Novedades en el tratamiento de datos personales en el sector de la investigación biomédica

Natalia Olivares Álvarez

Sarai Nieto Sánchez

Noviembre 2023

IdISSC INSTITUTO de INVESTIGACIÓN SANITARIA Hospital Clínico San Carlos

alaro avant Seguridad de la Información

Programa

1. **Breve recordatorio sobre los conceptos fundamentales del RGPD aplicados al ámbito de la investigación biomédica:** especial referencia a la diferencia entre datos seudonimizados y datos anonimizados

2. **Licitud del tratamiento para fines de investigación clínica:** especial referencia a la publicación de las bases de datos de los Estudios
    a. Bases legítimas
    b. Criterios interpretativos Dictamen 3/2019 del CEPD

3. **Transferencias internacionales de datos**
    a. Conceptos básicos sobre las Transferencias internacionales de datos
    b. Garantías para las Transferencias internacionales de datos
        i. Especial mención USA
        ii. Nuevas Cláusulas Contractuales Tipo adoptadas por la Comisión – Decisión de Ejecución (UE) 2021/914 de la Comisión

1. Breve recordatorio sobre los conceptos fundamentales del RGPD aplicados al ámbito de la investigación biomédica: especial referencia a la diferencia entre datos seudonimizados y datos anonimizados

Recordatorio: conceptos clave

Datos personales: toda información sobre una persona física identificada o identificable («el interesado»). **Ejemplo**: nombre y apellidos, dirección de email, edad, sexo, DNI, nº teléfono, HC, fotografías, voz, historial médico, muestras biológicas humanas que contengan datos genéticos como ADN, etc.

Interesado: persona física de la cual se tratan los datos. Es el titular, el propietario de los datos objeto del tratamiento y respecto al que se debe poner el foco → protección de los derechos y libertades del interesado. **Ejemplo**: participante en proyecto de investigación.

Tratamiento de datos personales: 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. **Ejemplo**: una empresa de hosting, por el hecho de almacenar la información en sus sistemas, ya estaría realizando un tratamiento de datos personales.

Responsable del tratamiento: persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento. **Ejemplo**: Centro responsable de las HC de los participantes en proyecto.

Encargado del tratamiento: persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento. **Ejemplo**: monitor de proyecto de investigación (encargado del Promotor).

Destinatario: persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. **Ejemplo**: cuando entre dos entidades se firma un MTA, la entidad que recibe las muestras sería el destinatario.

Corresponsable: cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. **Ejemplo**: si dos entidades organizan conjuntamente un evento y ambas deciden qué datos se van a recabar, con qué finalidades, si se les va a enviar información comercial, etc.

Recordatorio: conceptos clave

Si bien anteriormente hemos clarificado algunos conceptos fundamentales recogidos en el RGPD, es un error común que en el sector de la investigación **se tienda a pensar que en determinados proyectos de investigación no se tratan datos personales**.

Como hemos visto anteriormente, la edad, el sexo, la estatura o el peso de una persona, son datos de carácter personal, por lo que aunque no se estén tratando datos que identifican directamente a una persona, como el nombre, apellidos, o el DNI, el tr**atamiento de datos como la edad, el sexo, etc., por si solos podrían llegar a identificar a dicha persona**.

Como veremos a continuación, los **datos codificados (seudonimizados)** recogidos en un cuaderno de recogida de datos, **también son datos personales**.

Así mismo, nos podemos encontrar en la situación de contratar una empresa de transporte de muestras biológicas que afirme que no trata datos personales. ¿Cuál sería la respuesta correcta a dicha afirmación? Que la empresa de transporte de muestras biológicas **SÍ trata datos personales**, ya que el tratamiento de datos implica, entre otros: la recogida, la organización y la conservación.

Datos seudonimizados vs datos anonimizados

¿Cuál es la importancia de diferenciar estos conceptos?

- ✓ Determinar si nos encontramos ante datos personales o no;
- ✓ Determinar si aplica la normativa de protección de datos (identificabilidad).

DATOS SEUDONIMIZADOS (y la información adicional vinculada con dicho conjunto de datos)	Quedan dentro del ámbito de aplicación de la normativa de protección de datos personales	Deben determinarse las responsabilidades y cumplirse todas las obligaciones establecidas en el RGPD y la LOPDgdd
DATOS ANONIMIZADOS	NO quedan dentro del ámbito de aplicación de la normativa de protección de datos personales	No obligación cumplimiento RGPD ni LOPDgdd, pero puede estar bajo el ámbito de aplicación de otras normativas

Datos seudonimizados vs datos anonimizados

Seudonimización ≠ Anonimización

SEUDONIMIZACIÓN: tratamiento de datos de carácter personal, de manera que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que la 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.

Características:

- **Separar el dato identificativo del resto** de los datos;
- Se trata de una **medida técnica** que reduciría el vínculo existente entre los datos de carácter personal y la persona a la que identifican;
- **Codificación**;
- El tratamiento de seudonimización genera dos nuevos conjuntos de datos: la **información seudonimizada** y la **información adicional** que permite revertir el proceso;
- El tratamiento que genera el conjunto de datos seudonimizados, y la información adicional vinculada con dicho conjunto de datos, es un tratamiento de datos personales → Proceso de seudonimización requiere **cumplimiento de normativa de protección de datos**.

