Crue-Secretarías Generales

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

Guía para Investigadores y gestores de Investigación.

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

AVISO:

Este documento se trata de una guía sobre cómo cumplir la normativa de protección de datos personales en los tratamiento 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.¿Qué es un dato personal?

Dato personal es cualquier información sobre una persona física identificada o 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.

Ejemplos de datos personales: DNI, número de expediente, imagen, voz.

Hay algún tipo de datos personales que se tienen un régimen de protección reforzado por la norma, y su tratamiento requiere la concurrencia de una causa que lo justifique. Estos datos son las categorías especiales de datos siguientes:

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

1.2.¿Qué es un tratamiento?

Tratamiento es cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados.

Algunos ejemplos de tratamiento:

- La recogida (captura de información donde existen datos de carácter personal)
- El registro (inscribir o grabar la información en algún tipo de sistema o dispositivo, automatizado o no automatizado, para su posterior tratamiento)
- La organización (ordenar y estructurar la información para facilitar su tratamiento)
- La conservación (mantener la información durante un determinado periodo de tiempo)
- La adaptación o modificación (alterar o cambiar la información)
- La extracción (obtener la información de un sistema o dispositivo original para su envío o traspaso a otro sistema o dispositivo)
- La consulta (buscar los datos sobre el sistema o dispositivo en el que se encuentra registrada)

- La utilización (usar la información para una finalidad concreta)
- La comunicación por transmisión (enviar los datos a otro destinatario desde su sistema o dispositivo origen a través de medios electrónicos)
- La 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)
- La supresión (eliminar, hacer desaparecer la información en el sistema o dispositivo en el que esté originalmente registrada)
- O la destrucción (inutilizar un soporte físico para evitar el acceso a la información)

1.3.¿Qué son datos anónimos o anonimizados?

Son los que se refieren a aquella información que no guarda relación con una persona física identificada o identificable, o aquellos datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo.

Como regla práctica general no basta suprimir el nombre y los apellidos para hacer una información anónima sino que se deben aplicar técnicas que no permitan volver a vincular los datos anónimos con la identidad de las personas participantes.

1.4.¿Qué son datos seudonimizados?

Los datos seudonimizados son aquellos que se pueden atribuir a una persona física mediante la utilización de 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.

Se trata de una medida de seguridad.

Los datos seudonimizados son datos personales y les resulta de plena aplicación la normativa de protección de datos personales.

1.5.¿Quién es el 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 correspondiente será responsable de dicho tratamiento. Todas las personas implicadas en la investigación, como gestoras del tratamiento de los datos personales, estarán obligadas a cumplir con la normativa de protección de datos y aquellas instrucciones que la Universidad emita sobre esta materia.

1.6.¿Qué es la base de legitimación?

Para poder tratar los datos personales se precisa de, el menos, una las bases de legitimación establecidas en el artículo 6 del RGPD. Esencialmente en las investigaciones científicas son las siguientes:

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

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;

En el caso de las universidades privadas, además pueden basar el tratamiento en la siguiente base de legitimación:

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.

1.7.¿Qué es una cesión o comunicación de datos personales?

Es una operación de tratamiento consistente en la transmisión de datos personales fuera del ámbito de control del responsable del tratamiento. La comunicación de datos debe estar fundamentada en alguna de las bases de legitimación del artículo 6 del RGPD.

1.8.¿Qué es una transferencia internacional de datos?

Las transferencias internacionales de datos (TID) son cualquier 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) u organizaciones internacionales. Para su realización se deberán cumplir con los requisitos establecidos en el Capítulo V del RGPD.

Ejemplos:

- Colaboración con una universidad de Australia.
- Contratación de un servicio prestado des de China.

1.9.¿Quién es el encargado del tratamiento?

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.

Ejemplos: contratar un servicio en la nube, empresa que destruye documentación, empresa que nos proporciona y mantiene un software, organización de congresos, transcripción de grabaciones, fotógrafos, empresa que realiza una encuesta...

En ningún caso son encargados de tratamiento los empleados de la Universidad autorizados a tratar datos personales para cumplir con sus funciones.

