de la Autoridad de Protección de Datos de Singapur: https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/guia-y-herramienta-basica-de-anonimizacion

1.4. Tratamiento (Art. 4.2 del RGPD)

El RGPD en su artículo 4.2 define tratamiento como cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como:

- Recogida (captura de información donde existen datos de carácter personal);
- Registro (inscribir o grabar la información en algún tipo de sistema o dispositivo, automatizado o no automatizado, para su posterior tratamiento);
- Organización (ordenar y estructurar la información para facilitar su tratamiento);
- Conservación (mantener la información durante un determinado periodo de tiempo);
- Adaptación o modificación (alterar o cambiar la información);
- Extracción (obtener la información de un sistema o dispositivo original para su envío o traspaso a otro sistema o dispositivo);
- Consulta (buscar los datos sobre el sistema o dispositivo en el que se encuentra registrada);
- Utilización (usar la información para una finalidad concreta);
- Comunicación por transmisión (enviar los datos a otro destinatario desde su sistema o dispositivo origen a través de medios electrónicos);
- Difusión o cualquier otra forma de habilitación de acceso, cotejo, o interconexión, limitación (poner a disposición de otros usuarios o destinatarios la información registrada en un sistema o dispositivo);
- Supresión (eliminar, hacer desaparecer la información en el sistema o dispositivo en el que esté originalmente registrada);
- Destrucción (inutilizar un soporte físico para evitar el acceso a la información)

1.5. Responsable del tratamiento (Art. 4.7 del RGPD)

Responsable del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

Por lo tanto, siempre que, para el desarrollo de la actividad de investigación, el investigador trate un dato personal, la Universidad o el órgano que se haya establecido será responsable de dicho tratamiento, y el investigador estará obligado a cumplir con la normativa de protección de datos personales (RGPD y Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales, en adelante, LOPDyGDD) según las normas y directrices que haya podido dictar el responsable del tratamiento.

1.6. Corresponsabilidad del tratamiento (Art. 26 del RGPD)

Tiene lugar cuando dos o más entidades conjuntamente deciden los fines y los medios del tratamiento. En estos casos se deberá suscribir un acuerdo entre las partes que regule las funciones y relaciones respectivas de los corresponsables en relación con los interesados

Como ejemplo puede darse un supuesto de corresponsabilidad cuando dos o más universidades presentan un proyecto de investigación en el cual han definido conjuntamente el contenido de la encuesta que se realizará y han determinado la herramienta que se usará.

1.7. Encargado del tratamiento (Art. 4.8 y 28 del RGPD)

El encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

Por ejemplo, si contratamos la prestación de un servicio como el de almacenamiento en la nube de un tercero o la transcripción de las grabaciones de entrevistas, ese tercero es un encargado del tratamiento.

En estos casos deberá suscribirse un acuerdo de encargo de tratamiento.

Existen las siguientes cláusulas contractuales tipo aprobadas por la Comisión: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32021D0915

Y unas directrices aprobadas conjuntamente por la AEPD, la APDCAT y la AVPD: https://www.aepd.es/sites/default/files/2019-10/guia-directrices-contratos.pdf

1.8. Licitud del tratamiento (Art. 6 del RGPD)

Para poder tratar los datos personales se precisa de, el menos, una de las siguientes bases de legitimación:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

> Nota. Es importante no confundir el consentimiento para el tratamiento de los datos personales que regula el RGPD y al que se refiere este apartado, con el consentimiento informado que se puede requerir desde la ética u otra normativa (como por ejemplo la normativa reguladora de los

ensayos clínicos)

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

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

En caso de carecer de base de legitimación el tratamiento será ilícito.

1.9. Transferencia internacional de datos (Art. 44 y ss. del RGPD)

Las transferencias internacionales de datos suponen un flujo de datos personales desde el territorio español a destinatarios establecidos en países fuera del Espacio Económico Europeo (los países de la Unión Europea más Liechtenstein, Islandia y Noruega) o a organizaciones internacionales.

Se podrán hacer transferencias internacionales de datos en los siguientes casos:

- A un territorio o uno o varios sectores específicos de ese país u organización internacional que hayan sido declarados de nivel de protección adecuado por la Comisión Europea.
- Mediante la aportación de garantías adecuadas. Estas garantías podrán ser:
  a) Un instrumento jurídicamente vinculante y exigible entre autoridades u organismo públicos.

  b) Norma corporativas vinculantes.

  c) Cláusulas tipo. Que será una las garantías más frecuentemente utilizadas. A estos efectos la comisión ha aprobado las cláusulas que pueden localizarse aquí: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv%3AOJ.L_.2021.199.01.0031.01.SPA&toc=OJ%3AL%3A2021%3A199%3ATOC&utm_term=Nota+informativa+ELZABURU+-+Nuevas+Clausulas+Contractuales+Tipo+para+flujos+de+datos+personales&utm_campaign=Clientes+directos+espa%3Foles&utm_source=e-goi&utm_medium=email

  d) Códigos de conducta.

  e) Mecanismos de certificación

- Transferencias con autorización de una autoridad de control.
- En determinadas situaciones específicas (art. 49 RGPD)

Más información al respecto: https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/transferencias-internacionales

2. Principios de la protección de datos. ¿Cómo se deberían tratar los datos personales?

Los datos deben tratarse con sujeción a los siguientes principios:

El principio de licitud. Para poder tratar datos personales se debe disponer de, al menos, alguna de las condiciones vistas en el apartado 1.8 anterior denominado Licitud del Tratamiento;

El principio de lealtad y transparencia que supone la necesidad de informar al interesado; Según el principio de autodeterminación informativa que implica el derecho a la protección de datos, el interesado tiene derecho a conocer el tratamiento que se está haciendo de sus datos, por quien, por qué..., y ese derecho se convierte en una obligación para el responsable del tratamiento. Hay que facilitar la información a que se refiere el art. 13-14 del RGPD.

El principio de limitación de la finalidad que supone que los datos han de ser tratados para fines determinados explícitos y legítimos, sin que puedan utilizarse para fines incompatibles con los iniciales. No obstante, no se considerará incompatible con los fines iniciales el tratamiento con fines de archivo de interés público, fines de investigación científica e histórica o fines estadísticos.

Principio de minimización. Los datos objeto de tratamiento deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

Supone la necesidad de aplicar medidas técnicas y organizativas para garantizar que sean objeto de tratamiento los datos que únicamente sean precisos para cada uno de los fines específicos del tratamiento reduciendo la extensión del tratamiento, y limitando a lo necesario el plazo de conservación y su accesibilidad.

Sólo deben tratarse los datos que justificadamente sean necesarios para el desarrollo de la actividad de la investigación. Ante la duda o falta de clara justificación en cuanto a la necesidad del tratamiento de un dato personal, éste debe excluirse de dicho tratamiento.

En principio, la investigación se debe hacer con datos anónimos o anonimizados, y cuando los objetivos de la investigación no se puedan logran, sólo entonces se deberían usar datos personales seudonimizados y, en última instancia, sin seudonimizar.

Por otro lado, los datos deben estar accesibles exclusivamente a las personas debidamente autorizadas que deban tratar dichos datos. Por ejemplo: Si un investigador trabaja con unos determinados datos para realizar la parte que le corresponde de su actividad, no debe tener acceso a otros cuyo tratamiento no es

necesario para la actividad que desarrolla dicho investigador. Habrán de adoptarse medidas técnicas y organizativas para evitar que esto ocurra, como organizar la información con permisos de acceso a partes determinadas de la misma.

El principio de limitación del plazo de conservación, de modo que no sean tratados por más tiempo que el necesario para los fines del tratamiento. Una vez transcurrido el plazo de tratamiento los datos deberán ser destruidos o anonimizados.

Los principios de integridad y confidencialidad, adoptando las medidas necesarias para la garantía de su seguridad de modo que se eviten los riesgos de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Todo ello, además, desde el principio de la responsabilidad proactiva. Se deben cumplir estos principios y, al mismo tiempo, debemos ser capaces de demostrar que los cumplimos.

Además, el RGPD regula el principio de Protección de datos desde el diseño y por defecto:

Protección de datos desde el diseño: Teniendo en cuenta las circunstancias del tratamiento y los riesgos para los derechos de los interesados, el responsable aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebida para aplicar de forma efectiva los principios de protección de datos, o como la minimización de datos, y deberá integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del RGPD y proteger los derechos de los interesados.

