UNIVERSIDAD COMPLUTENSE MADRID

GUÍA BÁSICA PROTECCIÓN DATOS EN INVESTIGACIÓN

Guía básica para la protección de datos en la investigación

1. NOCIONES BÁSICAS SOBRE EL DERECHO DE PROTECCIÓN DE DATOS

✓ **Es un derecho fundamental** reconocido tanto en la Constitución Española, como en diversos tratados internacionales (especialmente en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea).

✓ Este derecho **se encuentra regulado en** el "Reglamento general de protección de datos, 2016/679" **(RGPD**) -norma de la UE- y en nuestra "Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos y garantía de derechos digitales" **(LOPD-GDD).**

✓ **Su objeto es** la protección de las **personas naturales o físicas** en relación con el tratamiento de datos personales, y se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención.

- ✓ Por tanto, no afecta al tratamiento de los datos de personas jurídicas (sociedades, asociaciones, fundaciones, Administraciones e Instituciones Públicas, etc.).

- ✓ Tampoco afecta al tratamiento de personas fallecidas, sin perjuicio de ciertas facultades que tienen los herederos y las personas vinculadas al fallecido por razones familiares o de hecho, en los términos que contempla la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales.

✓ **Un dato personal es "toda información sobre una persona física identificada o identificable".**

- ✓ Una persona es **identificable** cuando su identidad puede determinarse directa o indirectamente mediante uno o varios elementos específicos característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.

- ✓ 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.

✓ El derecho a la protección de datos se materializa en una serie de derechos concretos, cuyo ejercicio es gratuito, y que se refieren al **derecho de acceso** a los datos personales, el **derecho a rectificarlos**, el **derecho a cancelar o suprimirlos (derecho al olvido)** y el **derecho de oposición** al tratamiento o cesión. Asimismo comprende el **derecho a**

limitar el acceso, el **derecho a la portabilidad** de los datos propios, y el **derecho a no ser objeto de perfiles personales sobre los que se tomen decisiones automatizadas**.

✓ Se entiende por **«tratamiento»**, cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción. Es decir, todo lo que se haga con los datos personales, desde su recogida a su destrucción, pasando por la conservación, comunicación, etc, constituye un tratamiento de datos personales.

✓ Los datos personales **deben ser tratados de acuerdo con determinados principios**, concretamente:

- ✓ Los datos deben ser tratados de **manera lícita, leal y transparente** en relación con el interesado: es decir, proporcionando toda la información relativa al tratamiento de sus datos, y recabando su consentimiento expreso;
- ✓ recogidos con fines determinados, explícitos y legítimos, estando prohibido su tratramiento ulterior de manera incompatible con los fines que motivaron la recogida (**«limitación de la finalidad»**);
- ✓ que sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (principio de **«minimización de datos»**);
- ✓ exactos y, si fuera necesario, actualizados (**«exactitud»**);
- ✓ mantenidos de forma que se permita la identificación de los interesados únicamente durante el tiempo necesario para los fines del tratamiento de los datos personales (**«limitación del plazo de conservación»**);
- ✓ tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas (**«integridad y confidencialidad»**).

✓ Todo esto culmina en la **responsabilidad proactiva**, es decir, el responsable del tratamiento debe velar por cumplir los principios del tratamiento, aplicando para ello las medidas técnicas y organizativas que resulten adecuadas; y además, debe ser capaz de demostrar que ha sido diligente en la efectiva aplicación de dichos principios.

Recuerda:

El cumplimiento de la responsabilidad proactiva requiere que todo tratamiento que lleve a cabo el responsible cumpla los principios de:

- **Licitud, lealtad y transparencia**
- **Limitación de la finalidad**
- **Minimización de datos**
- **Exactitud**
- **Limitación de plazo de conservación**
- **Integridad y confidencialidad**

✓ Para ello, el responsable debe adoptar decisiones internas y aplicar medidas que cumplan en particular los principios de protección de datos **desde el diseño** (velando por el cumplimiento íntegro de la normativa de protección de datos desde antes de poner en marcha cualquier iniciativa docente o investigadora) y **por defecto** (tratando únicamente los datos que sean imprescindibles en cada caso).

