Un aspecto muy importante del proyecto de investigación es el concerniente a la protección de los datos personales a utilizar en la misma. Esta protección es especialmente relevante en caso de que se tenga planificado recoger datos personales relativos a algún tipo de colectivo vulnerable.

Concepto de dato personal

Son **datos personales** "toda información sobre una persona física identificada o identificable; 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" (Art. 4.1 RGPD[1]). Por lo tanto, dato personal no es solo el nombre y los apellidos de una persona, sino toda información referida a esta o que pueda identificarla.

Concepto de tratamiento

La normativa de protección de datos (RGPD y LOPDGDD[2]) se aplica a los tratamientos de datos personales y no solo a los ficheros. Define el RGPD al **tratamiento** como "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como 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" y al **fichero** como "todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica".

Serán, por tanto, tratamientos de datos personales:

- su recogida mediante impresos o formularios web
- su registro o almacenamiento en un fichero
- su organización o estructuración mediante ordenación, segmentación, filtrado, etc.
- su conservación mediante la realización de copias de seguridad
- su modificación o actualización como la corrección de errores
- su extracción o exportación de datos de una base de datos para un uso puntual
- su consulta o visualización en listados o en pantallas de visualización de datos
- su utilización para los fines para los que se recogieron los datos
- su comunicación por transmisión a un tercero distinto de la universidad o difusión mediante publicación

[1] RGPD: 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)
[2] LOPDGDD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

- su cotejo, acceso o interconexión con otros sistemas para su verificación
- su limitación o bloqueo de los datos para evitar su uso
- su borrado, supresión o destrucción, fundamentalmente cundo dejen de ser de utilidad

La normativa no se aplica a los ficheros, sistema de información o base datos, sino a cada uno de los tratamientos que se realizan sobre los datos personales almacenados en esos ficheros, sistemas de información o bases de datos.

Principios que se deben seguir al tratar datos personales

- **Principio de "licitud, lealtad y transparencia"**, que consiste en que los datos deben ser tratados de manera lícita, leal y transparente con la persona cuyos datos sean tratados.
- **Principio de "limitación de la finalidad"** que implica, por una parte, la obligación de que los datos sean tratados con una o varias finalidades determinadas, explícitas y legítimas y, por otra, que se prohíbe que los datos recogidos con unos fines determinados, explícitos y legítimos sean tratados posteriormente de una manera incompatible con esos fines. No se considera incompatible con los fines iniciales el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. No obstante, la normativa de protección de datos establece para estos tratamientos ulteriores de los datos ciertas condiciones relacionadas con la información al interesado y las condiciones de los tratamientos.
- **Principio de "minimización de datos"**, es decir, que los datos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
- **Principio de "exactitud"**, es decir, los datos deben ser exactos y, si fuera preciso, actualizados, debiendo adoptarse todas las medidas razonables para que se rectifiquen o supriman los datos inexactos en relación con los fines que se persiguen.
- **Principio de "limitación del plazo de conservación"**, que está relacionado con el de minimización. Igual que solo pueden tratarse los datos adecuados, pertinentes y necesarios para una finalidad, la conservación de esos datos debe limitarse en el tiempo al logro de los fines que el tratamiento persigue. Una vez que esas finalidades se han alcanzado, los datos deben ser borrados o, al menos, desprovistos de todo elemento que permita identificar a los interesados.

  No obstante, los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas a fin de proteger los derechos y libertades de los interesados.
- **Principio de "integridad y confidencialidad"**. Básicamente, impone a quienes tratan datos la obligación de actuar 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 con el objetivo de protegerlos frente a cualquier riesgo que amenace su seguridad.
- **Principio de "responsabilidad proactiva"**. Se deberán aplicar medidas técnicas y organizativas apropiadas para garantizar y estar en condiciones de demostrar que el tratamiento de datos personales se lleva a cabo de conformidad con la normativa de protección de datos.

La responsabilidad proactiva implica adoptar medidas que aseguren razonablemente que se está en condiciones de cumplir con estos principios, con los derechos de las personas cuyos datos se tratan y de las garantías que se establecen en la normativa de protección de datos. Entre estas medidas se encuentran:

- Protección de los datos personales desde el diseño
- Protección de datos personales por defecto
- Aplicar medidas de seguridad derivadas del análisis y gestión de los riegos a los que están expuestos los datos
- Realización de evaluaciones de impacto sobre la protección de los datos si el tratamiento de los datos puede suponer un alto riegos para los derechos y libertades de las personas cuyos datos se vayan a tratar

La UCLM establece **medidas técnicas y organizativas apropiadas** para la protección de los datos personales que trata. Entre dichas medidas, se aplican las incluidas en el Esquema Nacional de Seguridad (ENS) para evitar la pérdida, alteración, acceso no autorizado o cualquier otro riesgo que pueda afectar a la privacidad de los datos personales.

Cuando se vayan a tratar datos personales será necesario utilizar exclusivamente los sistemas de información, aplicaciones y herramientas informáticas instruccionales que la UCLM pone a disposición de sus usuarios que incorporarán e implementarán las medidas de seguridad adecuadas a la tipología de datos personales que se vayan a tratar.

Además, antes de iniciar un nuevo tratamiento de datos personales, de su recogida, almacenamiento, comunicación o cualquier otra forma de tratar los datos, será necesario realizar un análisis sobre los riesgos a los que el tratamiento o los datos puedan verse sometidos, tales como el acceso no autorizado y su pérdida, destrucción o daño accidental. En los casos en los que el tratamiento utilice nuevas tecnologías y por su naturaleza, alcance, contexto o fines suponga un alto riesgo para los derechos y libertades de las personas físicas, se realizará una evaluación sobre el impacto que dicho tratamiento tendría sobre la protección de los datos personales.

Tratamiento de datos personales en la investigación

Tratar datos personales en el desarrollo de una investigación supone que debemos cumplir con estos principios. Sin embargo, no se aplican las normas de protección de datos personales cuando los datos que se vayan a tratar están **previamente anonimizados**. Como regla general, siempre que el desarrollo de la investigación lo permita, se utilizarán datos anonimizados, lo que sería la forma más segura de garantizar la privacidad de las personas de las que provienen los datos porque no sería posible su identificación.

No obstante, se debe garantizar que no sería posible que con un esfuerzo razonable se pueda identificar a una persona. En este sentido, existe tres riesgos relacionados con la anonimización:

1. La posibilidad de identificar a una persona por ciertas características únicas dentro del conjunto datos.
2. La posibilidad de establecer relaciones entre los distintos tipos de datos que permitan identificar a una persona.
3. El conjunto de los datos ofrezca información cuya naturaleza permita deducir la identidad de

una persona.

Cuando el objeto de la investigación implique necesariamente conocer la identidad de las personas cuyos datos van a ser tratados, entonces dichos datos se deberán **seudonimizar** o realizar un proceso de disociación de la información personal del resto de información que impida que estos datos se puedan atribuirse a una persona sin utilizar información adicional. Esta información adicional deberá estar separada y sujeta a medidas técnicas y organizativas destinadas a impedir que se pueda identificar a las personas cuyos datos son tratados. Este proceso de seudonimización es reversible y cuando sean necesario se podrá volver a identificar a los sujetos objeto de la investigación a través de dicha información adicional.

El objetivo de la seudonimización es minimizar el tratamiento de los datos personales a lo imprescindible, de tal modo que durante las fases de la investigación en que no sea necesario conocer la identidad de las personas se traten los datos seudonimizados.