La AEPD ha aprobado una guía sobre este principio que puede consultarse en el siguiente enlace: https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf

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

Por lo tanto, para la aplicación de este principio deben adoptarse medidas en los siguientes cuatro ámbitos:

a) La cantidad de datos personales objeto de tratamiento, que, habrán de ser exclusivamente los necesarios;
b) La extensión del tratamiento, que se refiere al alcance del mismo y que habrá de ser el menor de los posibles para cumplir la finalidad del tratamiento (para la publicación de información que pueda afectar a un grupo de interesados, la misma debe realizarse en una intranet y no en abierto con acceso universal);

c) El periodo de conservación, que deberá limitarse al tiempo necesario para cumplir la finalidad del tratamiento, y
d) la accesibilidad de los datos, de modo que, por defecto, sólo estén accesibles a aquellas personas que precisen su tratamiento en el proyecto de investigación los datos necesarios para el desarrollo de las funciones de esa persona y no otros que no lo sean. Por ejemplo, no debemos compartir los datos en una carpeta accesible a todos los miembros de un equipo de investigación si no está justificada la necesidad que todos los miembros deban acceder a todos los datos, sino cada dato o grupo de datos a quien deba tratarlos para el desarrollo de su función.

La AEPD ha aprobado una guía sobre este principio que puede consultarse en el siguiente enlace: https://www.aepd.es/es/media/guias/guia-proteccion-datos-por-defecto.pdf

3. ¿Qué derechos pueden ejercer los participantes en la investigación?

Los participantes en los proyectos de investigación pueden solicitar mediante el correspondiente procedimiento adoptado por el responsable del tratamiento el ejercicio de los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad, oposición.

Derecho de acceso (art. 15 del RGPD): permite al participante en la investigación obtener confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, la información relativa al uso que se hace de sus datos personales, con qué finalidad y legitimación se realiza el tratamiento, la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos, de ser posible el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo, y la posible existencia de decisiones automatizadas, incluida la elaboración de perfiles. Este derecho incluye la posibilidad que la persona participante obtenga una copia de los datos personales que se estén tratando en la actividad de investigación.

Derecho de rectificación (art. 16 del RGPD): La persona participante tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional. Para el ejercicio del derecho, la persona interesada deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento.

Derecho de supresión ("el derecho al olvido") (art. 17 del RGPD): El derecho a la supresión es la consecuencia del derecho que tienen los ciudadanos a solicitar y obtener de los responsables, que los datos personales sean suprimidos cuando, entre otros casos, estos ya no sean necesarios para la finalidad con la que fueron recogidos, cuando se haya retirado el consentimiento o cuando estos se hayan recabado de forma ilícita.

Derecho a la limitación del tratamiento (art. 18 del RGPD): El derecho a la limitación tiene como efecto

el cese en el tratamiento, pero con carácter transitorio o parcial, por un determinado periodo de tiempo o con determinados fines. El interesado puede solicitar la limitación en el tratamiento en varios supuestos, por ejemplo, cuando impugne su exactitud, mientras el responsable hace las verificaciones correspondientes o cuando se haya opuesto al tratamiento mientras se verifica si los motivos legítimos del responsable prevalecen.

Derecho a la portabilidad (art. 20 del RGPD): Permite a las personas interesadas recibir los datos personales que han proporcionado a un responsable del tratamiento, en un formato estructurado, de uso común y legible por máquina, así como transmitirlos a otro responsable del tratamiento, siempre y cuando sea técnicamente posible y sin necesidad de la intervención de la persona interesada. Sólo se aplica si su tratamiento se lleva a cabo por medios automatizados y, por lo tanto, no cubre los archivos en papel. Para poder ejercer este derecho, las operaciones del tratamiento deben basarse bien en el consentimiento de la persona interesada, o bien en un contrato. Los tratamientos basados en otra base de legitimación no son objeto de este derecho.

Derecho de oposición (art. 21 del RGPD): Por motivos relacionados con su situación particular los participantes pueden oponerse a que el responsable realice un tratamiento de sus datos personales; incluso cuando se traten con fines de investigación científica o histórica o fines estadísticos, siempre que la licitud del tratamiento se base en el cumplimiento de una misión de interés público, en el ejercicio de poderes públicos o para la satisfacción de un interés legítimo. El responsable dejará de tratarlos salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

¿Puede haber excepciones a los derechos de los participantes? Conforme establece el artículo 89.2 del RGPD: “Cuando se traten datos personales con fines de investigación científica o histórica o estadísticos el Derecho de la Unión o de los Estados miembros podrá establecer excepciones a los derechos contemplados en los arts. 15, 16, 18 y 21” pero estas excepciones están sujetas a ciertas limitaciones, puesto que solo se podrán prever si es que el ejercicio de los derechos pudiera implicar un obstáculo para el logro de los fines científicos y cuanto estas sean necesarias para alcanzar esos fines. Estos artículos se refieren a los derechos de acceso, rectificación, limitación y oposición.

La disposición adicional decimoséptima de la LOPDyGDD contempla esta posibilidad en su letra e). Cuando se traten datos personales con fines de investigación en salud, y en particular la biomédica, en tres supuestos: primero, los derechos se ejerzan directamente ante los investigadores o centros de investigación que utilicen datos anonimizados o seudonimizados; segundo, cuando su ejercicio se refiera a datos obtenidos en la investigación y, tercero cuando su ejercicio pueda comprometer determinados intereses (seguridad del Estado, la defensa, la seguridad pública u otros objetivos importantes de interés público general), siempre que en este último caso la excepción esté expresamente recogida por una norma con rango de Ley.

4. ¿Cuándo y cómo se debe realizar una evaluación de impacto relativa a la protección de datos personales?

Una evaluación de impacto relativa a la protección de datos (EIPD), es un proceso de análisis del tratamiento de datos personales que pretende determinar las medidas técnicas y organizativas que se deben implementar para reducir los riesgos que el tratamiento puede ocasionar a las personas titulares de los datos personales con carácter previo al inicio del tratamiento. Sobre la EIPD se pueden consultar las directrices WP248 del Comité Europeo de Protección de Datos y del anterior Grupo de Trabajo del Art. 29.

El artículo 35 del RGPD establece que será obligatorio realizar una EIPD siempre que el tratamiento comporte un **alto riesgo** para los derechos y libertades de las personas físicas. La AEPD, la APDCAT, la AVPD y el CTPDA a partir de las , han elaborado la lista siguiente de criterios para determinar si un tratamiento puede comportar dicho alto riesgo:

1) **Tratamiento que implique la evaluación o puntuación de aspectos personales**, incluida la elaboración de perfiles. (Ej. Se realiza un proyecto en colaboración con un banco al efecto de mejorar los algoritmos que se utilizan para evaluar a los clientes mediante una base de datos de utilización de las tarjetas de crédito)
2) **Tratamiento que implique la toma de decisiones automatizadas con efectos jurídicos significativos o similares**. (Ej. Se desarrolla un algoritmo que califica a los estudiantes a partir de determinadas evidencias académica sin intervención del profesorado)
3) **Tratamiento que implique la observación sistemática de las personas**. ((Ej. Videovigilancia de las personas que pasan por una plaza, que entran en un centro comercial o en una biblioteca pública al efecto de estudiar su movilidad)
4) **Tratamiento de datos sensibles**: tratamiento de categorías especiales de datos a las que se refiere el art. 9.1 del RGPD, de datos relativos a condenas o infracciones penales a que se refiere el art. 10, o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos.
5) **Tratamientos que impliquen el uso de datos biométricos** con el propósito de identificar de manera única a una persona física.
6) **Tratamientos que impliquen el uso de datos genéticos** para cualquier fin.
7) **Tratamiento de datos a gran escala**: el GT29 recomienda que se utilicen los siguientes criterios para determinar si se realiza un tratamiento a gran escala:
    a) Número de personas afectadas, bien como cifra concreta o como proporción de la población correspondiente
    b) Volumen de datos o la variedad de datos
    c) Duración del tratamiento
    d) Alcance geográfico del tratamiento