✓ Estas medidas pueden consistir, entre otras, en:

- ✓ Reducir al máximo el tratamiento de datos personales (minimización);
- ✓ Seudonimizar lo antes posible los datos personales. Para ello, deben aplicarse medidas técnicas y organizativas que permitan disociar la información adicional que sirve para identificar a una persona concreta, y custodiarla de forma separada del resto de información. La seudonimización es una de las medidas que ayudan de forma efectiva a reducir los riesgos para las personas afectadas.
  - **«seudonimización»**: 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 técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.
- ✓ Dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad.
- ✓ Aplicar medidas de seguridad informática, tales como el cifrado de la información, que impidan el acceso de terceros no autorizados; utilización de dispositivos seguros, etc.

RECUERDA:

Al diseñar un Proyecto de investigación basado en el tratamiento de datos personales, o si se van a tratar datos personales para el desarrollo de la investigación, el IP debe asegurarse de que los datos se van a tartar conforme a los principios indicados (licitud, lealtad y transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación de la conservación, e integridad y confidencialidad), adoptando para ello las medidas adecuadas a la tipología de datos y conforme al estado de la técnica.

✓ La licitud del tratamiento implica que **todo tratamiento de datos personales debe estar legitimado** por alguna de las bases jurídicas que identifica el RGPD. A saber:

- ✓ El consentimiento del interesado
- ✓ La celebración de un contrato
- ✓ Por obligación legal
- ✓ La protección de intereses vitales del interesado o de un tercero
- ✓ El interés público
- ✓ El interés legítimo

Como regla general, el tratamiento de los datos personales en la investigación está amparado en el **consentimiento** y, solo en algunos supuestos específicos, en el interés público.

✓ **La libre autonomía de la persona es el fundamento del que se derivan los derechos específicos a otorgar el consentimiento y a obtener la información previa**.

✓ **El «Consentimiento»** se define en el RGPD como toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen. Y en materia de Investigación Biomédica, la Ley 14/2007, lo define como la la manifestación de la voluntad libre y consciente válidamente emitida por una persona capaz, o por su representante autorizado, precedida de la información adecuada.

✓ En general, el consentimiento tiene que ser expreso, por lo que ni se presupone, ni puede venir premarcado. Debe ser siempre informado y transparente, y puede revocarse en cualquier momento y con la misma facilidad con la que se prestó.

✓ No obstante, **cuando hablamos de investigación biomédica o de una investigación que va a recabar datos sensibles o de colectivos vulnerables, se require el consentimiento explícito e informado**.

✓ Para ello, deberá redactarse toda la información de manera que sea exacta, completa, accesible y visible, y de fácil comprensión para el interesado, utilizando un lenguaje sencillo y claro.

✓ El consentimiento se recabará de manera que pueda identificarse a quien lo presta. En ejercicio de la responsabilidad proactiva, el consentimiento deberá quedar suficientemente acreditado, y el responsable (IP) deberá conservar la prueba de su obtención durante todo el tiempo que dure la investigación y aún después, por el tiempo en el que pueda ser refutada la investigación, a fin de poder demostrar la obtención de los consentimientos sobre la participación de los sujetos fuente para la obtención de resultados.

RECUERDA:

Cuando hablamos de investigación biomédica o de una investigación que va a recabar datos que merecen una especial protección, se require el consentimiento explícito e informado del interesado.

En ejercicio de la responsabilidad proactiva, el consentimiento deberá quedar suficientemente acreditado –pudiendo identificar al que lo presto-, y el responsable (IP) deberá conservar la prueba de su obtención durante todo el tiempo que dure la investigación y aún después, por el tiempo en el que pueda ser refutada la investigación, a fin de poder demostrar la obtención de los consentimientos sobre la participación de los sujetos fuente para la obtención de resultados.

✓ **Los menores, pueden consentir, con carácter general, por sí solos si tienen 14 años cumplidos.** Por tanto, los menores de 14 años requieren de consentimiento de sus representantes legales. Si solo se puede conseguir el consentimiento de uno de ellos, resulta conveniente que éste se responsabilice del consentimiento del otro representante legal del menor. **No obstante, existen supuestos en los que la edad para consentir el tratamiento o la cesión de datos es superior a 14 años**, cuando el acto o negocio jurídico exigen que el menor tenga una edad mayor para poder realizar válidamente dicho acto o negocio jurídico. Por ejemplo, **en el ámbito sanitario, la edad para que un menor consienta por sí solo es de 16 años**. Y se requiere de **18 años para enajenar o gravar bienes de extraordinario valor** (que no pueden realizar por sí solos ni tan siquiera los menores emancipados).