Datos seudonimizados vs datos anonimizados

Considerando 26 RGPD:

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.

La seudonimización en el RGPD como medida de seguridad apropiada:

***Seguridad del tratamiento de datos personales (artículo 32 del RGPD);**

***Técnica que puede promover la protección de datos desde el diseño (artículo 25 del RGPD).**

Es una forma de cumplir con el principio de responsabilidad proactiva establecido en el artículo 5 RGPD.

Datos seudonimizados SON datos personales para ambas partes, incluso para la parte que no tiene la "llave" para reidentificar al interesado.

Datos seudonimizados vs datos anonimizados

Conjunto de datos seudonimizados está protegido por cuatro tipos de garantías:

Proceso de seudonimización	Principios y garantías del RGPD	Garantías en función del riesgo	Garantías contra brechas de datos
Impedir la reidentificación sin disponer de la información adicional	Establecer limitaciones, entre otras: • a las finalidades, • el periodo de conservación, • la comunicación de los datos seudonimizados	Garantías adicionales que incorpore el tratamiento de los datos seudonimizados en función del riesgo para los derechos y libertades de las personas físicas	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

Datos seudonimizados vs datos anonimizados

ANONIMIZACIÓN: tratamiento de datos, de manera que ya no resulte posible atribuir a una persona física identificada o identificable.

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

¿Qué entendemos por "resultar posible"? Considerando 26 RGPD: *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****.*

Nivel de reidentificabilidad dependiendo de tecnología disponible, tiempo, coste, etc.

Necesario eliminar o reducir al mínimo los riesgos de reidentificación de los datos anonimizados

Datos seudonimizados vs datos anonimizados

Características anonimización:

- Datos anonimizados no permiten identificar al sujeto porque **no hay vínculo entre el identificador y el sujeto** → no será posible la vinculación del dato con la persona a la que hubiese identificado;
- **Información que no guarda relación con una persona** física identificada o identificable;
- **Información agregada**, estadística;
- El tratamiento de anonimización genera un **único y nuevo conjunto de datos**;
- 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 → **Proceso anonimización requiere cumplimiento de normativa de protección de datos**.

Datos anonimizados **NO son datos personales**

(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)

Datos seudonimizados vs datos anonimizados

Garantías. Sobre el conjunto de datos anonimizados, desde el punto de vista del RGPD, solo aplica un tipo de garantías:

Proceso de Anonimización	Principios y garantías del RGPD	Garantías en función del riesgo	Garantías contra brechas de datos
Robustez del proceso de anonimización contra la posible reidentificación.	Establecen limitaciones, entre otras: • a las finalidades, • el periodo de conservación, • la comunicación de los datos seudonimizados	Garantías adicionales que incorpore el tratamiento de los datos seudonimizados en función del riesgo para los derechos y libertades de las personas físicas	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

Una vez el conjunto de datos está anonimizado, desaparece la obligación de implementar los otros tres conjuntos de garantías, al menos desde el punto de vista de la normativa de protección de datos.

Datos seudonimizados vs datos anonimizados

El concepto de ”anonimización” en la Ley 14/2007, de Investigación biomédica (LIB)

- El artículo 3.c) LIB entiende por **«Anonimización»:**

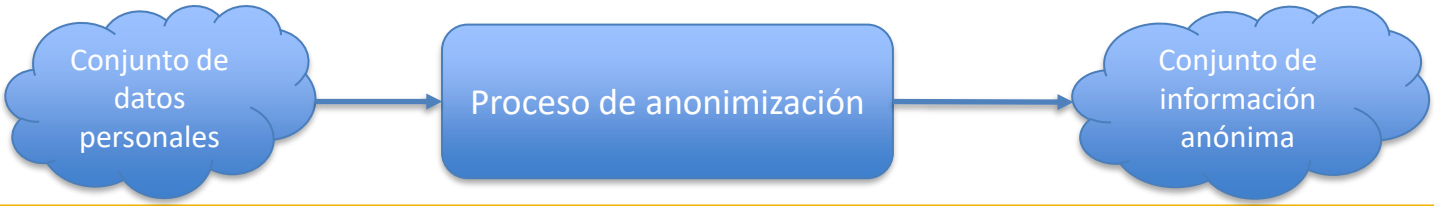
  proceso por el cual deja de ser posible establecer por medios razonables el nexo entre un dato y el sujeto al que se refiere. Es aplicable también a la muestra biológica.

- El artículo 3.h) LIB entiende por «**Dato anónimo**»:

  dato registrado sin un nexo con una persona identificada o identificable.