8) **Tratamiento que implique el cruzamiento de conjuntos de datos** provenientes de otros tratamientos o diferentes responsables de tal manera que exceda las expectativas razonables de las personas interesadas.
9) **Tratamiento de datos referentes a personas vulnerables**: cualquier caso en que se pueda identificar un desequilibrio en la relación entre la posición del interesado y el responsable del tratamiento (Ej. Tratamiento de datos de menores, asilados, pacientes).
10) **Tratamiento que requiera el uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas**. (Ej. Combinar el uso de huellas dactilares y reconocimiento facial para controlar el acceso).
11) **Tratamiento que impida ejercer un derecho o utilizar un servicio o ejecutar un contrato**: se incluyen los tratamientos dirigidos a permitir, modificar o denegar el acceso de los interesados a un servicio o un contrato (Ej. Se realiza un proyecto para desarrollar un algoritmo que evalúe a los estudiantes con la información que tiene la universidad al efecto de determinar si se les concede una ayuda)

Cuantos más aspectos de los anteriores estén presentes en un tratamiento, más probable será que se presente un alto riesgo y, por lo tanto, que se requiera realizar una EIPD. En concreto, las autoridades de protección de datos han indicado que **será probablemente necesario realizar un EIPD cuando se presenten como mínimo 2 de los aspectos anteriores**. Si bien no se descarta que, en algunos casos, un responsable del tratamiento pueda considerar que un tratamiento que cumple solo uno de los criterios mencionados requiera una EIPD o bien que, cuando un tratamiento implique dos de los aspectos citados, el responsable del tratamiento considere que el tratamiento no genera un alto riesgo para los derechos y libertades de las personas afectadas y, por lo tanto, no sea necesario llevar a cabo una EIPD. En este caso, será necesario que se documente en detalle las razones por las cuales no ha realizado una EIPD (principio de responsabilidad proactiva) así como la opinión del delegado de protección de datos.

El GT29 ha indicado que la EIPD debe iniciarse tan pronto como sea viable en el diseño del proyecto que requiera el tratamiento de datos personales incluso aunque algunas de las acciones que necesiten tratar datos personales no estén totalmente definidas aún. Además, no descarta que sea necesario repetir pasos concretos de la EIPD a medida que avance el proceso de desarrollo debido a que la selección de determinadas medidas técnicas u organizativas puede afectar al impacto o probabilidad de los riesgos que suponga el tratamiento. Por lo tanto, se debe tener presente que la realización de una EIPD no es una medida estática, sino que es un proceso continuo a lo largo del ciclo de vida del tratamiento y, por lo tanto, también del proyecto de investigación.

Respecto la metodología a utilizar para realizar una EIPD, el RGPD no establece ninguna concreta sino que deja libertad al responsable del tratamiento en su elección. Se pueden consultar las siguientes guías:

- Guía sobre la gestión del riesgo y evaluación de impacto en tratamientos de datos personales de la AEPD
- Guía práctica sobre la evaluación de impacto relativa a la protección de datos en el RGPD de la APDCAT
- Aplicación para las evaluaciones de impacto relativas a la protección de datos de la APDCAT

- Metodología de evaluación del impacto relativa a la protección de datos en salud elaborada por la Fundació TIC Salut Social y el Observatorio de Bioética y Derecho de la Universitat de Barcelona basada en la guía de la APDCAT
- Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679 del Grupo de Trabajo del Artículo 29 y, posteriormente, avaladas por el Comité Europeo de Protección de Datos
- Metodología y herramienta para realizar evaluaciones de impacto relativas a la protección de datos elaboradas por la Commission Nationale de l'Informatique et des Libertés (CNIL)
- Metodología y plantilla para realizar evaluacones de impacto relativas a la protección de datos elaboradas por el Information Commissioner's Office (ICO)

Como toda obligación de la normativa de protección de datos personales, debe ser cumplida por el responsable del tratamiento y no por el delegado de protección de datos de acuerdo con los artículos 24 y 39 del RGPD. En relación con la EIPD, al delegado de protección de datos le corresponde supervisar el cumplimiento de esta obligación y asesorar en aquellas cuestiones que se le requiera (por ejemplo, sobre si es necesaria la realización de una EIPD, sobre la metodología a seguir, sobre las medidas y garantías a implementar para mitigar los riesgos, y sobre el resultado de la EIPD). Asimismo, también se debería pedir asesoramiento al responsable de seguridad en relación con las cuestiones que se planteen en materia de seguridad de la información.

En todo caso, se debería documentar las intervenciones del delegado de protección de datos y del responsable de seguridad y las decisiones tomadas a partir de ellas de acuerdo con el principio de responsabilidad proactiva.

Finalmente, se debe tener en cuenta que el artículo 35.10 del RGPD establece que, cuando ello proceda, el responsable del tratamiento debe obtener la opinión de las personas interesadas en relación con el tratamiento de datos personales objeto de la EIPD. El GT29 ha indicado que, en todo caso, se debe documentar el motivo en base al cual se considera que no corresponde obtener dicha opinión, por ejemplo, porque tiene un coste desproporcionado, porque es impracticable o porque pondría en riesgo la confidencialidad o los resultados del proyecto de investigación. Asimismo, también ha dicho que su opinión se puede obtener mediante encuestas o mediante consulta a los representantes de los interesados si existen.

5. Medidas de seguridad técnicas y organizativas

En el Reglamento General de Protección de Datos no se establecen unas medidas concretas de seguridad a aplicar a los tratamientos de datos. Únicamente se indica que son los responsables y encargados del tratamiento los que deben valorar las medidas a aplicar atendiendo a los tipos de tratamientos realizados, los riesgos existentes, el estado de la técnica, el contexto y los costes.

La Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales establece que las Universidades públicas deberán aplicar a los tratamientos de datos personales las medidas de seguridad

que correspondan de las previstas en el Esquema Nacional de Seguridad.

Además, se deberán cumplir las normativas específicas propias de la Universidad (Política de Seguridad, Protocolo de Gestión de incidentes, y otras normas de seguridad de la información aprobadas por cada Institución).

En el caso de que sea necesario realizar una evaluación de impacto relativa a la protección de datos personales (EIPD), habrá que tener en cuenta las medidas que en dicha evaluación se determinen necesarias implementar para reducir el riesgo que el tratamiento puede ocasionar a las personas titulares de los datos personales.

Preferentemente se deberían utilizar las infraestructuras y programas contratados a nivel institucional por las universidades para reducir los riesgos que comporte el tratamiento de datos personales. En caso de que se necesite utilizar otras infraestructuras o programas se debería contactar con el Delegado de Protección de Datos y el Responsable de Seguridad para garantizar el cumplimiento de la normativa.

5.1. ¿En qué consiste la anonimización de los datos personales?

La finalidad del proceso de anonimización es eliminar o reducir al mínimo los riesgos de reidentificación de los datos anonimizados manteniendo la veracidad de los resultados del tratamiento de los mismos, es decir, además de evitar la identificación de las personas, los datos anonimizados deben garantizar que cualquier operación o tratamiento que pueda ser realizado con posterioridad a la anonimización no conlleva una distorsión de los datos reales.

En el diseño del proceso de anonimización será necesario prever las consecuencias de una eventual reidentificación de las personas que pudiera generar un perjuicio o merma de sus derechos. Igualmente será necesario prever una hipotética pérdida de información por negligencia del personal implicado, por falta de una política de anonimización adecuada o por una revelación de secreto intencionada que diera lugar a la pérdida de las variables de identificación o claves de identificación de las personas.

Para un adecuado diseño del proceso de anonimización se puede consultar la Guía con orientaciones publicada por la AEPD (https://www.aepd.es/es/documento/guia-orientaciones-procedimientos-anonimizacion.pdf) y el Dictamen 05/2014 sobre técnicas de anonimización del Grupo de Trabajo del Artículo 29 (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_es.pdf).

5.2. ¿En qué consiste la seudonimización de los datos personales?

La seudonimización se encuentra definida en el artículo 4.5) del Reglamento, como la información que, sin incluir los datos denominativos de un sujeto afectado permiten, a través de la asociación con información adicional, determinar quién es el individuo que está detrás de los datos seudonimizados.

Por tanto, se puede considerar la seudonimización como una barrera técnica u organizativa para gestionar el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas destinadas a garantizar que los datos personales no se atribuyan a una persona física

identificada o identificable.

El fundamento es reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos.