✓ Además, está prohibido cualquier tratamiento o cesión de datos y/o imágenes de un menor que atente, de manera objetiva, contra su **honor, intimidad y propia imagen.** En tales casos, **la obtención del consentimiento del propio menor o de sus representantes legales no sirve** para legitimar dicha intromisión ilegítima.

2. CONCEPTO DE RESPONSABLE, CORRESPONSABLES Y ENCARGADO DEL TRATAMIENTO

✓ **El titular de los datos es, *siempre,* la persona interesada o concernida.** Toda persona física es "dueña" de sus propios datos, sin perjuicio de la existencia de determinadas bases jurídicas que pueden legitimar un tratamiento incluso aunque no exista consentimiento del titular de los datos.

✓ **El "responsable de un tratamiento" (*controller*) 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.

✓ Mientras que el "**encargado del tratamiento" *(processor*)** es la persona que trata los datos siguiendo las indicaciones del responsable. Es decir, lo hace siguiendo las instrucciones, los fines y medios marcados por el responsable.

✓ Por consiguiente, si un estudiante, un doctorando o un investigador determina los fines y medios de un tratamiento de datos personales de su TFG/TFM, tesis doctoral o investigación, es responsable de ese tratamiento. Del mismo modo, la UCM es responsable de las actividades de tratamiento que realiza y gestiona su personal.

RECUERDA:

El "responsable de un tratamiento" (controller) 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.

Si un estudiante, un doctorando o un investigador determina los fines y medios de un tratamiento de datos personales de su TFG/TFM, tesis doctoral o investigación, es responsable de ese tratamiento.

Por su parte, la UCM es responsable de las actividades de tratamiento que realiza y gestiona su personal, en el ejercicio de sus funciones.

✓ En la investigación, y sobre todo **en los proyectos de investigación entre diversos grupos** o "*partners*", puede haber una **responsabilidad conjunta o corresponsabilidad** (*join controllers*), cuando intervienen distintos responsables que llevan a cabo la actividad descrita de forma conjunta. En los casos en los que haya corresponsables del tratamiento, estos determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el Reglamento. Para ello, firmarán un documento en el que se fije el acuerdo de corresponsabilidad, con los fines y medios que se utilizan para llevar a cabo el tratamiento, la cooperación entre los corresponsables para responder al ejercicio de derechos; cuando sea necesario, una metodología de evaluación de impacto conjunta; y, si procede, un mecanismo acordado de contratación de encargados de tratamiento.

✓ En otras ocasiones, existe un único responsable, que es el que decide en exclusiva los fines y los medios del tratamiento, encomendando a otras personas físicas o jurídicas que desarrollen o lleven a cabo determinados tratamientos en calidad de encargados. En este caso, es **necesario suscribir** **un contrato de encargado del tratamiento (artículo 28 RGPD)**, que delimite los tratamientos autorizados y los medios que va a emplear el encargado para garantizar la integridad y confidencialidad de la información y los mecanismos de coordinación en caso de brechas de seguridad, posibilidades de subcontratación, y demás elementos del cumplimiento normativo.

LA AEPD ofrece unas directrices para elaborar, contratos del artículo 28 RGPD en: https://www.aepd.es/media/guias/guia-directrices-contratos.pdf.

3. EL REGISTRO DE LAS ACTIVIDADES DEL TRATAMIENTO

✓ En la actualidad, todo responsable –y también todo encargado– debe elaborar un inventario en el que se registre cada actividad de tratamiento que lleva a cabo, a fin de ofrecer información específica sobre dicho tratamiento a las personas afectadas. Dicho registro deberá contener toda la información indicada a continuación:

a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y, cuando proceda, del delegado de protección de datos;

b) los fines del tratamiento;

c) una descripción de las categorías de interesados y de las categorías de datos personales;

d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;

e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional;

f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;

g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad aplicadas.

✓ El registro constará por escrito, incluso en formato electrónico, y será facilitado a los interesados cuando lo soliciten.

✓ La UCM tiene publicados su inventario de actividades del tratamiento en la dirección web https://www.ucm.es/dpd/actividades-generales Y, más concretamente el RAT correspondiente a la actividad de investigación está accesible en https://www.ucm.es/data/cont/media/www/pag-126969/Grupos%20de%20Investigaci%C3%B3n.pdf

3.- TRATAMIENTOS DE DATOS SENSIBLES

✓ Todos los datos personales deben ser protegidos. Sin embargo, esa protección debe reforzarse cuando se tartan datos datos personales que, por su naturaleza, son **particularmente sensibles** en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales.

✓ Debemos tener especial cuidado y atención con:

(a) Las **categorías especiales** de datos relativas al origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física. Estos datos gozan de una protección reforzada y compleja.

(b) Los datos personales relativos a **condenas e infracciones penales**, que solo podrán tratarse bajo ciertas circunstancias.

(c) Los datos personales relativos a **infracciones y sanciones administrativas**, que, salvo que medie el consentimiento expreso o en los supuestos previstos por la Ley, solo podrán tratarse por los órganos competentes para la instrucción del procedimiento sancionador, para la declaración de las infracciones o la imposición de las sanciones, y por los abogados y procuradores para la defensa de sus clientes.

(d) Datos relativos a **colectivos vulnerables**, como pueden ser las víctimas de violencia de género, abuso o agresión sexual o acoso; menores de edad, personas ancianas, personas con discapacidad o enfermedad grave o en riesgo de exclusion social. Se incluyen también las víctimas de violencia de género.

✓ Si bien el tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales (pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación *unívocas* de una persona física); debemos tener en cuenta que dicho tratamiento puede provocar una potente injerencia en el entorno privado de la persona interesada y, además, puede afectar a su honor e intimidad, especialmente en el caso de menores (porque son derechos fundamentales a los que se aplica otras leyes como la Ley Orgánica de Protección al honor, intimidad y propia imagen o la de protección del menor).

RECUERDA:

Todos los datos personales deben ser protegidos. Sin embargo, esa protección debe reforzarse cuando se tartan datos datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales.

Merecen especial protección:

- **las categorías especiales de datos a que se refiere el art. 9 del RGPD, los datos relativos**
- **los datos relativos a condenas e infracciones penales**
- **los datos relativos a infracciones y sanciones administrativas**
- **los datos que afectan a colectivos vulnerables o en riesgo de exclusión**

✓ Antes de iniciar un nuevo tratamiento de datos personales, **cuando sea probable que conlleve un alto riesgo para los derechos y libertades de los interesados, es necesario realizar una evaluación de impacto en protección de datos (EIPD)**.

✓ El RGPD advierte de la necesidad de realizar esta EIPD, cuando nos encontremos ante los siguientes casos:

- ✓ Evaluación sistemática y exhaustiva de datos personales basada en un tratamiento automatizado. Por ejemplo, elaboración de perfiles para tomar decisiones que produzcan efectos jurídicos para las personas.
- ✓ Tratamiento a gran escala de datos personales sensibles.
- ✓ Observación sistemática a gran escala de zonas de acceso público.

✓ Por su parte, la Agencia Española de Protección de Datos (AEPD) ha facilitado un listado –no exhaustivo– en los que es necesario realizar esta previa EIPD. A saber:

- ✓ Tratamientos que impliquen ***perfilado o valoración de sujetos***, incluida la recogida de datos del sujeto en múltiples ámbitos de su vida (desempeño en el trabajo, personalidad y comportamiento), que cubran varios aspectos de su personalidad o sobre sobre sus hábitos.
- ✓ Tratamientos que impliquen ***la toma de decisiones automatizadas o que contribuyan en gran medida a la toma de decisiones***, incluyendo cualquier tipo de decisión que impida a un interesado el ejercicio de un derecho o el acceso a un bien o un servicio o formar parte de un contrato.
- ✓ Tratamientos que impliquen la ***observación, monitorización, supervisión, geolocalización o control del interesado*** de forma sistemática y exhaustiva, incluida la ***recogida de datos y metadatos a través de redes***, aplicaciones o en zonas de acceso público, así como el ***procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, tv interactiva, aplicaciones móviles*****,** etc.