- El artículo 3.i) LIB entiende por **«Dato anonimizado o irreversiblemente disociado»:**

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



Datos seudonimizados vs datos anonimizados

Reflexión seudonimización VS anonimización:

- La definición teórica es clara, pero, hoy en día es **complejo**, en el campo de la investigación y por la tecnología que existe, **concluir que un dato está anonimizado** (**salvo datos agregados**).
- Los procesos de **anonimización y seudonimización** son una herramienta válida para garantizar la **privacidad de los datos** personales y sus **limitaciones** son **inherentes al avance de la tecnología**.
- Aunque no pueda unir el conjunto de información con el dato identificativo, el **conjunto de la información sí permite singularizar** o inferir a la persona (**datos seudonimizados**).
- La **seudonimización no es** un método de **anonimización**.
- La seudonimización y la anonimización **no siguen el mismo proceso**.
- Los **derechos y libertades de los interesados** han de estar **igualmente protegidos** tanto en los tratamientos de anonimización como en los procesos de seudonimización.
- Se han de diseñar y validar los tratamientos de anonimización pensando en la protección de los derechos de los interesados → poder demostrar un **nivel objetivo de calidad** en el tratamiento de anonimización.

En cualquier caso, **la reversión de la anonimización supone la plena aplicación del RGPD** a los sujetos obligados que traten los datos personales.

Datos seudonimizados vs datos anonimizados

Caso práctico. Supongamos un proyecto de investigación en el que se va a recabar determinada información de los participantes (edad, género, estatura, origen racial, peso, código postal de residencia, código de identificación asignado al paciente del cual se conservarán las tablas de correspondencia), pero no se recabaran datos identificativos directos (nombre, apellidos, DNI).

¿Nos encontramos ante datos seudonimizados o anonimizados?

Estaremos ante tratamiento de **datos seudonimizados** por lo que aplicarán todas las obligaciones de la normativa:

- Valorar el tratamiento de datos que se va a realizar;
- Determinar qué figura (responsable, encargado, etc.) se va a ocupar respecto a esos datos;
- Cumplimiento de los principios de tratamiento de tales datos;
- Establecer una licitud para el tratamiento de los datos;
- Información a los interesados respecto al tratamiento de sus datos;
- Aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo;
- Firmar los contratos de encargado de tratamiento/corresponsabilidad/otros, en su caso;
- Privacidad desde el diseño y por defecto;
- Atender ejercicios de derecho del interesado;
- Etc.

Datos seudonimizados vs datos anonimizados

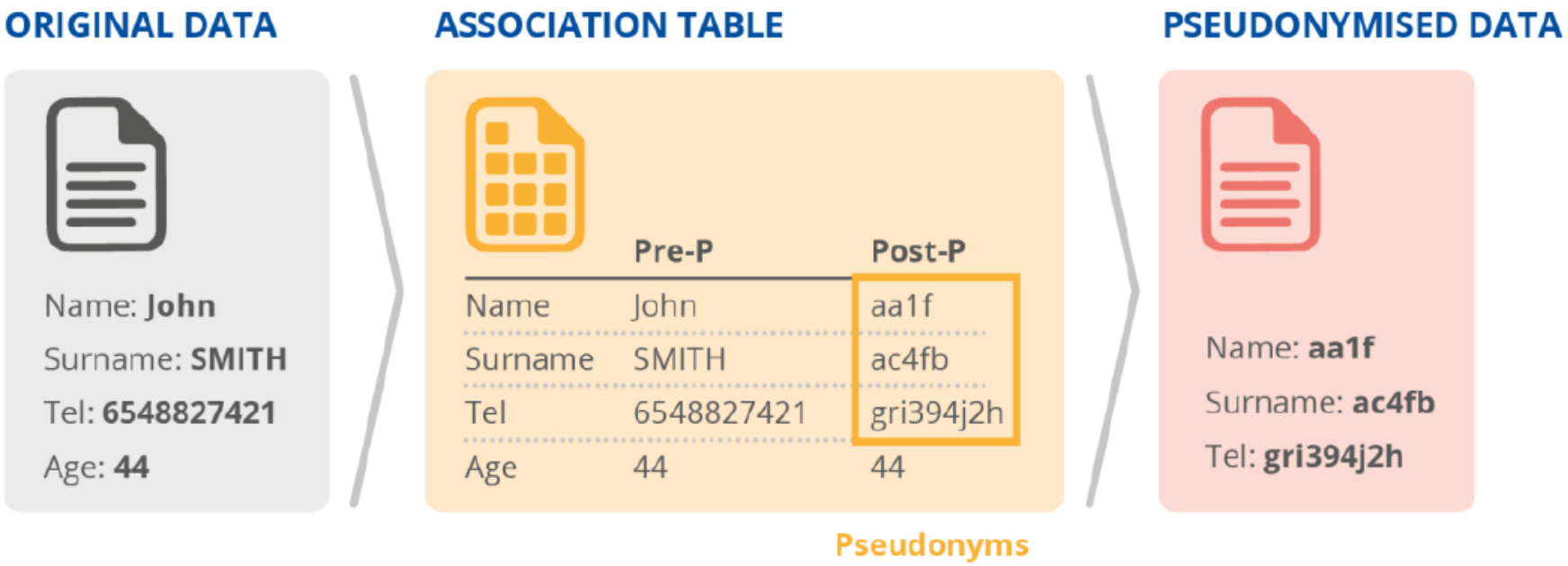
Procedimiento de codificación - GUIA DE ENISA (Agencia de la Unión Europea para la Ciberseguridad): LA ADOPCIÓN DE TÉCNICAS DE SEUDONIMIZACIÓN. EL CASO DEL SECTOR SANITARIO. EJEMPLO.

La seudonimización puede ser desde una opción «sencilla» hasta un proceso muy complejo, tanto a nivel técnico como organizativo. Por este motivo, es realmente importante definir tanto las metas y los objetivos de la seudonimización en cada caso particular, como la operación de tratamiento.

La seudonimización **tiene por objeto proteger** los datos personales ocultando la identidad de las personas en un conjunto de datos, por ejemplo, sustituyendo uno o varios identificadores personales (nombre, la fecha de nacimiento, el número de seguridad social, etc.) por los denominados seudónimos (y protegiendo adecuadamente el vínculo entre los seudónimos y los identificadores iniciales).

- Este vínculo, conocido a menudo como secreto de seudonimización, suele almacenarse en una tabla de correspondencia y puede utilizarse para volver a identificar a la persona asociando los seudónimos a los datos originales.
- Únicamente puede acceder a la tabla de correspondencia la entidad que realizó inicialmente la seudonimización, a la que se suele denominar «entidad de seudonimización».

La seudonimización es una de las distintas **técnicas de «desidentificación»** (como la agregación, la ofuscación, el enmascaramiento, etc.) destinadas a eliminar la asociación entre un conjunto de datos de identificación y el sujeto de los datos → ayuda a **reducir el riesgo de vincula**r datos personales de una persona concreta en diferentes ámbitos de tratamiento de datos (por ej. brecha de los datos personales, la seudonimización dificulta la tarea de asociar los datos vulnerados a la persona titular de los mismos).



Fuente: GUIA DE ENISA – La adopción de técnicas de seudonimización. El caso del sector sanitario.

2. Licitud del tratamiento para fines de investigación clínica:

especial referencia a la publicación de las bases de datos de los Estudios

Licitud del tratamiento para fines de investigación clínica

Art. 6 del **RGPD**:

- **Consentimiento** del interesado.
- Ejecución de un **contrato**.
- Cumplimiento de **obligación legal**.
- Proteger **intereses vitales** del interesado o de otra persona física.
- **Interés público**/ejercicio de poderes públicos conferidos al responsable.
- Satisfacción de **intereses legítimos** perseguidos por responsable o tercero.

Art. 8 **LOPDGDD** establece el tratamiento de datos por **obligación legal, interés público** o **ejercicio de poderes públicos**:

- Cumplimiento de una **obligación legal** exigible al responsable cuando lo prevea una norma de Derecho UE o norma con rango de ley.
- Misión realizada en **interés público** o ejercicio de poderes públicos cuando derive de una competencia atribuida por una norma con rango de ley.

Y además, cuando se traten datos de categorías especiales (por ejemplo, salud, genéticos, etc.) debe concurrir alguna de las **circunstancias del art. 9.2 RGPD** para levantar la prohibición general de tratamiento de este tipo de datos personales (indicada en el articulo 9.1 RGPD): **consentimiento explícito**; protección **intereses vitales** del interesado; fines de **medicina preventiva o laboral**, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social; razones de **interés público en el ámbito de la salud pública**, etc.

El **Dictamen 3/2019, del Comité Europeo de Protección de Datos (CEPD)**, recoge criterios interpretativos respecto de dichas bases jurídicas en relación con el Reglamento 536/2014 sobre ensayos clínicos de medicamentos (REC) y, en particular, para el tratamiento de datos de ensayos clínicos con fines de investigación en salud, que promueven el desarrollo de estas de actividades. El CEPD considera que no todas las operaciones de tratamiento relacionadas con el «uso primario» de datos de ensayos clínicos persiguen los mismos fines y se ajustan a la misma base jurídica.

Licitud del tratamiento para fines de investigación clínica

(**Dictamen CEPD continuación**) El CEPD considera que hay que distinguir entre:

Operaciones de tratamiento relacionadas exclusivamente con actividades de investigación

- Consentimiento explícito * → Art. 9.2.a RGPD Consentimiento explícito
- Interés público → Art. 9.2.i RGPD Interés público
- Interés Legítimo → Art. 9.2.j RGPD Investigación

Operaciones de tratamiento relacionadas con fines de protección de la salud, niveles de calidad y seguridad de los medicamentos generando datos fiables y sólidos (fines relacionados con la fiabilidad y la seguridad)

- Obligación legal → Art.9.2.i RGPD para tratamiento de categorías especiales (razones de interés público en el ámbito de la salud pública)

*Dictamen 3/2019 sobre las preguntas y respuestas acerca de la relación entre el Reglamento sobre ensayos clínicos y RGPD (desequilibrio poder entre promotor/investigador y participantes).

Licitud del tratamiento para fines de investigación clínica

Disposición Adicional 17ª de la Ley Orgánica 3/2018, apartado segundo - para el tratamiento de datos personales en INVESTIGACIÓN EN SALUD y, en particular, biomédica.

Cuando los proyectos revistan un evidente interés para la salud pública o de terceros, el consentimiento puede ceder:

- ✓ no consentimiento en situaciones de excepcional relevancia y gravedad para la salud publica (incluso manteniéndose los datos de identificación del sujeto fuente);

- ✓ 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;

- ✓ no consentimiento siempre que:
  - los datos seudonimizados;
  - separación técnica y funcional entre quien realice la investigación y quien seudonimice;
  - confidencialidad.

Licitud del tratamiento para fines de investigación clínica

Datos de investigación

Los **datos de investigación** o researchdata:

- ✓ Todo aquel material que ha sido registrado durante la investigación, reconocido por la comunidad científica y que sirve para certificar los resultados de la investigación que se realiza.

- ✓ Pueden ser:
  - ❑ Numéricos, descriptivos o visuales.
  - ❑ Encontrarse en estado bruto o analizados, pueden ser experimentales u observacionales.

- ✓ Los datos incluyen: cuadernos de laboratorio, cuadernos de campo, datos de investigación primaria (incluidos los datos en papel o en soporte informático), cuestionarios, cintas de audio, videos, desarrollo de modelos, fotografías, películas, y las comprobaciones y las respuestas de la prueba.

- ✓ No son considerados datos finales de investigación: notas de laboratorio, sets de datos parciales, análisis preliminares, borradores de trabajos, planes para investigaciones futuras, informes que han tenido un proceso de revisión por pares, comunicaciones con colegas, objetos físicos, ejemplares de laboratorio.

- ✓ **Los datos abiertos (open data) son datos que pueden ser utilizados, reutilizados y redistribuidos libremente por cualquier persona, y que se encuentran sujetos, cuando más, al requerimiento de atribución y de compartirse de la misma manera en que aparecen. Este concepto está relacionado con el de Open Science (Ciencia abierta)**.

Licitud del tratamiento para fines de investigación clínica

Datos de investigación

Open research science es un concepto amplio que significa acceso abierto a la ciencia y que engloba:

- Open Access: suele referirse al acceso abierto a las publicaciones;
- Open research data: es el acceso abierto a los datos de investigación.

¿Es obligatorio poner en acceso abierto la investigación financiada con fondos públicos? Sí:

A nivel europeo: programas Horizonte 2020 (años 2014-2020) y Horizonte Europa (2021-2027).

*El **horizonte 2020** ha sido hasta la fecha el programa de investigación e innovación más ambicioso puesto en marcha por la Unión Europea. Los beneficiarios de estas subvenciones estaban obligados a poner en acceso abierto en un repositorio los resultados de la investigación (publicaciones y datos). Su art. 29.3 establecía la obligación de los investigadores de desarrollar un Plan de Gestión de datos (PGD) y de depositar los resultados en un repositorio de datos.

***Horizonte Europa** es el programa marco de investigación e innovación (I+I) de la Unión Europea (UE) para el período 2021 - 2027. Es un instrumento fundamental para llevar a cabo las políticas de I+D+I de la UE. Con este nuevo programa marco se continúa con el apoyo a los principios de la Ciencia Abierta con el objetivo de lograr una mejor difusión y explotación de los resultados de investigación e innovación, así como apoyar a la participación activa de la sociedad:

- ❑ Acceso abierto obligatorio para las publicaciones: los beneficiarios se asegurarán de que ellos o los autores conservan los derechos de la propiedad intelectual necesarios para cumplir los requisitos de acceso abierto.
- ❑ Garantizar el acceso abierto a los datos de investigación: de conformidad con el principio «tan abierto como sea posible y tan cerrado como sea necesario»; plan obligatorio de gestión de datos para datos FAIR (fáciles de encontrar, accesibles, interoperables y reutilizables) y datos de investigación abiertos.
- ❑ Apoyo a las habilidades de los investigadores en materia de ciencia abierta, así como sistemas de recompensa.
- ❑ Uso de la Nube Europea de la Ciencia Abierta (https://digital-strategy.ec.europa.eu/es/policies/open-science-cloud).

Licitud del tratamiento para fines de investigación clínica

Datos de investigación

A nivel nacional:

*__Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación__. La llamada Ley de la Ciencia de 2011 obliga a poner en acceso abierto los resultados de la investigación (publicaciones y datos) financiada con fondos de los Presupuestos Generales del Estado. Lo vemos a continuación.

*__Real Decreto 576/2023, de 4 de julio__, por el que se modifican el Real Decreto 99/2011, de 28 de enero, por el que se regulan las enseñanzas oficiales de doctorado; el Real Decreto 1002/2010, de 5 de agosto, sobre expedición de títulos universitarios oficiales; y el Real Decreto 641/2021, de 27 de julio, por el que se regula la concesión directa de subvenciones a universidades públicas españolas para la modernización y digitalización del sistema universitario español en el marco del Plan de Recuperación, Transformación y Resiliencia. El Real Decreto indica que las tesis aprobadas en cada Universidad deben depositarse en un repositorio institucional.

Si bien estas políticas de requerimiento están centradas principalmente en la publicación en abierto de los artículos de revistas y los datos de investigación, la publicación en Acceso Abierto contempla también, con las peculiaridades propias, la publicación en abierto de las contribuciones en congresos y sus actas, conferencias científicas, los libros o capítulos de libros y, muy especialmente, los Recursos Educativos en Abierto (REA).