Significa que han de asignarse roles y accesos a la información claramente definidos entre aquellas personas que asignan seudónimos a los participantes (rol técnico) y aquellas que, al usar los datos seudonimizados, no han de acceder a los datos identificativos del sujeto participante (rol investigador). También habría que definir si el rol técnico mantiene la base de datos que une seudónimo con identidad (archivo con los datos personales) o esto lo mantiene un tercer rol (rol gestor).

Sería deseable que todos los proyectos contasen con un plan de tratamiento de datos seudonimizados en el que se explicitasen:

- Quién recoge los datos y asigna los seudónimos (rol técnico)
- Quién custodia la base de datos que permite la reidentificación de seudónimos (rol gestor)
- Quién realiza la investigación con los datos seudonimizados (rol investigador)

Esta asignación de roles debe ser interpretada teniendo en cuenta que en una investigación puede haber diferentes funciones y tareas asumidas por cada uno de los participantes. En el caso en que una o varias personas tuviesen simultáneamente varios roles, habría que explicar claramente el motivo de forma justificada y explicar cómo se mantienen las garantías relativas a la identificabilidad de los sujetos.

5.3. ¿Qué medidas de seguridad específicas se pueden adoptar para evitar la reidentificación y el acceso de terceros no autorizados a los datos?

De forma enumerativa (no exhaustiva), se pueden adoptar algunas de las siguientes medidas:

- Separación de roles.
- Acceso al archivo con los datos personales solo mediante clave y con registro de accesos solo por parte de los roles previamente autorizados.
- Localización del archivo con los datos personales en lugares seguros establecidos por las instituciones.
- Asignación de seudónimos no derivados de datos identificativos (nombre, DNI, lugar de tratamiento, nº de historia clínica, etc.).

5.4. ¿Cómo se puede proteger la información en formato digital (en la nube, PCs, HD, dispositivos, etc.)?

Cada institución habrá determinado, mediante la Política de Seguridad de la Información, el conjunto de directrices para gestionar y proteger la información que se trata. Desarrollando la misma, se habrán aprobado procedimientos, instrucciones, etc., regulando apartados específicos que se deberá cumplir. Ante cualquier duda en relación a esta documentación de seguridad propia de cada Institución, se recomienda ponerse en contacto con el Delegado de Protección de Datos o el Responsable de Seguridad de la Institución.

Entre las medidas de seguridad que se pueden adoptar, se encuentran las siguientes:

- Control de accesos: los dispositivos deberán contar con sistemas de autenticación que impidan el acceso no autorizado a los mismos. Asimismo, la información será accesible, únicamente, por el personal que la necesite para su trabajo, según los roles o perfiles.
- Uso de contraseñas: las contraseñas deficientes o mal custodiadas pueden favorecer el acceso y el uso no autorizado de los datos. Para reducir el riego se recomienda:
  - Utilizar contraseñas robustas. La forma más segura de obtener una contraseña robusta es utilizar un generador de contraseñas que nos permita elegir, longitud, tipo de caracteres, etc. No obstante, cuanto más complejas sean, mayor será la dificultad para recordarlas. Por ello, lo más recomendable es utilizar un gestor de contraseñas y así solo tener que recordar y conservar la clave maestra, la que abre el gestor. Existe software open-source que puede ser utilizado, por ejemplo, KeePass (https://sourceforge.net/projects/keepass/).
  - No compartir con nadie.
  - No utilizar la misma contraseña para acceder al correo electrónico, aplicaciones institucionales, redes sociales, tiendas online, etc.
  - Siempre que sea posible, habilitar un doble factor de autenticación.
- Bloqueo de sesión: se activará el bloqueo de la pantalla transcurrido un periodo razonable, no superior a 5 minutos.
- Cifrado de la información: de esta manera el fichero será inaccesible a otras personas que no sepan la clave de descifrado. Para el caso de dispositivos portables es especialmente relevante para que solo el propietario de la misma pueda descifrarla y que sea inaccesible por otras personas en caso de pérdida del dispositivo.
- Uso de aplicaciones estandarizadas por la Universidad. Preferentemente se deberían utilizar las infraestructuras y programas contratados a nivel institucional por las universidades. En caso que se necesite utilizar otras infraestructuras o programas se debería contactar con el Delegado de Protección de Datos y el Responsable de Seguridad para garantizar el cumplimiento de la normativa.
- No es recomendable la utilización de dispositivos de almacenamiento locales (discos de equipos de sobremesa, discos USB, …) para almacenamiento de datos personales.
- Para el acceso seguro desde redes públicas a determinados recursos de la intranet será necesario la utilización de un cliente de redes privadas virtuales.
- Publicar sin vincular a motores de búsqueda, por ejemplo, usando los archivos robots.txt.

5.5. ¿Qué medidas de seguridad se deben tomar para proteger la información en soporte papel?

La información en papel está expuesta a mayores riesgos que la información digital ya que esta última puede ser protegida mediante niveles de acceso o por diferentes medios tecnológicos. La información en papel es especialmente vulnerable ante los siguientes riesgos:

- Pérdida o extravío.

- Alteración fraudulenta.
- Destrucción no autorizada.
- Deterioro o daño significativo.
- Divulgación no autorizada.

Por ello, es recomendable, con carácter general, trabajar con datos personales en soporte electrónico, de modo que la utilización del soporte en papel sea residual y limitada a los supuestos estrictamente necesarios.

Entre las medidas de seguridad que se recomienda aplicar a la documentación en soporte papel que contenga datos personales se encuentran las siguientes:

- Para impedir el acceso no autorizado, se recomienda guardar y custordiar bajo llave siempre que no se estén utilizando y tratando. Se deberían evitar malas prácticas como dejar los documentos encima de la mesa; dejar las llaves accesibles, etc.
- Se deberían adoptar medidas para que los documentos impresos no estén accesibles a terceros hasta que son recogidos de la impresora por su propietario, como por ejemplo utilizando código de usuario.
- Se debe evitar la reutilización de documentos con datos personales, por ejemplo, para tomar notas.

5.6. ¿Qué es y cómo actuar ante una brecha de seguridad?

Brecha de seguridad de datos personales son 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.

Algunas de las categorías en las que se pueden clasificar son:

- Brecha de confidencialidad: acceso a la información por quien no está autorizado o tiene un propósito ilegítimo para acceder a ella.
- Brecha de integridad: alteración de la información original y la sustitución de datos puede ser perjudicial para el individuo.
- Brecha de disponibilidad: impide el acceso a los datos originales cuando es necesario. Puede ser temporal (los datos son recuperables, pero tomará un periodo de tiempo y esto puede ser perjudicial para el individuo), o permanente (los datos no pueden recuperarse).

Cuando se observe o sospeche que existe una incidencia o brecha de seguridad se deberá comunicar a la mayor brevedad posible. Se recomienda consultar el procedimiento de gestión de brechas de seguridad aprobado por cada Institución, en el cual se hará referencia al medio de comunicación de la misma y la manera de actuar.

Los casos más comunes de posible violación de datos personales son:

1. Acceso a datos no autorizados:

- Encargo del tratamiento sin el contrato correspondiente.
- Acceso indiscriminado a impresoras, fotocopiadoras, etc.
- Acceso a información confidencial no autorizada
- Acceso no autorizado a los sistemas informáticos.

2. Comunicación no autorizada de datos:

- Transmisión ilícita de datos a un destinatario. Error en la dirección de correo.
- Vulneración del secreto profesional.
- Publicación de imágenes sin autorización del interesado.
- Envío de correos electrónicos masivos sin ocultar los destinatarios (copia oculta).
- Transferencia internacional de datos sin estar sujeta a una decisión de adecuación de la UE o garantías adecuadas de protección de datos.

3. Alteración de datos:

- Modificación de datos malintencionada.
- Falsificación de datos.
- Recuperación ineficaz de copias de respaldo.

4. Pérdida de información:

- Extravío u olvido de soportes (portátil, "pendrive" o disco externo)
- Robo o sustracción de información (portátil, "pendrive" o disco externo)

5. Destrucción de datos:

- No usar destructora de papel o de soportes digitales.

Para más información se puede consultar el documento del Comité Europeo de Protección de Datos denominado "Directrices 1/2021 sobre ejemplos de notificación de violaciones de la seguridad de los datos personales".

