UNIVERSIDAD DE BURGOS

GUIA DE AYUDA AL INVESTIGADOR

1.- ¿Qué es un dato personal?

El RGPD los define así:

> «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

Debemos tener en cuenta que el elemento determinante es la "identificabilidad" de una persona. En el momento en el que en un contexto en el que podamos vincular cualquier información a una persona estaremos tratando datos. Por ejemplo, si somos capaces de vincular "pie pronador" en un estudio biomecánico con determinadas personas.

Hay datos que por su naturaleza merecerán una especial protección:

- «datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;
- «datos genéticos»: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;
- «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

En todos estos casos RGPD impone obligaciones adicionales en términos de base legal para los tratamientos, análisis de riesgos para los derechos de las personas y medidas de cumplimiento normativo aplicables.

2.- ¿Debe aplicarse la normativa a los datos seudonimizados?

Sí, los datos seudonimizados siguen siendo datos personales en el contexto del Reglamento General de Protección de Datos:

> «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;

La razón para ello está en la posibilidad de re-identificar a las personas.

3.- ¿Cuándo trato datos personales?

La definición de tratamiento es particularmente extensiva en el RGPD y alcanza a prácticamente cualquier operación que se realice con los datos tanto en el mundo analógico como en el digital:

> «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;

Además, podemos integrar los datos en bases de datos, o ficheros:

> «fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

Del mismo modo que existen categorías de datos a los que se protege especialmente por su sensibilidad, hay tratamientos a los que el RGPD concede un especial valor. Estos tratamientos, vinculados al análisis de las personas son cada vez más frecuentes en el uso de la analítica de datos y requieren de tareas adicionales como el desarrollo de una evaluación de impacto relativa a la protección de datos.

4.- ¿Qué es un tratamiento?

Si consideramos la definición del RGPD, se observa que prácticamente cualquier manipulación de datos personales es un tratamiento:

> «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;

Además, existen tratamientos como la elaboración de perfiles para los que el RGPD incorpora obligaciones adicionales como, por ejemplo, desarrollar una evaluación de impacto en la protección de datos:

> «elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;

Este tipo de tratamientos podría ser frecuente en el ámbito de la investigación en psicología, sociología o marketing, entre otros ámbitos.

Por otra parte, esos tratamientos pueden determinar la construcción de entornos complejos y sistematizados, -de sistemas de información-, que en la terminología del RGPD se denominan ficheros:

> «fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

5.- ¿Quién es el responsable cuando tratamos datos personales en una investigación?

El responsable podría definirse como aquella persona que decide para qué y cómo se van a usar los datos:

> «responsable del tratamiento» o «responsable»: 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 el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

El concepto amplio de la definición permite considerar como responsable de los tratamientos de datos personales en una investigación a la organización cuando las decisiones las adoptan personas adscritas a las mismas, siempre que se respeten las condiciones previstas en el protocolo para investigación con datos personales. Las decisiones de tratamiento que no respeten los procedimientos generarán responsabilidad individual a la persona infractora.

6.- ¿Y si la investigación la encomienda otra entidad?

Cuando el universo de datos, las metodologías de análisis y los fines específicos de la investigación los defina personal investigador concretándose la relación en una mera entrega de resultados la organización a la que pertenezca será responsable de los eventuales tratamientos.

La otra entidad en virtud de un contrato para realizar una investigación también podría asumir el rol del llamado encargado del tratamiento. En tales casos se determinarán específicamente las reglas de cumplimiento normativo.

7.- ¿Qué es un encargado del tratamiento?

El RGPD lo define así:

«encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento; Cuándo necesitamos usar un recurso externo de otra entidad para almacenar o procesar datos el proveedor es nuestro encargado. Cuando un investigador desarrolla por contrato una investigación cuyos datos, finalidades y objetivos son definidos por otra entidad, la otra entidad podría ser considerada encargada del tratamiento en algunos casos.

8.- Si se seudonimiza o anonimiza la información ¿no hay datos?, ¿debo aplicar este PROTOCOLO?

La seudonimización hace posible que parte de los que acceden a la información no sean capaces de reidentificar.

> «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;

Pero, para la organización, o para quién tenga la capacidad de hacerlo, siguen siendo datos personales y, por tanto, es necesario aplicar las cautelas y garantías que prevé la legislación.

> (26) 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.

Ahora bien, RGPD no se aplicará cuando los datos se hayan anonimizado completamente:

> (26) (…) Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por lo tanto los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación.