✓ Tratamientos que impliquen el **uso de categorías especiales de datos** (***datos de salud física y psíquica, orientación sexual, ideología***), ***datos relativos a condenas o infracciones penales*** los que se refiere el o datos que permitan determinar la ***situación financiera o de solvencia patrimonial*** o deducir información sobre las personas relacionada con categorías especiales de datos.

✓ Tratamientos que impliquen el uso de ***datos biométricos*** con el propósito de identificar de manera única a una persona física.

✓ Tratamientos que impliquen el uso de ***datos genéticos*** para cualquier fin.

✓ Tratamientos que impliquen el uso de datos a gran escala. Para determinar si un tratamiento se puede considerar a gran escala se considerarán los criterios establecidos en la guía WP243 "Directrices sobre los delegados de protección de datos (DPD)" del Grupo de Trabajo del Artículo 29.

✓ Tratamientos que impliquen la ***asociación, combinación o enlace de registros de bases de datos de dos o más tratamientos con finalidades diferentes*** o por responsables distintos.

✓ Tratamientos de datos de **sujetos vulnerables o en riesgo de exclusión social**, incluyendo ***datos de menores de 14 años, mayores con algún grado de discapacidad, discapacitados, personas que acceden a servicios sociales y víctimas de violencia de género***, así como sus descendientes y personas que estén bajo su guardia y custodia.

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

✓ Tratamientos de datos ***que impidan a los interesados ejercer sus derechos, utilizar un servicio o ejecutar un contrato***, como por ejemplo tratamientos en los que los datos han sido recopilados por un responsable distinto al que los va a tratar y aplica alguna de las excepciones sobre la información que debe proporcionarse a los interesados según el artículo 14.5 (b, c, d) del RGPD.

✓ **El Contenido del Informe de Evaluación de impacto (IEI), artículo 35.7 RGPD deberá incluir como mínimo:**

✓ Una ***descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento***, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento.

✓ Una ***evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento*** con respecto a su finalidad.

✓ Una **evaluación de los *riesgos para los derechos y libertades de los interesados***.

✓ Las ***medidas previstas para afrontar los riesgos*****, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales**, y a **demostrar la conformidad con el RGPD,** teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras

personas afectadas.

✓ En caso de no poder mitigar el riesgo, el responsable deberá consultar a la Agencia de Protección de Datos (AEPD). La autoridad de control podrá hacer recomendaciones o prohibir el tratamiento.

RECUERDA:

- **Toda investigación que conlleve una actividad de tratamiento de datos personales, deberá inventariarse, y conservarse el registro para su puesta a disposición de los interesados o de la Autoridad de Control.**
- **Si la investigación se lleva a cabo con otros responsables, será necesario firmar un contrato entre responsables (*controller to controller*).**
- **Si en la investigación se encomienda algún tratamiento a un encargado, deberá firmarse un contrato específico (*controller to processor*)**
- **En algunos casos, cuando el tratamiento conlleve un alto riesgo para los derechos y libertades de los afectados, será necesario realizar una previa Evaluación de Impacto en Protección de Datos.**

4. RECOMENDACIONES ESPECÍFICAS PARA LA INVESTIGACIÓN

✓ Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable.

✓ Los **datos personales seudonimizados**, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable.

- ✓ 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.

✓ Sin embargo, es **información anónima** aquella que no guarda relación con una persona física identificada o identificable, así como los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo.

La información anónima es un conjunto de datos que no guarda relación con una persona física identificada o identificable.

La información seudonimizada es un conjunto de datos que no puede atribuirse a un interesado sin utilizar información adicional, requiere que dicha información adicional figure por separado y, además, esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