6. ¿Qué información se debe facilitar a los participantes en relación con el tratamiento de datos personales?

De acuerdo con el artículo 13 del RGPD y sin perjuicio de la información que se requiera facilitar a los participantes desde una perspectiva ética o por la ley de investigación biomédica en relación con el uso de muestras biológicas, cuando los datos son recogidos directamente de la persona participante en la actividad de investigación, se le debe facilitar la información requerida por dicho artículo en relación con el uso que se dará a sus datos personales, la cual se enumera seguidamente:

a) La identidad y los datos de contacto del responsable o del representante.
b) Los datos de contacto del delegado de protección de datos.
c) Las finalidades del tratamiento de los datos personales.

d) La base jurídica del tratamiento.
e) Cuando el tratamiento se base en el art. 6.1 f) del RGPD, los intereses legítimos del responsable o de un tercero.
f) Los destinatarios o categorías de destinatarios de los datos personales y, en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional.
g) El plazo durante el cual se conservarán los datos personales (si es posible), o los criterios utilizados para determinar ese plazo.
h) El derecho de acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, u oposición al tratamiento, así como el derecho a la portabilidad de los datos.
i) El derecho a retirar el consentimiento en cualquier momento (siempre que el tratamiento esté basado en el art. 6.1.a o 9.2.a del RGPD).
j) El derecho a presentar una reclamación frente a la autoridad de control.
k) Si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir el contrato y si el interesado está obligado a facilitar los datos personales y sus posibles consecuencias si no se facilitan estos datos.
l) La existencia de decisiones automatizadas, incluida la elaboración de perfiles.

En los **anexos** de esta guía se pueden consultar modelos para dar cumplimiento al precepto anterior en función de si se tratarán categorías especiales de datos o si se darán transferencias internacionales de datos.

Es relevante indicar que el artículo 11 de la LOPDyGDD permite que la obligación anterior se pueda cumplir mediante un sistema de dos capas, es decir, facilitando a la persona afectada la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información. La información básica deberá contener, al menos, los siguientes aspectos:

a) La identidad y los datos de contacto del responsable o del representante.
b) Las finalidades del tratamiento de los datos personales.
c) El derecho de acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, u oposición al tratamiento, así como el derecho a la portabilidad de los datos.
d) La existencia de decisiones automatizadas, incluida la elaboración de perfiles, y su derecho a oponerse a la adopción de dichas decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar.

En caso que los datos no se hayan recogido directamente de la persona participante en la actividad de investigación, además de los aspectos anteriores, también se le debe informar del origen de los datos y de las categorías de datos recibidos para dar cumplimiento al artículo 14 del RGPD. En caso de que se decida utilizar el sistema de dos capas indicado, en la información básica también se deberá indicar el origen de los datos y de las categorías de datos recibidos.

En relación con el cumplimento de los artículos 13 y 14 del RGPD se pueden consultar los documentos siguientes:

- Guía para el cumplimiento del deber de informar de la AEPD, APDCAT y AVPD.
- Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679 del Grupo de Trabajo del Artículo 29 y, posteriormente, avaladas por el Comité Europeo de Protección de Datos.

Finalmente, es relevante destacar que la disposición adicional 17ª de la LOPDyGDD en su apartado 2º, letra c), establece una obligación específica en relación con el artículo 13 del RGPD cuando indica que se considerará lícita 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 concreto, dicho precepto establece que en dichos casos el responsable del tratamiento debe publicar la información que requiere el artículo 13 del RGPD 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. Por lo tanto, se deberán adoptar medidas técnicas y organizativas para facilitar dicha información de la manera requerida.

7. ¿Cuándo se debe formalizar un acuerdo de encargado de tratamiento y qué contenido debería tener? ¿Qué acciones se deben adoptar? (Protección de datos por diseño en la contratación de prestaciones de servicios)

Es evidente que, en el ámbito universitario, nos encontraremos con la necesidad de realizar contrataciones de prestación de servicios para el adecuado desarrollo y cumplimiento de las funciones y competencias asignadas a las Universidades. Estas prestaciones de servicios por parte de colaboradores externos, tiene repercusión en el ámbito de la protección de datos personales, pues puede implicar que dichos colaboradores traten datos personales con respecto a los cuales, la Universidad es responsable frente a los titulares o interesados. En estos casos es necesario que terceros ajenos a nuestra entidad traten datos personales por nuestra cuenta, y bajo nuestras instrucciones, ya sea por necesidades de los servicios o unidades, de gestión, de docencia, o relativas a la investigación para el cumplimiento de las finalidades que tiene atribuida nuestra Universidad.

Se habla así, de un encargado del tratamiento (colaborador externo prestador del servicio) y de responsable del tratamiento (Universidad), cuya relación jurídica (Universidad y colaborador externo prestador de un servicio), en lo referido al tratamiento de datos personales a realizar, debe instrumentarse necesariamente y por imperativo legal mediante un contrato. Surge así la necesidad de suscribir el CONTRATO DE ENCARGADO DE TRATAMIENTO DE DATOS PERSONALES. En este mismo sentido se expresa la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP) en su Disposición adicional vigésima quinta.

Por tanto, si el contrato implica el tratamiento de datos de carácter personal se deberá respetar en su integridad el RGPD (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, y la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de datos Personales y Garantía de Derechos Digitales (LOPDyGDD).

Ejemplos:

1) Contratación con una empresa que se encarga de destruir papel.
2) Contratación de un software a una empresa que se encargue del mantenimiento/análisis, tratamiento/consulta, etc., y por tanto tendrá acceso a datos. Supuesto muy normal en investigaciones.

Para más información se recomienda consultar:

- La Guía Orientativa para la formalización de encargos de tratamiento de datos personales en el ámbito universitario.
- Directrices 07/2020 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» en el RGPD del Comité Europeo de Protección de Datos

8. Registro del tratamiento de la actividad de investigación

Identificación del procedimiento de cada universidad. Es un paso obligatorio y previo a la realización del tratamiento, ya que se trata de una medida organizativa que reduce el riesgo en el tratamiento de los datos.

Según establece la normativa de protección de datos, los datos personales deben tratarse de conformidad con una serie de principios básicos y garantías que tienen como finalidad limitar el impacto negativo que pudiera tener el tratamiento en los derechos de las personas, y garantizar la equidad, transparencia y responsabilidad de los tratamientos de datos, la calidad de datos y la confidencialidad.

Dentro de estos principios y garantías hacemos referencia en este apartado a la obligación de la identificación del tratamiento, y su inscripción en el Registro de Actividades de Tratamiento de la entidad.

De conformidad con las definiciones incluidas en el primer apartado de esta guía, es evidente que en las Universidades se van a realizar actividades de investigación que implicarán un tratamiento de datos personales, independientemente del método utilizado para ello (por ejemplo, entrevistas, cuestionarios, recuperación directa en línea, diseño de aplicaciones etc.).

Por ello será necesario que el responsable del tratamiento de datos personales que se vaya a realizar (Investigador, profesor etc.), como consecuencia de la actividad investigadora, defina las actividades de tratamiento incluyendo toda la información que se requiere en la normativa, paso fundamental que requiere tener claro cuáles son las finalidades y legitimación del tratamiento de datos personales. Todo ello se realizará con el apoyo del DPD de su institución.

Se deberá por tanto analizar la actividad a realizar e identificar la siguiente información:

1. Actividad de Tratamiento de datos personales.
2. Finalidad de la actividad.
3. Legitimación.
4. Objeto del tratamiento.
5. Categoría de datos personales objeto de tratamiento (en su caso).
6. Procedencia de los datos personales.
7. Interesados cuyos datos personales van a ser objeto de tratamiento.
8. Plazo de conservación de los datos.
9. Cesiones de datos o transferencias Internacionales.
10. Medidas de seguridad.
11. Identificación de encargados de tratamiento (en su caso).

Se recomienda consultar al delegado de protección de datos la necesidad de incluir l**os tratamientos así identificados** en el Registro de actividades de tratamiento de la Universidad.

9. ¿Cuándo se debe formalizar un acuerdo de corresponsabilidad del tratamiento y qué contenido debería tener?

En actividades de investigación, como p.e. los Proyectos de Investigación, es muy frecuente la colaboración entre distintas Universidades, o entre Universidades y otras entidades.