Licitud del tratamiento para fines de investigación clínica

Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación.

Artículo 1. Objeto.

Esta ley establece el marco para el fomento de la investigación científica y técnica y sus instrumentos de coordinación general, con el fin de contribuir a la generación, difusión y transferencia del conocimiento para resolver los problemas esenciales de la sociedad. El objeto fundamental es la promoción de la investigación, el desarrollo experimental y la innovación como elementos sobre los que ha de asentarse el desarrollo económico sostenible y el bienestar social.

Artículo 11. Sistema de Información sobre Ciencia, Tecnología e Innovación.

1. Se crea, bajo la dependencia del Ministerio de Ciencia e Innovación, el Sistema de Información sobre Ciencia, Tecnología e Innovación, como instrumento de captación de datos y análisis para la elaboración y seguimiento de la Estrategia Española de Ciencia, Tecnología e Innovación, y de sus planes de desarrollo.

(…)

3. Los agentes del Sistema Español de Ciencia, Tecnología e Innovación cooperarán aportando información sobre sus actuaciones en materia de investigación científica y técnica, que se les solicitará de acuerdo con los criterios aprobados por el Consejo de Política Científica, Tecnológica y de Innovación. La información a aportar también podrá abarcar las actuaciones con el sector privado. Dichos criterios deberán respetar el ámbito competencial de las distintas Administraciones y la normativa sobre confidencialidad y privacidad de la información y de protección de datos de carácter personal.

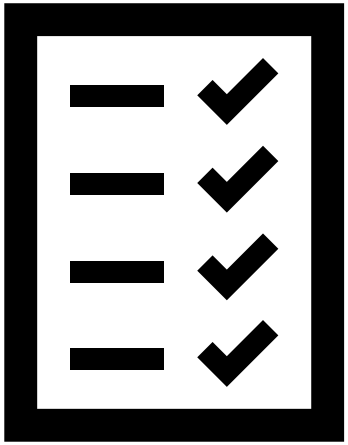
Licitud del tratamiento para fines de investigación clínica

Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación.

Artículo 15. Deberes del personal investigador.

1. Los deberes del personal investigador que preste servicios en universidades públicas, en Organismos Públicos de Investigación de la Administración General del Estado o en organismos de investigación de otras Administraciones Públicas serán los siguientes: (…)

l) Adoptar las medidas necesarias para el cumplimiento de la normativa aplicable en materia de protección de datos y de confidencialidad.



Licitud del tratamiento para fines de investigación clínica

Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación.
Artículo 37. Ciencia abierta.

1. Los agentes públicos del Sistema Español de Ciencia, Tecnología e Innovación impulsarán que se haga difusión de los resultados de la actividad científica, tecnológica y de innovación, y que los resultados de la investigación, incluidas las publicaciones científicas, datos, códigos y metodologías, estén disponibles en acceso abierto. El acceso gratuito y libre a los resultados se fomentará mediante el desarrollo de repositorios institucionales o temáticos de acceso abierto, propios o compartidos.

2. El personal de investigación del sector público o cuya actividad investigadora esté financiada mayoritariamente con fondos públicos y que opte por diseminar sus resultados de investigación en publicaciones científicas, deberá depositar una copia de la versión final aceptada para publicación y los datos asociados a las mismas en repositorios institucionales o temáticos de acceso abierto, de forma simultánea a la fecha de publicación.

3. Los beneficiarios de proyectos de investigación, desarrollo o innovación financiados mayoritariamente con fondos públicos deberán cumplir en todo momento con las obligaciones de acceso abierto dispuestas en las bases o los acuerdos de subvención de las convocatorias correspondientes. Los beneficiarios de ayudas y subvenciones públicas se asegurarán de que conservan los derechos de propiedad intelectual necesarios para dar cumplimiento a los requisitos de acceso abierto.

4. Los resultados de la investigación disponibles en acceso abierto podrán ser empleados por las Administraciones Públicas en sus procesos de evaluación, incluyendo la evaluación del mérito investigador.

Licitud del tratamiento para fines de investigación clínica

(continuación)

5. El Ministerio de Ciencia e Innovación facilitará el acceso a los repositorios de acceso abierto y su interconexión con iniciativas similares nacionales e internacionales, promoviendo el desarrollo de sistemas que lo faciliten, e impulsará la ciencia abierta en la Estrategia Española de Ciencia, Tecnología e Innovación, reconociendo el valor de la ciencia como bien común y siguiendo las recomendaciones europeas en materia de ciencia abierta.

Además del acceso abierto, y siempre con el objetivo de hacer la ciencia más abierta, accesible, eficiente, transparente y beneficiosa para la sociedad, los Ministerios de Ciencia e Innovación y de Universidades, cada uno en su ámbito de actuación, así como las Comunidades Autónomas en el marco de sus competencias, promoverán también otras iniciativas orientadas a facilitar el libre acceso y gestión de los datos generados por la investigación (datos abiertos), de acuerdo a los principios internacionales FAIR (sencillos de encontrar, accesibles, interoperables y reutilizables), a desarrollar infraestructuras y plataformas abiertas, a fomentar la publicación de los resultados científicos en acceso abierto, y la participación abierta de la sociedad civil en los procesos científicos, tal como se desarrolla en el artículo 38.