- ✓ Transformar un conjunto de datos personales en información anónima o seudonimizada exige realizar un tratamiento sobre dichos datos personales.
  - ✓ El tratamiento de anonimización genera un único y nuevo conjunto de datos. Por ejemplo, una estadística conlleva la anonimización de los datos de los que se parte para su elaboración. De un porcentaje es muy difícil extraer el identidad de una persona incluida en ese porcentaje (si bien, en determinadas circunstancias, el cruce de información podría llegar a permitir esa reidentificación).
  - ✓ El tratamiento de seudonimización genera dos nuevos conjuntos de datos: la información seudonimizada y la información adicional que permite revertir la anonimización. Por ejemplo, si en la investigación se analiza la situación de "un paciente", esa información está seudonimizada, puesto que podría reidentificarse al paciente.
- ✓ El conjunto de datos anonimizados no está bajo el ámbito de aplicación de la normativa reguladora de la protección de datos, aunque pudiera estar bajo el ámbito de aplicación de otras normas (p. ej. de seguridad nacional, salud pública, infraestructuras críticas, etc.) En este caso debe tenerse en cuenta que:
  - ✓ El tratamiento que generan los datos anonimizados sí es un tratamiento de datos personales, que puede considerarse compatible con el fin original del tratamiento de datos personales del que proceden los datos.
  - ✓ Para que el conjunto de datos anonimizados sea conforme a la normativa reguladora de la protección de datos, deberá vigilarse la robustez del proceso de anonimización contra la posible reidentificación.
  - ✓ Una vez que el conjunto de datos está correctamente anonimizado, su tratamiento queda fuera del ámbito de aplicación del RGPD en la medida que es posible demostrar objetivamente que no existe capacidad material para asociar los datos anonimizados a una persona física determinada, directa o indirectamente, ya sea mediante el uso de otros conjuntos de datos, informaciones o medidas técnicas y materiales que pudieran existir a disposición de terceros.
  - ✓ Por tanto, sobre la información anónima no es necesario implementar las garantías de protección de datos ni los principios del tratamiento.

✓ La Unión Europea recomienda que los ficheros de datos personales destinados a investigación sean principalmente ficheros anonimizados, con un doble fin: evitar la compleja gestión en materia de protección de datos y favorecer la libre circulación de datos anonimizados en el ámbito del Big Data.

Los datos se considerarán anonimizados en la medida que no exista una probabilidad razonable que cualquier persona pueda identificar a la persona física en el conjunto de datos.

Dicha evaluación ha de tener en cuenta los costes, el tiempo requerido para llevar a cabo la reidentificación o los medios tecnológicos necesarios para conseguir la reversión de la anonimización, tanto los actuales como teniendo en cuenta los avances tecnológicos.

La AEPD publica una guía con los 10 malentendidos de la anonimización:

https://www.aepd.es/es/documento/10-malentendidos-anonimizacion.pdf

✓ **El conjunto de datos seudonimizados, y la información adicional vinculada** con dicho conjunto de datos, **SÍ** están bajo el ámbito de aplicación del RGPD, así como el tratamiento que los genera.

✓ De ahí que el conjunto de datos seudonimizados esté protegido por cuatro tipos de garantías:

- ✓ en primer lugar, el propio tratamiento de seudonimización que ha de impedir la reidentificación sin disponer de la información adicional;
- ✓ en segundo lugar, los principios y garantías del RGPD que establecen limitaciones, entre otras, a las finalidades, el periodo de conservación o la comunicación de los datos seudonimizados;
- ✓ en tercer lugar, las garantías adicionales que incorpore el tratamiento de los datos seudonimizados en función del riesgo para los derechos y libertades de las personas físicas;
- ✓ en cuarto lugar, derivado del anterior, las garantías técnicas y organizativas dispuestas al efecto de impedir la materialización de brechas de datos personales, tanto sobre conjunto seudonimizado como de la información adicional.

✓ La seudonimización es uno de los mecanismos idóneos para la seguridad de la información tratada con fines de investigación en salud y, en particular, biomédica.

✓ Es muy importante recordar que **el uso de datos personales seudonimizados con fines de investigación en salud pública y, en particular, biomédica deberá ser sometido siempre al informe previo del comité de ética de la investigación previsto en la normativa sectorial**, para comprobar las medidas de seguridad y confidencialidad respecto de los datos que permiten la reidentificación, y que dicha reidentificación se realice únicamente cuando se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos, o sea necesaria para garantizar una adecuada asistencia sanitaria.

✓ **La praxis habitual en Medicina es que la historia clínica del paciente tenga dos tipos de accesos. Un primer acceso a la historia clínica con los datos personales de identificación** del paciente, que es el que utiliza el médico que debe de prestar asistencia sanitaria personalizada. **Y un segundo acceso, al conjunto de historias clínicas seudonimizadas, para que puedan ser consultadas por los servicios de salud pública y por los grupos de investigación**, respetando la intimidad y el honor del paciente y resultando imposible que el investigador pueda identificar a ningún paciente, salvo que utilice un proceso de "reidentificación", controlado por una persona o grupo limitado de personas, que tienen que comprobar además si existe causa justificada para la reidentificación.