En este sentido, tal como nos indica el art. 26 del RGPD, **si ambas instituciones determinan conjuntamente los objetivos y medios del tratamiento de datos** que se va a realizar en la actividad investigadora, estamos ante un supuesto de **Corresponsabilidad en el tratamiento**.

Con la finalidad del cumplimiento de los principios básicos y garantías para la protección de los datos personales y limitar el impacto negativo que pudiera tener el tratamiento en los derechos de las personas, y para garantizar la equidad, transparencia y responsabilidad de los tratamientos de datos, la calidad de datos y la confidencialidad, se establece la necesidad en estos casos de establecer un acuerdo entre corresponsables, que se recomienda que tenga el siguiente contenido mínimo:

- Identificación de las partes.
- Obligación y compromiso de cumplimiento normativo.
- Finalidad y objeto del tratamiento de datos personales.
- Datos objeto de tratamiento.
- Interesados cuyos datos sean objeto de tratamiento.
- Responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por la normativa:
    - Establecer qué parte recoge los datos.
    - Cómo se hace efectivo el derecho a la información (art. 12 y ss RGPD)
    - Establecimiento de un punto de contacto.

  - Procedimiento de ejercicio de derecho.
  - Medidas de seguridad a establecer.
  - Procedimientos de brecha de seguridad.
  - Régimen de posibles acuerdos a adoptar (p.e. contratación de encargado por alguna de las partes, uso de datos para otra finalidad…)
  - Establecimiento del procedimiento para acordar la realización de transferencias internacionales
  - Realización o no de una evaluación de impacto relativa a la protección de datos personales.
- Régimen de responsabilidades de las partes.

Para más información, se recomienda consultar las Directrices 07/2020 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» en el RGPD del Comité Europeo de Protección de Datos.tratamiento» y «encargado del tratamiento» en el RGPD del Comité Europeo de Protección de Datos.

10. ¿Cuándo se considera que participan menores en la actividad de investigación?

En relación con el tratamiento de datos personales, el art. 8 del RGPD prevé que los Estados miembros puedan reducir el límite de edad en que los menores pueden consentir el tratamiento de datos personales en el marco de la oferta de servicios de la sociedad de la información hasta los 13 años. Si se examina la LOPDyGDD se puede comprobar que su art. 7.1 ha establecido los 14 años como la edad mínima a partir de la cual los menores pueden consentir cualquier tratamiento de sus datos personales siempre que no haya otra norma específica que exija la asistencia de los titulares de la patria potestad o tutela.

Respecto dicha excepción, el dictamen CNS 41/2020 de la APDCAT dice que a la investigación científica en salud le son de aplicación las previsiones de la normativa relativa a la autonomía del paciente y, por lo tanto, el consentimiento otorgado por un menor será válido salvo que no sea competente, ni intelectual, ni emocionalmente, para comprender el alcance de la intervención sobre su salud y que, en estos casos, será necesario que el consentimiento sea otorgado por su representante, excepto que sean menores emancipados o mayores de dieciséis años y no implique un grave riesgo para la vida o salud del menor. Se debe tener en cuenta que, según la APDCAT, la mención a los mayores de dieciséis años se trata de una simple presunción que hace el legislador en relación con la competencia de los menores para comprender el alcance de la intervención y, por lo tanto, aunque los menores tengan dieciséis años le sigue correspondiendo al responsable del tratamiento demostrar que disponían de la suficiente comprensión en el momento de consentir el tratamiento de datos personales. En caso contrario, para que el tratamiento de sus datos sea lícito, el responsable deberá requerir el consentimiento de los titulares de la patria potestad o tutores, habiendo escuchado previamente la opinión del menor.

Finalmente, y en cuanto al uso de muestras biológicas con fines de investigación biomédica, el artículo 4.2 de la Ley 14/2007, de 3 de julio, de investigación biomédica requiere que la persona participante

tenga como mínimo dieciocho años para consentir dicho uso.

Sobre la obtención del consentimiento para el tratamiento de datos personales de menores de edad de acuerdo con lo anterior, se recomiendan las Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679 del Comité Europeo de Protección de Datos.

11. Tratamientos de datos que consistan en captaciones de voz y/ o imagen

Las captaciones de voz y/o imagen (fotografías y grabaciones de voz y/o imagen) constituyen tratamientos de datos personales que han de atender a las mismas pautas que los restantes tratamientos de datos. No obstante, por sus especiales características, es importante tener en cuenta los siguientes puntos:

- Al igual que en la solicitud de datos en formularios, encuestas o entrevistas por escrito, al realizar grabaciones o fotografías hay que facilitar la información preceptiva relativa al tratamiento de datos personales (punto 6 de este documento), y asimismo solicitar el consentimiento de la persona titular de los datos cuando esa es la base que legitima su tratamiento. Debe guardarse constancia de la prestación del consentimiento (art. 7.1 RGPD) y de que se ha facilitado la información preceptiva en materia de protección de datos (art. 13 RGPD). Cuando se solicita el consentimiento para realizar las grabaciones, este hecho puede constar directamente al inicio de la propia grabación. Habrá supuestos, no obstante, en los que el tratamiento de datos no se fundamenta en el consentimiento, sino en el interés público (v.gr. grabaciones con base en el art. 18 de la Ley 40/2015, de régimen jurídico del sector público, o en el art. 8 de la LO 1/1982 de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen). No obstante, también debe garantizarse que la persona afectada ha recibido la información preceptiva en materia de protección de datos. En este punto, para que quede constancia de la concreta información facilitada, sería preferible emplear documentos escritos (en papel o electrónicos) o formularios en línea; si no es viable, podría ofrecerse esta información al inicio de la grabación, oralmente o a través del chat, e incluso facilitando enlaces a la política de protección de datos del responsable del tratamiento.
- Los destinos de las grabaciones pueden ser muy diversos: por ejemplo, obtener información para un trabajo de investigación, que no implica la difusión de la grabación; o por el contrario, publicar la propia grabación (v.gr. en redes sociales, o en un entregable del propio proyecto). Es importante clarificar cuál es la finalidad y el uso previsto para las grabaciones; además, en el caso en que las finalidades sean diferentes (por ejemplo, para la ejecución del proyecto y, posteriormente, para difundir la grabación en congresos), deben distinguirse adecuadamente para presentar cada una de ellas de forma individual, para que la persona afectada pueda prestar su consentimiento para todos los fines previstos o solo para alguno/s. Asimismo, debe recordarse la regulación especial de determinados tipos de grabaciones: por ejemplo, las realizadas con fines

de videovigilancia (art. 22 LOPDyGDD). (Vid. Guía de la AEPD para el uso de videocámaras con fines de seguridad y otras finalidades).

- Al tratarse de materiales de vídeo o audio, hay que aplicar medidas de seguridad especialmente adecuadas para este tipo de soportes. Así, por ejemplo, en el caso de que se empleen para obtener información (v.gr. grabación de entrevistas), debería restringirse su acceso al mínimo número de personas posible, o podrían ser destruidas en el caso de que se hiciera una transcripción de la información necesaria.

12. ¿Cómo se deben publicar los datos de conformidad a la Ley de Transparencia?

De conformidad con la Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno, con respecto a la publicidad activa de la información, los datos serán publicados según los artículos 5 y siguientes de la misma en los que se establecen los principios básicos para llevarlos a cabo y que serán los cimientos para una correcta protección y transparencia de los mismos. A efectos ejemplificativos, los datos que con carácter general serán objeto de publicidad de conformidad a la Ley de Transparencia:

- Producción y divulgación científica; proyectos de investigación
- Grupos de investigación: catálogo, número de miembros y colaboradores, proyectos asociados, fuentes de financiación
- Proyectos nacionales, europeos e internacionales
- Centros y servicios de investigación (institutos, laboratorios, etc.)
- Principales resultados relacionados con la actividad investigadora: sexenios, tesis defendidas, ponencias, comunicaciones, índices de impacto, “ranking” de investigadores, presencia de la Universidad en los “ranking” de calidad científica, en redes sociales, etc.
- Principales resultados relacionados con la transferencia de los resultados de investigación: publicaciones, patentes solicitadas y concedidas, creación de empresas de base tecnológica
- Plan propio de investigación: programas de I+D+i, ayudas para la realización de tesis doctorales, bolsas de viaje, organización de congresos y conferencias
- Datos agregados sobre recursos humanos: personal investigador en formación, contratos con cargo a proyectos, otros contratos, etc.
- Internacionalización: proyectos compartidos, indicadores de movilidad internacional en centros de investigación, financiación obtenida
- Estancias del personal investigador en centros de investigación nacionales e internacionales.
- Cátedras institucionales y de empresa
- Comisiones I + D + i (comités de ética, normas, etc.)
- Memorias de investigación
- Evolución del número de doctores participantes en contratos y convenios
- Actuaciones en infraestructuras científico-tecnológicas
- Resultados obtenidos por los grupos de investigación de la Universidad en evaluaciones efectuadas por la Agencia Estatal de Investigación (AEI), por otras instituciones, organizaciones o la propia Universidad

- Ayudas, premios, incentivos y reconocimientos a la excelencia académica, investigadora y docente que se otorgan en la Universidad
- Tesis doctorales (datos de referencia, índices de impacto, etc.)