6. Lo anterior será compatible con la posibilidad de tomar las medidas oportunas para proteger, con carácter previo a la publicación científica, los derechos sobre los resultados de la actividad de investigación, desarrollo e innovación, de acuerdo con las normativas nacionales y europeas en materia de propiedad intelectual e industrial, obtenciones vegetales o secreto empresarial.

Licitud del tratamiento para fines de investigación clínica

Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación.

Disposición adicional novena. Protección de datos de carácter personal.

1. Lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, y en el Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) será de aplicación al tratamiento y cesión de datos derivados de lo dispuesto en esta ley.

2. Los agentes públicos de financiación y de ejecución deberán adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, tratamiento o acceso no autorizados.

3. El Gobierno regulará, previo informe de la Agencia Española de Protección de Datos, el contenido académico y científico de los currículos del personal docente e investigador de Universidades y del personal investigador que los agentes de financiación y de ejecución pueden hacer público sin el consentimiento previo de dicho personal.

Licitud del tratamiento para fines de investigación clínica

En este sentido…si bien en los proyectos de financiación pública existe una ley que ampara la publicación de los datos asociados a la investigación, esta misma ley obliga al cumplimiento de lo establecido en la normativa de protección de datos, por lo que, **para llevar a cabo esa comunicación de datos, en caso de que la información que se vaya a publicar no se encuentre agregada** (es decir, sea anonimizada) porque impidiera cumplir el fin de dicha publicación, **se deberán adoptar las siguientes medidas en cuanto a protección de datos**:

- Cumplir con las instrucciones de la normativa en la cual se ampare la publicación de los datos y publicar únicamente la información que sea necesaria.
- La información que se debe recoger de los sujetos debe ser consistente con los objetivos del estudio. Se deben sopesar los datos que se recogen, principalmente cuando se refieren a información especialmente sensible (salud, adicción a sustancias nocivas, vida sexual, etc.).
- Incluir este aspecto en el Plan de Gestión de Datos o Data Management Plan: desde el comienzo del proyecto de investigación se debe definir el tratamiento que recibirán los datos que se utilicen durante la investigación.
- Informar al interesado de la publicación de sus datos, en caso de que no se vayan a publicar únicamente datos agregados (estadísticas).
- Cumplimiento de los Principios FAIR (fáciles de encontrar, accesibles, interoperables y reutilizables).
- Realizar las publicaciones en sitios seguros, como en las revistas en las que se publican las bases de datos en acceso abierto. En estos casos se deben cumplir la exigencias de publicación de cada revista (**en ocasiones se exige que los datos publicados sean anónimos, pero, en todo caso, deben encontrarse codificados o seudonimizados**), en consonancia con el cumplimiento de la normativa relativa a protección de datos.

3. Transferencias internacionales de datos

Conceptos básicos sobre las Transferencias internacionales de datos

«tratamiento transfronterizo»:
a) el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o
b) el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro;

Por tanto, las **comunicaciones de datos a destinatarios establecidos en países fuera del Espacio Económico Europeo** se consideran Transferencias internacionales de datos (en adelante "**TID**").

Supuestos más habituales:

- Servicios de atención al cliente;
- Alojamiento de datos en un servidor ubicado en otro estado (Cloud Computing), por ejemplo, el eCRD;
- Transferencias bancarias alrededor del mundo o empresas de envío de dinero;
- Asistencia sanitaria internacional;
- Comunicación de muestras en proyectos de investigación;
- Envío de datos de empleados o de clientes por todo el mundo en los Grupos empresariales con sedes en distintos estados.

A continuación veremos las garantías más habituales para TID en casos de investigación

Garantías para las Transferencias internacionales de datos

Transferencias basadas en una decisión de adecuación

Cuando las entidades receptoras de los datos se encuentren en un país, 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**. Hasta la fecha los países y territorios que han sido declarados como adecuados son los siguientes:

- **Suiza**. Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000
- **Canadá**. Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos
- **Argentina**. Decisión 2003/490/CE de la Comisión, de 3 de junio de 2003
- **Guernsey**. Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003
- **Isla de Man**. Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004
- **Jersey**. Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008
- **Islas Feroe**. Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010
- **Andorra**. Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010
- **Israel**. Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011
- **Uruguay**. Decisión 2012/484/UE, de la Comisión, de 21 de agosto de 2012
- **Nueva Zelanda**. Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012
- **Japón**. Decisión de 23 de enero de 2019
- **Reino Unido**. Decisión de 28 de junio de 2021
- **República de Corea**. Decisión de 17 de diciembre de 2021
- **EU- USA Data Privacy Framework**. Decisión de 10 de julio de 2023

Garantías para las Transferencias internacionales de datos

Transferencias basadas en una decisión de adecuación: Especial mención USA

El TJUE invalida el acuerdo Privacy Shield para la transferencia de datos entre la Unión Europea y los EEUU

16-7-2020 | Tribunal de Justicia de la Unión Europea

10 min

Tras invalidar el primer acuerdo sobre transferencia de datos entre la UE y los Estados Unidos, el Tribunal invalida también el acuerdo "Privacy Shield" que le sustituyó. Por el contrario, se declara la validez de la Decisión de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países.