1.10. ¿Qué es la corresponsabilidad del tratamiento?

Existe corresponsabilidad en el tratamiento de datos personales cuando dos o más responsables tratan conjuntamente datos, estableciendo también conjuntamente los medios y fines del tratamiento.

La corresponsabilidad es muy frecuente en proyectos de investigación en los que participan varias

universidades, para conseguir la finalidad conjunta de la investigación científica relativa al proyecto.

2. ¿Cuáles son los Principios a seguir en el tratamiento de los datos personales?

Los datos deben tratarse con sujeción a los siguientes principios:

2.1 El principio de licitud. Conforme se ha visto en el apartado 1.6 que precede, debemos disponer siempre de al menos una base de licitud que podrá ser el consentimiento del interesado, la realización de una misión en interés público, o en el caso de universidades privadas un interés legítimo.

2.2 El principio de lealtad y transparencia que supone la necesidad y obligación de informar de manera concisa, inteligible y con un lenguaje claro y sencillo al interesado. Respecto a la transparencia, ver el apartado 4.

2.3 El principio de limitación de la finalidad que supone que los datos han de ser tratados para fines determinados y concretos. De manera excepcional, los datos podrán ser tratados para fines de investigación científica, considerándose en estos supuestos este tratamiento compatible con la finalidad inicial.

2.4 Principio de minimización. 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, limitando a lo necesario el plazo de conservación y su accesibilidad. Además, los datos deben estar accesibles exclusivamente a las personas debidamente autorizadas que deban tratar dichos datos.

En el ámbito de la investigación, como regla general se deben utilizar datos anónimos o anonimizados. En caso de que los objetivos del proyecto no se puedan conseguir con estos tipos de datos, entonces se podrían utilizar datos personales. Llegados a este caso, solo se pueden obtener los datos estrictamente necesarios para conseguir dichos objetivos.

2.5 Principio de limitación del plazo de conservación de modo que no sean tratados por más tiempo que el necesario para los fines del tratamiento.

2.6 Principios de integridad y confidencialidad, adoptando las medidas necesarias para su garantía evitando o minimizando los riesgos de destrucción, pérdida o alteración accidental o ilícita de los datos, o la comunicación o acceso no autorizados a dichos datos.

2.7 Principio de la responsabilidad proactiva. Se deben cumplir las previsiones del RGPD y, además, debemos ser capaces de demostrar que los cumplimos.

2.8 Principio de 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 presente Reglamento y proteger los derechos de los interesados.

2.9 Principio de protección de datos por defecto. 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.

3. ¿Cuándo se debe tener en cuenta la protección de datos personales?

Siempre se debe tener en cuenta en la fase de diseño de toda actividad, incluso en las actividades con fines de investigación científica. Esto no solo permite dar un cumplimiento efectivo a dicha normativa, sino que además evita la necesidad de gastar más recursos económicos, humanos y temporales y abrir fases que ya se consideraban cerradas cuando la protección de datos se tiene en cuenta al final del diseño de la actividad en vez de al principio.

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

De acuerdo con el artículo 13 del RGPD, cuando los datos son recogidos directamente de la persona participante en la actividad de investigación, se le debe facilitar determinada información en relación con el uso que se dará a sus datos personales. En los anexos de la guía de investigación 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.

En caso de 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 cumplimento al artículo 14 del RGPD.

Es recomendable 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.

A las personas participantes se les debe facilitar la información anterior sobre el tratamiento de los datos personales sin perjuicio de aquella otra información que se deba proporcionar desde una perspectiva ética.

5. ¿Cuáles son los derechos en materia de protección de datos personales de la persona participante?

- Derecho de acceso
- Derecho de rectificación
- Derecho de supresión
- Derecho a la limitación
- Derecho a la portabilidad
- Derecho de oposición

5.1. ¿En qué consiste el derecho de acceso?

El derecho de acceso permite a la persona participante conocer:

- Si se están tratando datos personales suyos
- Qué datos son
- Posibilidad de obtener una copia
- Finalidad y base legitimadora
- Si se comunica y comparte información a terceros
- Garantías y medidas de protección

Ejemplo: Una persona que es usuaria de la biblioteca puede pedir que se le faciliten todos los datos personales que tengan sobre ella: cuando empleó los servicios de la biblioteca por primera vez, qué libros ha pedido en préstamo, si le han impuesto sanciones, etc.