Con carácter general, la publicidad de la información se deberá realizar previa disociación de los datos de carácter personal salvo en los supuestos concretos y específicos en los que la Ley de Transparencia prevea otra cosa. De conformidad a la Ley de Transparencia y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, las Universidades deberán disponer de un Registro de Actividades de Tratamiento (RAT) en el que publicarán el inventario de actividades de tratamiento en aplicación del artículo 31 de la citada Ley Orgánica. De esta forma, será necesaria la colaboración del personal investigador junto con el Comité de Ética para la definición de la concreta actividad de tratamiento que corresponda, tal cual se ha explicitado en esta guía.

Por último, la información será publicada en las correspondientes sedes electrónicas o páginas web y de una manera clara, estructurada y entendible para los interesados y, preferiblemente, en formatos reutilizables. Toda la información será comprensible, de fácil acceso y gratuito y estará a disposición de las personas con discapacidad en una modalidad suministrada por medios o en formatos adecuados de manera que resulten accesibles y comprensibles, conforme al principio de accesibilidad universal y diseño para todos.

13. ¿Cómo se deben reutilizar los datos?

En cuanto a la reutilización de datos, el análisis de la normativa europea de protección de datos (Reglamento General de Protección de Datos), de la Directiva 2019/1024, sobre datos abiertos y la reutilización de la información del sector público y del Reglamento UE 2022/868 de Gobernanza de Datos, podemos estimar que la reutilización consiste en el uso, por personas físicas o jurídicas, de información generada por organismos públicos, con fines comerciales o no. La reutilización puede concebirse como copia, modificación, extracción de datos.

Con respecto a los datos de investigación, debemos ser conscientes de que las Universidades deben adoptar medidas para apoyar que los datos de investigaciones financiadas públicamente sean plenamente reutilizables, interoperables y de acceso abierto, teniendo en cuenta las limitaciones que pudieran derivarse de los derechos de propiedad intelectual e industrial, la protección de datos personales y la confidencialidad, la seguridad y los intereses comerciales legítimos.

De esta manera, las actividades de transferencia de conocimiento y los datos de investigación serán reutilizables para fines comerciales o no comerciales cuando sean financiados con fondos públicos y cuando los investigadores, las universidades o las organizaciones que realizan actividades de investigación o que financien la investigación ya hubieran puesto tales datos a disposición del público a través de un repositorio institucional o temático y, en todo caso, con pleno respeto a la normativa vigente en materia de propiedad intelectual y de protección de datos de carácter personal, y por tanto, teniendo en cuenta la adecuada anonimización o en su defecto la seudonimización de los datos de investigación para su difusión. Finalmente, también debe considerarse que la información se publicará en las sedes

electrónicas o páginas web y de forma clara, estructurada y entendible para los interesados y en formatos reutilizables.

14. ¿Cómo se deben suprimir los datos?

La forma de suprimir los datos dependerá del formato y de los contratos que la universidad tenga suscritos con empresas que ofrezcan servicios de destrucción. Si se dispone de esos servicios y están disponibles para el investigador deberán ser utilizados. En el caso de que no existan o no estén disponibles para el investigador, se podrán usar recursos propios que los sustituyan.

- En el caso de documentación en soporte papel que contenga datos personales se utilizarán los servicios de destrucción contratados por la Universidad o mediante la utilización de destructoras de papel.
- En el caso de formato CD, DVD y similar, se destruirá físicamente el soporte.
- En el caso de discos duros, pendrives y formatos digitales similares, se debería usar un software de borrado seguro de información siguiendo las indicaciones facilitadas por la Área TIC de la Universidad. En caso de que no exista ninguna herramienta proporcionada por la universidad, existe software *open source* que puede utilizarse, como, por ejemplo: (https://sourceforge.net/projects/eraser/).

15. ¿Qué se debe hacer si se produce una modificación sustancial del tratamiento en la actividad de investigación?

Si se produce un cambio sustancial del tratamiento de datos en la actividad de investigación, la persona afectada tendría que ser informada de estas nuevas cuestiones relativas al tratamiento de sus datos personales.

No obstante, lo cierto es que esta situación puede resultar bastante problemática en el ámbito de una investigación: en primer lugar, porque según se va avanzando en una investigación, es frecuente que surjan nuevas necesidades que impliquen nuevos tratamientos de datos; y en segundo lugar, porque puede resultar muy complicado informar de nuevo a todas las personas titulares de los datos. Por consiguiente, como medida de prevención ante estas posibles situaciones, se recomienda:

- En el momento de informar a las personas titulares de los datos, describir las finalidades previstas de forma precisa pero con suficiente amplitud, de tal modo que se pueda abarcar diversos tratamientos de datos dentro de un específico sector de la investigación científica (Considerando 33 RGPD) (Vid. EDPS 2020, A preliminary opinion on data protection and scientific research; y EDPB 2021, Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research).
- Diseñar una estrategia sencilla que permita un contacto posterior con las personas participantes en la investigación, para el caso de que sea necesario volver a contactar con ellas para informar sobre cambios sustanciales en el tratamiento de los datos. Es posible, incluso, diseñar el

desarrollo de proyecto de tal modo que se establezcan posibles contactos periódicos con las personas participantes en el trabajo de investigación.

- Debe hacerse de nuevo especial hincapié en la necesidad de establecer garantías de seguridad especialmente reforzadas para tratar y salvaguardar estas actividades de tratamiento de datos personales.

Anexo

Modelo 1: proyectos de investigación que no tratan categorías especiales de datos ni realizan transferencias internacionales de datos

¿Cómo se tratarán mis datos personales?

La [*denominación del responsable del tratamiento*] es, en relación con el cumplimiento de la normativa de protección de datos personales, la responsable legal del tratamiento de estos datos personales en el marco del proyecto. Ello no implica que tenga acceso *[ejemplo: a tu identidad, a las grabaciones o notas o al formulario de consentimiento informado]*, excepto por obligación legal (por ejemplo, si alguien presenta una reclamación ante la autoridad de control de protección de datos o ante un juez o tribunal).

De acuerdo con el Reglamento general de protección de datos personales de la Unión Europea, te informamos que los datos de contacto de la [*denominación del responsable del tratamiento*] son [*dirección postal del responsable del tratamiento*] y [*dirección de correo electrónico del responsable del tratamiento*], por si en algún momento deseas ejercer los derechos que te reconoce la normativa de protección de datos personales (puedes acceder a tus datos y solicitar su rectificación, supresión, oposición, portabilidad o limitación). En tal caso, deberás adjuntar una fotocopia del DNI o de otro documento válido que te identifique.

Los datos personales que se recojan únicamente se utilizarán con la finalidad de gestionar y ejecutar el proyecto de investigación [*denominación del proyecto de* investigación], en cumplimiento de una misión realizada en interés público (Ley Orgánica 6/2001, de 21 de diciembre, de Universidades). Los destinatarios de los datos personales son la propia universidad y, en concreto, el equipo de investigación del proyecto y, si los hay, los encargados del tratamiento de datos. No se considera ninguna cesión de datos a terceros, a menos que sea por obligación legal. Los datos personales se conservarán hasta que se hayan alcanzado los objetivos del proyecto y se hayan podido publicar los resultados (aproximadamente, hasta [*plazo de conservación de los datos – puede venir determinado por la convocatoria o el acuerdo de subvención*] años desde la finalización del proyecto).