✓ El **acceso a la historia clínica** está regulado en el artículo 16 de ley 41/2002, de derechos del paciente. Así, por ejemplo, cuando sea necesario para la prevención de un riesgo o peligro grave para la salud de la población, **las Administraciones competentes en salud pública podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública**, pero el acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos, a no ser que sea para proteger la vida o integridad física del titular de los datos o personas próximas, en cuyo caso está permitido el acceso, tratamiento y la cesión de datos sin consentimiento.

- ✓ **La LOPD-GDD ha previsto la posibilidad de "reutilizar" los datos de investigación con fines de salud** (física o mental) sin necesidad de obtener un nuevo consentimiento. En concreto, se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomedicina 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.

- ✓ Para ello es absolutamente **imprescindible contar con el informe previo favorable del Comité de ética.**

- ✓ Y además, debe informarse a los posibles interesados. Por ejemplo, a través del portal del organismo que desarrolle la investigación.

✓ La normativa de investigación y, en especial, la Ley 14/2007, de 3 de julio, de Investigación biomédica, han previsto la existencia de "**Comités de ética de la investigación**". Dichos comités tienen como misión garantizar el respeto a la dignidad, integridad e identidad del ser humano en lo que se refiere a la investigación con humanos, con muestras biológicas o con "datos" de origen humano, así como promover un comportamiento ético en la investigación. Por tanto, entre sus competencias está el velar por el cumplimiento de la normativa vigente aplicable en materia de protección de datos y de investigación cuando se vayan a utilizar datos personales de personas físicas identificadas o identificables, datos seudonimizados o datos anonimizados, por lo que **cualquier investigación que contenga datos personales deberá contar con la autorización del comité de ética competente en investigación sobre personas (es la llamada "ética de los datos", que exige que se cumpla la normativa de protección de datos, como derecho fundamental, en toda investigación con datos de personas**

físicas identificadas o seudonimizadas).

5. MEDIDAS DE SEGURIDAD PARA UNA INVESTIGACIÓN RESPETUOSA CON LA PROTECCIÓN DE DATOS PERSONALES.

✓ Una buena gestión de la seguridad de la información personal que se maneje en la investigación, recomienda abordar varios aspectos, que podemos agrupar en diferentes categorías.

✓ En relación con la clasificación de la información:

- ✓ Lo primero que debe evaluarse es si existe o no tratamiento de datos personales. Si la respuesta es afirmativa, deberá identificarse el grado de sensibilidad de los datos personales, a fin de diseñar unas medidas de seguridad adecuadas al riesgo.
    - Las medidas de seguridad apropiadas se concretarán una vez evaluada la sensibilidad y criticidad en el caso de revelación o modificación no autorizadas de dichos datos.
- ✓ Los datos personales se clasificarán y etiquetarán en función de su nivel de seguridad, a fin de que los usuarios –miembros del equipo de investigación con acceso a la información– conozcan la trascendencia de la información personal.
- ✓ En relación a esto, se establecerán procedimientos para el tratamiento de los datos en función de la clasificación realizada sobre la base de su sensibilidad o criticidad.

✓ En relación con la manipulación de los soportes (tanto soporte digital como papel):

- ✓ Gestión de soportes extraíbles: el uso de discos externos de almacenamiento puede suponer un riesgo para la seguridad, por lo que es necesario un control sobre el uso de este tipo de soportes. Por lo tanto, será útil la implantación de medidas de seguridad como por ejemplo cifrado, registros, monitorización de su uso o borrado seguro.
- ✓ Eliminación de soportes: una vez un soporte se deje de utilizar, deberá retirarse conforme a procedimientos claramente establecidos por el grupo de investigación.
- ✓ Soportes físicos en tránsito: cuando la información personal se traslade fuera de los límites físicos de la Universidad, los soportes con información estarán protegidos contra accesos no autorizados, usos indebidos o deterioro mediante medidas de seguridad tales como el establecimiento de procedimientos para cotejar las salidas con los soportes, la utilización de mensajeros o transportistas de confianza o el cifrado de la información.