5.2. ¿En qué consiste el derecho de rectificación?

El derecho de rectificación permite a la persona participante, cuando sus datos son inexactos, están incompletos o desactualizados instar a que se rectifiquen.

Ejemplo: Una oficina de crédito trata información facilitada por el anterior arrendador de una persona, según la cual ésta todavía le debe 3 meses del alquiler. La persona acaba de ganar un litigio según el cual la reclamación por los 3 meses de alquiler se considera infundada. Pues bien, puede pedir a la oficina de crédito que corrija los datos que posee sobre esta persona, de forma que no lo deje en una situación desventajosa en el futuro.

5.3. ¿En qué consiste el derecho de supresión y el derecho al olvido?

Se tendrá derecho a la supresión de los datos en alguna de las siguientes circunstancias:

- Si los datos se han recabado de manera ilícita.
- Si se retira el consentimiento que justificaba el tratamiento de los datos. Ejemplo: Una persona se inscribe en una red social. Pasado un tiempo, decide dejar de utilizar esta red social y quiere que su perfil desaparezca. Pues bien, puede pedir a la empresa titular de la red social que borre sus datos personales.
- Si los datos ya no son necesarios para la finalidad para la que se recogieron. Ejemplo: si se recogieron para la suscripción a un boletín de noticias que ya no se envía.
- Si existe una norma que obliga a la supresión de los datos. Ejemplo: Imágenes de una cámara de videovigilancia que hay que borrar en el plazo de un mes.

El derecho al olvido es el derecho a solicitar que los datos personales se supriman de las búsquedas en internet.

5.4. ¿En qué consiste el derecho a la limitación del tratamiento?

Este derecho consiste en que el responsable del tratamiento debe conservar los datos, pero no utilizarlos. Se aplica fundamentalmente mientras se dirimen otros derechos.

Ejemplo: Una persona quiere cambiarse de banco e interponer una demanda contra el banco del cual quiere dejar de ser cliente. A fin de garantizar que el banco no suprime sus datos personales que necesitará para la formulación de la demanda, la persona solicita la limitación del tratamiento de sus datos, de forma que el banco los tendrá que conservar sin poderlos emplear para ninguna finalidad no autorizada.

5.5. ¿En qué consiste el derecho a la portabilidad?

Consiste en el derecho a recibir los datos facilitados a una entidad responsable del tratamiento y transmitirlos a otra. También alcanzaría la transmisión de los datos personales directamente a otro responsable de tratamiento, en caso de que así lo pidiera el interesado y fuera técnicamente posible.

Ejemplo: Una persona es cliente de una compañía de telefonía, pero decide cambiarse a otra. Puede pedir a la actual compañía que transfiera sus datos personales a la nueva compañía.

5.6. ¿En qué consiste el derecho de oposición?

Generalmente es un derecho previo a la supresión o limitación de uso. 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.

Ejemplo: Una víctima de violencia de género se puede oponer a que se publique la dirección de su centro de trabajo.

5.7. ¿Quién puede ejercer los anteriores derechos?

Cualquier persona cuyos datos personales son, o han sido, tratados por la Universidad. Deberán ser los titulares de los datos, o bien, su representante legal.

5.8. ¿Es necesario que se presente algún tipo de documentación?

Si existe un formulario de solicitud y no puede firmarse electrónicamente será necesario aportar, y siempre que haya dudas sobre la identificación de la persona interesada, copia del D.N.I. o documento equivalente que acredite la identidad. En caso de que se actúe a través de representación legal deberá aportarse documento acreditativo de la representación. También deberán presentarse los documentos acreditativos de la petición que se formula, si corresponde.

5.9. ¿Tiene algún coste?

El ejercicio de estos derechos tiene carácter gratuito salvo cuando se den algunas circunstancias como

pueden ser: solicitudes manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, en cuyo caso se podrá cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o negarse a actuar respecto de la solicitud.

5.10. ¿En qué plazo hay que responder?

El plazo máximo para responder es de un mes. No obstante, en solicitudes complejas o que impliquen un gran volumen de datos, se podrá prorrogar la respuesta hasta dos meses más.

6. Seguridad de los datos personales

6.1. ¿Qué medidas de seguridad se deben implementar?

Se deben aplicar las medidas de seguridad que resulten necesarias como consecuencia del correspondiente análisis de riesgos realizado.

Además, se deberán cumplir las normativas específicas propias que cada Universidad haya aprobado: política de seguridad, gestión de usuarios, gestión de contraseñas, etc.

Es recomendable consultar cualquier duda al Delegado de Protección de Datos y al Responsable de Seguridad de la Universidad.

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

La anonimización es el proceso de convertir los datos en una forma en la que se eliminan las posibilidades de identificar a una persona. La finalidad es ofrecer mayores garantías para la protección de datos de las personas. Por ejemplo, la supresión del nombre y apellidos de las personas participantes no es suficiente para considerar que los datos han sido anonimizados.

Para un adecuado diseño del proceso de anonimización 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

En caso de publicar datos en repositorios, se recomienda consultar las herramientas de anonimización que proporcionan los propios repositorios.

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

La seudonimización de datos consiste en tratar los datos personales sin los datos identificativos del interesado, pero sin suprimir la vinculación entre los datos que consigan determinar la persona titular de los mismos.

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.

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

- Quién recoge los datos y asigna los seudónimos
- Quién custodia la base de datos que permite la reidentificación de seudónimos
- Quién realiza la investigación con los datos seudonimizados

6.4. ¿Qué diferencia hay entre anonimización y seudonimización?

La anonimización es un procedimiento donde los datos identificativos se disocian totalmente de los datos personales, es algo irreversible.

La seudonimización desvincula los datos identificativos, pero los datos seudonimizados mantienen datos adicionales que pueden reidentificar a los interesados, por tanto, es un procedimiento reversible.

6.5. ¿Se puede adoptar alguna medida para evitar la reidentificación y el acceso de terceros no autorizados a los datos?

Entre otras, se recomiendan 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.).

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

Es importante tener en cuenta la política de seguridad de cada Universidad y los procedimientos en materia de seguridad que cada una de ellas tenga aprobadas. Es muy probable que la información esté disponible en la web institucional. Ante cualquier duda es recomendable consultar con el Responsable de Seguridad o con el Delegado de protección de datos.

Como ejemplos para proteger la información:

- Uso de aplicaciones estandarizadas por la Universidad.
- Control de accesos: los dispositivos deberán contar con sistemas de autenticación que impidan el acceso no autorizado a los mismos.
- Mediante el uso de contraseñas. Se utilizarán contraseñas robustas. Para una gestión adecuada de contraseñas existe software open-source que ayuda a recordarlas, por ejemplo, KeePass (https://sourceforge.net/projects/keepass/). Es recomendable utilizar un multifactor 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: para el caso de dispositivos portables es conveniente cifrar la información para que solo el propietario de la misma pueda descifrarla y que sea inaccesible por otras personas en caso de pérdida del dispositivo.
- No se recomienda 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.
- Publicar datos personales en espacios de acceso restringido.

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

- Se recomienda, 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.
- La documentación en soporte papel que contenga datos personales debe guardarse y custodiarse bajo llave siempre que no se estén utilizando y tratando. Deberán evitarse malas prácticas como dejar los documentos encima de la mesa; dejar las llaves accesibles; reutilizar documentos con datos personales para hacer anotaciones, etc.
- Deberán adoptarse 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.

6.8. ¿Cómo actuar ante una brecha de seguridad?

Cada Universidad habrá aprobado un procedimiento de gestión de brechas de seguridad, en el cual se hará referencia al medio de comunicación de la misma. En caso de duda se debería consultar con el Delegado de Protección de Datos o el Responsable de Seguridad de la Universidad.

7. ¿Cuándo 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 con carácter previo al inicio del tratamiento 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.