Si consideras que tus derechos no han sido adecuadamente atendidos, puedes comunicarlo al delegado de protección de datos de la [*denominación del responsable del* tratamiento] por correo postal ([*dirección postal del delegado de protección de datos*]) o por correo electrónico ([*dirección de correo electrónico del delegado de protección de datos*]). También puedes presentar una reclamación ante la [*denominación de la autoridad de control competente*].

Modelo 2: proyectos de investigación que no tratan categorías especiales de datos y que realizan transferencias internacionales de datos

¿Cómo se tratarán mis datos personales?

La [*denominación del responsable del tratamiento*] es, en relación con el cumplimiento de la normativa de protección de datos personales, la responsable legal del tratamiento de estos datos personales en el marco del proyecto. Ello no implica que tenga acceso *[ejemplo: a tu identidad, a las grabaciones o notas*

o al formulario de consentimiento informado], excepto por obligación legal (por ejemplo, si alguien presenta una reclamación ante la autoridad de control de protección de datos o ante un juez o tribunal).

De acuerdo con el Reglamento general de protección de datos personales de la Unión Europea, te informamos que los datos de contacto de la [*denominación del responsable del tratamiento*] son [*dirección postal del responsable del tratamiento*] y [*dirección de correo electrónico del responsable del tratamiento*], por si en algún momento deseas ejercer los derechos que te reconoce la normativa de protección de datos personales (puedes acceder a tus datos y solicitar su rectificación, supresión, oposición, portabilidad o limitación). En tal caso, deberás adjuntar una fotocopia del DNI o de otro documento válido que te identifique.

Los datos personales que se recojan únicamente se utilizarán con la finalidad de gestionar y ejecutar el proyecto de investigación [*denominación del proyecto de* investigación], en cumplimiento de una misión realizada en interés público (Ley Orgánica 6/2001, de 21 de diciembre, de Universidades). Los destinatarios de los datos personales son la propia universidad y, en concreto, el equipo de investigación del proyecto. Asimismo, se ha contratado a la entidad [*denominación social de la entidad prestadora del servicio contratado*] ubicada en [*ubicación de la entidad contratada*] para que, como encargada del tratamiento de los datos, realice [*descripción de la actividad contratada que requerirá el tratamiento de datos personales*]. Esta transferencia internacional se realiza al amparo de [*Opción 1: la Decisión de adecuación -se debe indicar la denominación de la decisión de adecuación-][Opción 2: las cláusulas contractuales tipo aprobadas por la Comisión Europea*]. Los datos personales se conservarán hasta que se hayan alcanzado los objetivos del proyecto y se hayan podido publicar los resultados (aproximadamente, hasta [*plazo de conservación de los datos – puede venir determinado por la convocatoria o el acuerdo de subvención*] años desde la finalización del proyecto).

Si consideras que tus derechos no han sido adecuadamente atendidos, puedes comunicarlo al delegado de protección de datos de la [*denominación del responsable del* tratamiento] por correo postal ([*dirección postal del delegado de protección de datos*]) o por correo electrónico ([*dirección de correo electrónico del delegado de protección de datos*]). También puedes presentar una reclamación ante la [*denominación de la autoridad de control competente*].

Modelo 3: proyectos de investigación que tratan categorías especiales de datos y no realizan transferencias internacionales de datos

¿Cómo se tratarán mis datos personales?

La [*denominación del responsable del tratamiento*] es, en relación con el cumplimiento de la normativa de protección de datos personales, la responsable legal del tratamiento de estos datos personales en el marco del proyecto. Ello no implica que tenga acceso *[ejemplo: a tu identidad, a las grabaciones o notas o al formulario de consentimiento informado]*, excepto por obligación legal (por ejemplo, si alguien presenta una reclamación ante la autoridad de control de protección de datos o ante un juez o tribunal).

De acuerdo con el Reglamento general de protección de datos personales de la Unión Europea, te informamos que los datos de contacto de la [*denominación del responsable del tratamiento*] son [*dirección postal del responsable del tratamiento*] y [*dirección de correo electrónico del responsable del*

tratamiento], por si en algún momento deseas ejercer los derechos que te reconoce la normativa de protección de datos personales (puedes acceder a tus datos y solicitar su rectificación, supresión, oposición, portabilidad o limitación). En tal caso, deberás adjuntar una fotocopia del DNI o de otro documento válido que te identifique.

Los datos personales que se recojan únicamente se utilizarán con la finalidad de gestionar y ejecutar el proyecto de investigación [*denominación del proyecto de* investigación] conforme a tu consentimiento, el cual puedes revocar en cualquier momento sin que tenga efectos retroactivos. Los destinatarios de los datos personales son la propia universidad y, en concreto, el equipo de investigación del proyecto y, si los hay, los encargados del tratamiento de datos. No se considera ninguna cesión de datos a terceros, a menos que sea por obligación legal. Los datos personales se conservarán hasta que se hayan alcanzado los objetivos del proyecto y se hayan podido publicar los resultados (aproximadamente, hasta [*plazo de conservación de los datos – puede venir determinado por la convocatoria o el acuerdo de subvención*] años desde la finalización del proyecto).

Si consideras que tus derechos no han sido adecuadamente atendidos, puedes comunicarlo al delegado de protección de datos de la [*denominación del responsable del* tratamiento] por correo postal ([*dirección postal del delegado de protección de datos*]) o por correo electrónico ([*dirección de correo electrónico del delegado de protección de datos*]). También puedes presentar una reclamación ante la [*denominación de la autoridad de control competente*].

Modelo 4: proyectos de investigación que tratan categorías especiales de datos y realizan transferencias internacionales de datos

¿Cómo se tratarán mis datos personales?

La [*denominación del responsable del tratamiento*] es, en relación con el cumplimiento de la normativa de protección de datos personales, la responsable legal del tratamiento de estos datos personales en el marco del proyecto. Ello no implica que tenga acceso *[ejemplo: a tu identidad, a las grabaciones o notas o al formulario de consentimiento informado]*, excepto por obligación legal (por ejemplo, si alguien presenta una reclamación ante la autoridad de control de protección de datos o ante un juez o tribunal).

De acuerdo con el Reglamento general de protección de datos personales de la Unión Europea, te informamos que los datos de contacto de la [*denominación del responsable del tratamiento*] son [*dirección postal del responsable del tratamiento*] y [*dirección de correo electrónico del responsable del tratamiento*], por si en algún momento deseas ejercer los derechos que te reconoce la normativa de protección de datos personales (puedes acceder a tus datos y solicitar su rectificación, supresión, oposición, portabilidad o limitación). En tal caso, deberás adjuntar una fotocopia del DNI o de otro documento válido que te identifique.

Los datos personales que se recojan únicamente se utilizarán con la finalidad de gestionar y ejecutar el proyecto de investigación [*denominación del proyecto de* investigación] conforme a tu consentimiento, el cual puedes revocar en cualquier momento sin que tenga efectos retroactivos. Los destinatarios de los datos personales son la propia universidad y, en concreto, el equipo de investigación del proyecto. Asimismo, se ha contratado a la entidad [*denominación social de la entidad prestadora del servicio*

contratado] ubicada en [*ubicación de la entidad contratada*] para que, como encargada del tratamiento de los datos, realice [*descripción de la actividad contratada que requerirá el tratamiento de datos personales*]. Esta transferencia internacional se realiza al amparo de [*Opción 1: la Decisión de adecuación -se debe indicar la denominación de la decisión de adecuación-][Opción 2: las cláusulas contractuales tipo aprobadas por la Comisión Europea*]. Los datos personales se conservarán hasta que se hayan alcanzado los objetivos del proyecto y se hayan podido publicar los resultados (aproximadamente, hasta [*plazo de conservación de los datos – puede venir determinado por la convocatoria o el acuerdo de subvención*] años desde la finalización del proyecto).

Si consideras que tus derechos no han sido adecuadamente atendidos, puedes comunicarlo al delegado de protección de datos de la [*denominación del responsable del* tratamiento] por correo postal ([*dirección postal del delegado de protección de datos*]) o por correo electrónico ([*dirección de correo electrónico del delegado de protección de datos*]). También puedes presentar una reclamación ante la [*denominación de la autoridad de control competente*].