Fuente: diariolaley 16-7-2020

Garantías para las Transferencias internacionales de datos

Transferencias basadas en una decisión de adecuación: Especial mención USA

El **Tribunal de Justicia de la Unión Europea (TJUE) invalidó la Decisión (UE) 2016/1250 de la Comisión**, de 12 de julio de 2016, conocida como el **Escudo de Privacidad (Privacy Shield)** para las transferencias de datos a los Estados Unidos (en adelante "EEUU").

Hasta ese momento, las **transferencias internacionales de datos realizadas a empresas estadounidenses que estaban adheridas al Privacy Shield** estaban "**permitidas**" por las autoridades de protección de datos por considerar que esas empresas ofrecían garantías respecto al tratamiento de datos personales procedentes de EEE.

En **julio de 2020 el Tribunal de Justicia de la Unión Europea (TJUE) invalidó el acuerdo** entre la Unión Europea (UE) y Estados Unidos (EEUU), conocido como Privacy Shield o Escudo de Privacidad, para la transferencia de datos personales desde Europa a empresas estadounidenses adheridas a dicho Escudo (https://www.privacyshield.gov/list).

El TJCE consideró que el Derecho estadounidense (en particular, el artículo 702 de la Ley de Vigilancia de la Inteligencia Extranjera "Ley FISA", la Orden Ejecutiva 12333 y la Ley de la Nube "Cloud Act") no garantiza un nivel de protección sustancialmente equivalente al de la UE.

Garantías para las Transferencias internacionales de datos

Transferencias basadas en una decisión de adecuación: Especial mención USA

Press release | 10 July 2023 | Brussels

Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows

Today, the European Commission adopted its adequacy decision for the EU-U.S. Data Privacy Framework. The decision concludes that the United States ensures an adequate level of protection – comparable to that of the European Union – for personal data transferred from the EU to US companies under the new framework. On the basis of the new adequacy decision, personal data can flow safely from the EU to US companies participating in the Framework, without having to put in place additional data protection safeguards.

Fuente: An official website of the European Union

Garantías para las Transferencias internacionales de datos

Nuevas Cláusulas Contractuales Tipo adoptadas por la Comisión

Cláusulas estándar aprobadas por la Comisión Europea que deben incluirse en los contratos de transferencias internacionales de datos, cuando estas se realizan entre una organización sita en un país del Espacio Económico Europeo y una de fuera del EEE. **Nuevas cláusulas contractuales tipo:**
El 7 de junio de 2021, se publicó en el Diario Oficial de la Unión Europea el **nuevo modelo** de Cláusulas Contractuales Tipo (CCT) para las **transferencias internacionales de datos fuera del Espacio Económico Europeo**, mediante las cuales se pretende **actualizar las medidas de protección de datos y seguridad** a las que deben someterse estas transferencias.

Este n**uevo modelo**:

- ✓ **Se adapta al RGPD** incorporando el **principio de responsabilidad proactiva** o «accountability».

- ✓ Tiene en cuenta los **criterios expresados**:
  - ✓ (i) en la sentencia del Tribunal de Justicia de la Unión Europea de 16 de julio de 2020 (conocido como **Schrems II**), que invalidó el acuerdo Privacy;
  - ✓ (ii) las **Recomendaciones adoptadas por el Comité** Europeo de Protección de Datos.

Módulos:

1. **Primer módulo**: regula transferencias **entre responsables** de datos;
2. **Segundo módulo**: regula transferencias **desde un responsable a un encargado**;
3. **Tercer módulo**: regula transferencias **entre encargados**;
4. **Cuarto modulo**: regula transferencias cuando se producen **desde un encargado a un responsable**.

Garantías para las Transferencias internacionales de datos

Nuevas Cláusulas Contractuales Tipo adoptadas por la Comisión

Obligaciones al importador:

- Obligación de **notificar al exportador** de datos si, por algún motivo o cambio en la legislación de su país, la situación respecto a la **posibilidad de que autoridades públicas accedan a la información** objeto de la transferencia se ha visto incrementada;

- Deber de **comunicar al exportador** de los datos los **requerimientos legales de divulgación de datos** personales que haya recibido;

- **Indicar las medidas técnicas y organizativas** que implementará para garantizar la seguridad de los datos;

- **Notificar al exportador** su **imposibilidad de cumplir con los requisitos establecidos en las CCT**, con la consecuente obligación del exportador de suspender la transferencia de datos, salvo que el exportador pueda implementar medidas apropiadas (por ejemplo, medidas técnicas u organizativas incluidas en las Recomendaciones del CEPD) para hacer frente a esta situación.

Muchas gracias por su atención

Natalia Olivares Álvarez
natalia.olivares@alaroavant.com

Sarai Nieto Sánchez
sarai.nieto@alaroavant.com

alaro avant
Seguridad de la Información