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. Las autoridades de control en materia de protección de datos han elaborado una lista de criterios para determinar si un tratamiento puede comportar dicho alto riesgo y, por lo tanto, se deba realizar una EIPD. Se puede consultar dicha

lista en los siguientes enlaces: AEPD, APDCAT, APVD y CTPDA.

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 se debe descartar que sea necesario repetir pasos concretos de la EIPD a medida que avance el proceso de desarrollo del proyecto debido a que la selección de determinadas medidas técnicas u organizativas puede afectar a 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 del proyecto de investigación.

Respecto la metodología a utilizar para realizar una EIPD, el RGPD no establece ninguna concreta, sino que deja libertad en su elección. Se recomienda que se consulte al/la delegado/a de protección de datos para determinarla y para que pueda asesorar sobre otros aspectos que sean relevantes.

8. ¿Cómo se regula la relación entre responsable y encargado?

En estos casos se debe formalizar un acuerdo de encargo de tratamiento, con el contenido que indica el RGPD art. 28, donde se dan instrucciones sobre cómo proceder en el tratamiento de datos, y se establecen las obligaciones del encargado. Se recomienda consultar los modelos que haya podido publicar cada Universidad.

Entre Responsable y Encargado, no existe comunicación de datos, ya que se entiende que el encargado actúa por cuenta del responsable.

9. ¿Qué es el Registro de Actividades de Tratamiento?

En el Registro de Actividades del Tratamiento deben constar todos los tratamientos de datos personales que realiza la universidad. Se recomienda consultar al delegado de protección de datos sobre la necesidad de incluir las actividades de tratamiento de los proyectos de investigación en el Registro de Actividades de Tratamiento de la universidad.

10. ¿Cómo se debe regular la relación entre corresponsables del tratamiento?

La relación, obligaciones y tareas que va a tener cada corresponsable se debe determinara través de un documento jurídicamente vinculante. Deberá contener como 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.

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

De acuerdo con el artículo 7 de la LOPDyGDD, los menores pueden consentir el tratamiento de sus datos personales con fines de investigación científica a partir de los 14 años siempre que no haya una normativa específica que requiera otra edad u otros requisitos. En el ámbito de la investigación científica, se debe tener en cuenta las especificidades de la investigación en salud y de la investigación biomédica.

En el ámbito de la salud, en aplicación del art. 8 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente, el consentimiento otorgado por un mayor de 14 años será válido salvo que no sea competente, ni intelectual, ni emocionalmente, para comprender el alcance de la intervención sobre su salud. En estos casos, será necesario que el consentimiento sea otorgado por el titular de la patria potestad o tutela.

Finalmente, en el ámbito de la investigación biomédica, es decir, de la investigación que use datos genéticos o muestras biológicas, se requiere que la persona participante tenga al menos 18 años de acuerdo con el art. 4.2 de la Ley 14/2007, de 3 de julio, de investigación biomédica.

12. ¿Cómo se deben publicar los resultados de la investigación?

La publicidad de los resultados de investigación se deberá realizar previa anonimización de los datos de carácter personal, y por tanto, de conformidad al principio de minimización de datos, la regla general será la publicación de los resultados de investigación con datos anonimizados, y solo en el caso de que ello no sea posible, seudonimizados. Lo importante en los estudios e investigaciones son los resultados de las mismas, y no los datos de las personas que han contribuido a la realización de las investigaciones.

13. ¿Cómo se deben reutilizar los datos?

La reutilización puede concebirse como la copia, difusión, modificación, adaptación, extracción,

reordenación, combinación de la información y, además, facilita el desarrollo de nuevos productos, servicios y soluciones de alto valor socioeconómico.

Con respecto a los datos de investigación, se deben adoptar medidas para apoyar que los datos financiados públicamente sean reutilizables, interoperables y de acceso abierto, considerando las limitaciones derivadas de los derechos de propiedad intelectual e industrial, la protección de datos personales y la confidencialidad, la seguridad y los intereses comerciales legítimos. Respecto de la protección de datos, como regla general se deben reutilizar los datos de forma anonimizada. Cuando los fines perseguidos no se puedan conseguir con datos anonimizados, se pueden utilizar datos seudonimizados.