✓ Medidas organizativas y asignación de roles:

- ✓ Documentación de procedimientos sobre el tratamiento de datos personales: es recomendable recoger en procedimientos actualizados el reparto de

tareas, con la asignación de roles y responsabilidades, y mantenerlos a disposición de todos los miembros del equipo de investigación que los necesiten.

- ✓ Además, es importante identificar los requisitos de capacidad, de cara a ajustar la utilización de los recursos y garantizar el rendimiento del sistema. Así, se podrá gestionar por ejemplo mediante el borrado de datos obsoletos.

- ✓ Separación de los recursos de desarrollo, prueba y operación: en el marco del desarrollo de sistemas, de cara a garantizar la seguridad de la información deberían separarse los entornos de desarrollo e integración de los de producción. Por ejemplo, en el caso de desarrollar un sistema de gestión de nóminas, que en el momento de prueba se realice en un entorno separado de donde se contenga el resto de la información.

✓ **Los datos tienen que estar alojados en servidores seguros.** Todas las páginas web y servicios de almacenamiento que dependen de la UCM están en servidores seguros, y además están plenamente adaptados al Esquema Nacional de Seguridad.

✓ **Intercambio de información:** cuando mediante un recurso de comunicación se traslade información dentro del grupo de investigación o con una entidad externa es necesario que sea de manera segura, existiendo los siguientes controles de cara a proteger dichos intercambios:

- ✓ Establecimiento de políticas y procedimientos de intercambio de información, definiéndose medidas de seguridad en función del soporte en que tenga lugar el intercambio, por ejemplo, correo electrónico, fax, voz o vídeo.

- ✓ Acuerdos de intercambio de información: cuando se intercambie información con una organización externa, una opción para asegurar la protección de la confidencialidad es documentar un acuerdo en el que además se establezcan las responsabilidades del emisor y receptor en el uso de la información.

- ✓ Mensajería electrónica: es importante establecer medidas de cara a proteger las comunicaciones realizadas a través de correo electrónico, chats internos o redes sociales, así como la disponibilidad del servicio. Se recomienda el cifrado de toda la información que se remita por estos medios.

- ✓ Acuerdos de confidencialidad o no revelación: con carácter previo al intercambio de información confidencial deberá procederse a firmar el pertinente acuerdo de confidencialidad, que deberán quedar documentados y donde se recogerán las consecuencias en caso de incumplimiento del deber de secreto por alguna de las partes.

✓Una de las novedades más relevante que tiene el nuevo marco normativo de protección de datos es que **hay que informar *inmediatamente*,** en caso de "***brecha de seguridad"*** sobre los ficheros propios, **al delegado de protección de datos** de la institución, a fin de que éste pueda evaluar los riesgos, y decida si se tiene que comunicar a la Agencia Española de Protección de Datos y a los interesados afectados.

6. EL ACUERDO DE CONFIDENCIALIDAD O *NON DISCLOSURE AGREEMENT* "NDA"

✓ Los acuerdos de confidencialidad (en inglés *NDA*) son documentos o contratos en los que una concreta persona se obliga a guardar secreto sobre ideas, sobre el desarrollo de nuevos productos y procedimientos o sobre cualquier información personal e íntima que se derive de los datos personales y a los que tenga acceso legítimo.

✓ Por ello, cualquier investigador o tercero que pueda tener acceso legítimo a los datos debería tener firmado un compromiso de confidencialidad respecto de las informaciones y circunstancias que pueda conocer con ocasión de dicho acceso legítimo a datos personales, sobre todo si se están tratando datos especialmente protegidos o íntimos.

✓ Se recomienda que todo investigador conozca las diferentes conductas que pueden ser constitutivas de delito en materia de protección de datos, especialmente las previstas en el **artículo 197 del Código Penal.**

✓ **Para garantizar o reforzar el cumplimiento de la normativa de protección de datos, conviene que también firme un "compromiso de confidencialidad",** más allá de sus deberes de secreto profesional, **la persona responsable del proceso seudonimización**, (esto es, la persona que tiene acceso al proceso o variables que permiten la reidentificación de aquellos datos personales seudonimizados y que se ofrecen de forma anonimizada al resto de investigadores).