Por tanto, para que exista la anonimización debe ser irreversible para cualquier tercero sin un esfuerzo desproporcionado. Por tanto, quienes investiguen con datos anonimizados deben garantizar la aplicación de las previsiones de este PROTOCOLO en esta materia.

9.- ¿El RGPD nos prohíbe investigar con datos?

Todo lo contrario. En distintos considerandos y, singularmente en los artículos 9 y 89 RGPD se sientan las bases para hacer posible la investigación. Además, la disposición adicional decimoséptima sobre tratamientos de datos de salud de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales regula la investigación en salud y biomédica. Pero ello exige asegurarse del cumplimiento de las condiciones que legitiman la investigación y la adopción de las medidas necesarias paras garantizar los derechos de las personas.

10.- ¿Qué es la responsabilidad proactiva?

El Reglamento General de Protección de Datos obliga a las entidades a definir procedimientos que aseguren el cumplimiento de sus previsiones. Esto implica que **"no basta con informar y obtener el consentimiento de las personas"**, es necesario definir procesos de gestión integrales,

dirigidos a asegurar que se cumplen las leyes. Ello tiene consecuencias muy directas para la gestión y ordenación de la investigación:

a) Registro de las actividades de tratamiento.

Todos los tratamientos deben ser conocidos y documentados. La Ley nacional incluso prevé su publicación.

b) Garantía de los principios de protección de datos.

Debe asegurarse un tratamiento leal y lícito, justificar la base legal que lo legitima, y garantizar los derechos a la transparencia y los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición al tratamiento.

c) Protección de datos desde el diseño y por defecto.

La investigación, tanto en sus procesos como en su caso en el desarrollo de software o hardware, debe asegurar:

- La definición adecuada de los tipos de datos y el volumen necesario de los mismos (protección de datos por defecto).
- Que cualquiera de las especificaciones de la investigación, -formales o materiales, procedimentales o técnicas, y organizativas y de personal-, sea capaz de cumplir con el RGPD y garantizar los derechos de las personas concernidas (protección de datos desde el diseño).

d) Seguridad.

Para garantizar el derecho fundamental a la protección de datos la seguridad cumple una misión instrumental esencial.

11.- ¿Qué son las trasferencias internacionales?

Estas se producen cuando para realizar el tratamiento los datos son necesarias una transmisión de los mismos fuera del territorio del Espacio Económico Europeo.

12.- ¿Existen requisitos específicos para la investigación con datos en salud y biomédica?

Si, esta cuestión se regula en la disposición adicional decimoséptima sobre tratamientos de datos de salud de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. En esta norma se prevé:

- Aplicar la legislación específica al área que corresponda (por ejemplo la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica).
- La presencia de una base jurídica de legitimación para el tratamiento, en los términos previstos en la legislación sobre usos de la historia clínica y, la legislación específica, por ejemplo, en materia de ensayos clínicos.
- Adoptar medidas de seguridad.

▪ Revisar en relación con la participación de terceros:

- Que se han definido las relaciones entre todas las partes en consorcios de investigación y en particular los supuestos de corresponsabilidad en el tratamiento.
- Que se han previsto, en caso de existencia de prestadores de servicios externos, las condiciones previstas para el encargado del tratamiento.

▪ Asegurar la licitud en la finalidad de la investigación. La finalidad podrá abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora.

▪ Asegurar la existencia de consentimiento para la reutilización de datos procedentes de ensayos clínicos o la identificación en los restantes casos del origen de los datos en una investigación y la justificación de su uso para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial. En estos casos, deberá aportarse la metodología de cumplimiento del deber de transparencia (políticas de privacidad).

▪ La verificación de los requisitos exigibles en materia de protección de datos a la investigación con datos personales seudonimizados en el ámbito de la salud y la investigación biomédica:

1.º Una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación.

2.º Que los datos seudonimizados únicamente sean accesibles al equipo de investigación cuando:

i) Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.

ii) Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados.

3.º En su caso, los procedimientos previstos para la reidentificación de los datos en su origen, cuando con motivo de una investigación que utilice datos seudonimizados, 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.

▪ Verificar que en los tratamientos con fines de investigación en salud pública y, en particular, biomédica se ha realizado o se prevé realizar una evaluación de impacto que determine los riesgos derivados del tratamiento.

▪ Verificar la designación de un representante legal establecido en la Unión Europea, conforme al artículo 74 del Reglamento (UE) 536/2014, si el promotor de un ensayo clínico no está establecido en la Unión Europea. Dicho representante legal podrá coincidir con el previsto en el artículo 27.1 del Reglamento (UE) 2016/679.

▪ Verificar la investigación científica responde a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica.