Crue-Secretarías Generales

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

Guía para usuarios

Conceptos básicos para el tratamiento de datos personales en el proceso de elaboración de una tesis doctoral, un trabajo de fin de titulación o cualquier otro trabajo académico que realice el alumnado

*Como citar este informe:

Conceptos básicos para el tratamiento de datos personales en el proceso de elaboración de una tesis doctoral, un trabajo de fin de titulación o cualquier otro trabajo académico que realice el alumnado

28 de febrero de 2024

Grupo de Trabajo Delegadas y Delegados de Protección de Datos

Universidades participantes:

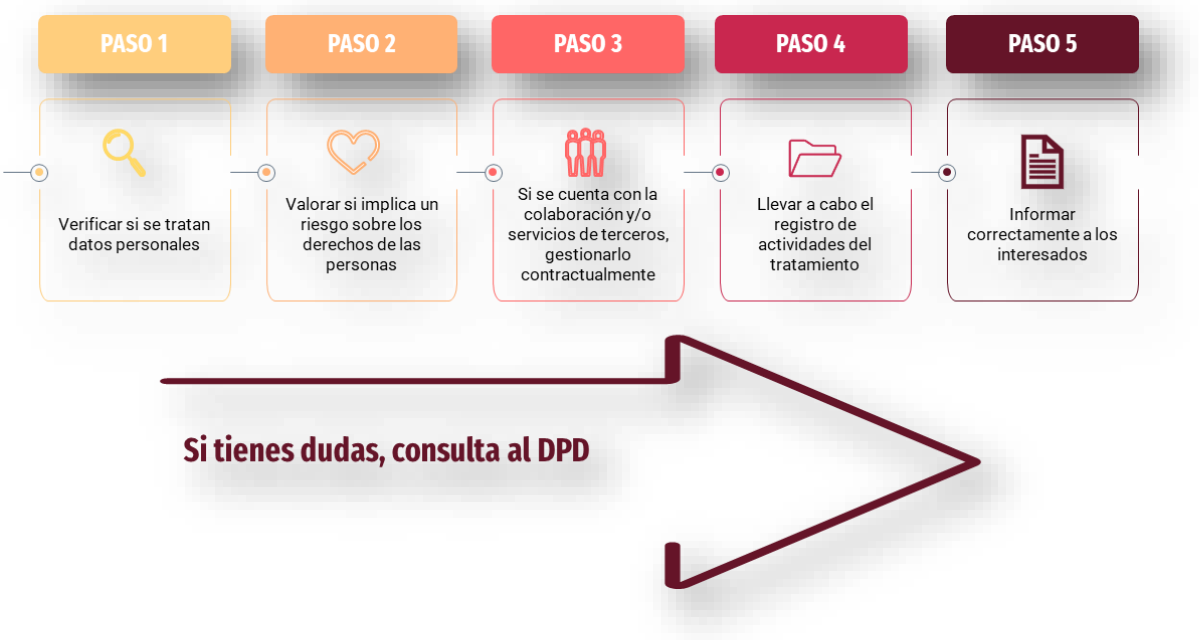
Universidad Pública de Navarra	Javier Zazu
Universidad Carlos III de Madrid	José Furones
Universidad Politécnica de Madrid	Luis Cancela
Universidad Internacional de la Rioja	Miguel Crespo

Índice

I. Alcance del presente documento

Este documento pretende orientar a las personas que dirijan, tutoricen o realicen tesis doctorales, trabajos fin de titulación u otros trabajos académicos (en adelante, la actividad o actividades), sobre cómo identificar si dichos trabajos implican un tratamiento de datos personales y, en caso afirmativo, qué medidas han de adoptar para cumplir con la normativa vigente en esta materia.

El objetivo previsto es la correcta aplicación práctica de las exigencias normativas en materia de protección de datos. Por ello, se ha evitado utilizar en exceso terminología jurídico-técnica que pueda confundir al lector, tratando de apoyar cada uno de sus apartados en ejemplos prácticos.



¡Aviso!

Cualquier duda adicional sobre este documento, respecto del contenido o forma de proceder, se debe consultar con el delegado de protección de datos de su universidad. Su contenido no vincula a los delegados de protección de datos de las universidades, los cuales tienen independencia en el ejercicio de las funciones de asesoramiento y supervisión que les establece la normativa de protección de datos personales.

II. Identificar si la tesis o trabajo implica el tratamiento de datos de carácter personal

Lo primero que debe saber la persona que realice alguna de estas actividades, es si va a tratar o no datos de carácter personal. Para ello, consideramos necesario mencionar ciertos conceptos que le ayudarán a la hora de determinar si nos encontramos o no ante dichos tratamientos.

Dato de carácter personal

Un dato de carácter personal es toda información sobre una persona física identificada o identificable, esto es, toda información relativa a una persona cuya identidad pueda determinarse directa o indirectamente mediante un identificador (nombre, localización, biometría, etc.).

Así mismo, existen categorías especiales de datos con un elevado grado de protección, dado su mayor potencial para afectar gravemente a los derechos de las personas, prohibiéndose, a priori, su tratamiento. Cuando nos encontremos ante el tratamiento de alguno de estos datos, se recomienda consultar al delegado de protección de datos.

Los datos personales de categoría especial son aquellos que revelen el 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.

Procede destacar que un dato que, por sí solo, no permita determinar la identidad de una persona, sí podría contribuir a su identificación en la medida en que se le añada otra información, debiendo considerarse un dato de carácter personal.

Ejemplos:

Los datos de carácter personal se dividen en categorías en base a la información que arrojan. En estas categorías podemos encontrar y clasificar:

- Datos identificativos: nombre y apellidos, DNI o documento de identificación análogo, dirección postal, correo electrónico, teléfono de contacto, fecha de nacimiento, firma, etc.
- Datos relativos a características personales: estado civil, datos de familia, fecha y lugar de nacimiento, edad, sexo, nacionalidad, lengua, características físicas o antropométricas, etc.
- Datos relativos a circunstancias sociales: alojamiento, vivienda, situación familiar, propiedades, posesiones, afiliaciones, estilo de vida, pertenencia a clubes y asociaciones, licencias, permisos, etc.
- Datos académicos: formación, titulación, historial del estudiante, pertenencia a colegios o asociaciones profesionales, etc.
- Datos profesionales: profesión, experiencia laboral, puesto de trabajo, datos no económicos de la nómina, historial del trabajador, numero de la seguridad social, etc.

- Categorías especiales: origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, etc.
- Otros: voz, imagen, ubicación, etc. Se debe tener en cuenta que la imagen y voz, atendiendo al tipo de tratamiento y técnicas implementadas, podrán ser considerados datos biométricos, siendo una categoría especial de datos personales.

Tratamiento de datos de carácter personal

Se entiende por tratamiento de datos de carácter personal cualquier operación de tratamiento sobre los mismos (recogida, análisis, comunicación, destrucción, utilización, etc.) efectuada a través de medios total o parcialmente automatizados, o no automatizados contenidos o destinados a ser incluidos en un fichero.

Ejemplos:

Nos podemos encontrar ante tratamientos de datos personales en cualquiera de los siguientes casos:

- Encuestas, formularios, cuestionarios online o en papel.
- Grabación de entrevistas.
- Registro de sonidos o imágenes relativos a una persona.
- Anotación de información sobre una persona.
- Registro biométrico del físico, los movimientos u otros rasgos de la persona.
- Acceso a archivos con datos personales.
- Contacto y selección de personas de interés.
- Etc.

Adicionalmente, merece una mención aparte el tratamiento de datos anónimos, que no está sujeto a la normativa de protección de datos (sólo tendrán carácter de anónimos aquellos datos que no permitan la identificación o reidentificación de una persona sin requerir el uso de recursos desproporcionados). Adquiere especial relevancia, dentro de los datos anónimos, el uso de bases de datos sintéticas (información generada artificialmente, la cual, no identifica o hace identificable directa o indirectamente a una persona física), como garantía de la anonimización.

Debido al continuo avance de la tecnología, debe asegurarse la certeza de la anonimización, dado que en la práctica los procesos de anonimización resultan altamente improbables. Procede citar algunos ejemplos en los que se califica erróneamente como datos anónimos aquellos datos procedentes de:

- Cuestionarios o formularios gestionados por herramientas on line dónde la propia herramienta gestionará el punto de acceso electrónico (IP) u otros identificadores en línea.

- Procesos de grabación (voz, imagen, referencias informativas, datos biométricos…), aunque no se cite directamente a la persona.

- Anotaciones de información sobre una persona que, aun no resultando identificada directamente, aludan a características singulares de las personas en relación con un grupo (persona más longeva, enfermedades raras, profesiones específicas, rasgos fisiológicos particulares…).
- Acceso a archivos que contengan datos de carácter personal, aun no resultando identificada directamente la persona, atendiendo al contexto previsto en el apartado anterior.
- Utilización de datos de contacto y selección de personas de interés en base a las necesidades de la actividad que se pretende realizar (puesto de trabajo o punto de contacto dentro de una empresa, dirección electrónica profesional…).
- Etc.

Los datos tratados conforme a los ejemplos anteriores no ostentan carácter anónimo. Tampoco se consideran anónimos los datos seudonimizados, que son aquellos datos que ya no pueden atribuirse a un interesado sin utilizar información adicional, pero en el momento que dicha información sea utilizada, se podrá reidentificar al interesado. Por ello, los datos seudonimizados son, en todo caso, datos de carácter personal.

Conclusiones

Atendiendo a las definiciones y ejemplos expuestos, si para el desarrollo de la actividad precisamos interactuar con personas, obtener información de personas o acceder a información que pueda contener o identificar a una persona, con independencia del medio o tecnología empleada, lo más probable es que estemos ante el tratamiento de datos de carácter personal. En este sentido, es necesario que garantice el cumplimiento de la normativa en materia de protección de datos, teniendo como referencia las siguientes normas:

- Reglamento General de Protección de Datos de la UE (RGPD).
- Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

En caso de que dude de si se encuentra ante un tratamiento de datos de carácter personal, consulte con el delegado de protección de datos.

III. Garantías asociadas a un proceso, realización o desarrollo de la actividad

Toda actividad de tratamiento de datos personales debe garantizar, desde su definición, la privacidad de los datos tratados cumpliendo la normativa aplicable en materia de protección de datos según los principios señalados a continuación.

Principios relativos al tratamiento

En el momento en que se inicie el proceso de diseño de una actividad se deberá evaluar si cumple con los principios básicos en materia de protección de datos. Por tanto, se deberá de garantizar que los datos son:

- Tratados de manera lícita, leal y transparente (principio de licitud, lealtad y transparencia).

  Ejemplo: los datos son obtenidos de manera legal, no recurriendo a BBDD o fuentes de datos sin garantías.

- Recogidos con fines determinados, explícitos y legítimos, y no ser tratados ulteriormente de manera incompatible con dichos fines (principio de limitación de la finalidad).

  Ejemplo: la recogida de datos de contacto en el marco de un TFE no puede ser empleada para la generación de una cartera de clientes.

- Adecuados, pertinentes y limitados a lo estrictamente necesario en relación con los fines para los que son tratados (principio de minimización).

  Ejemplo: se deberán usar datos anónimos o anonimizados y, si ello no fuera posible, los datos personales mínimos imprescindibles. Por ejemplo, si realizamos una encuesta en base al nivel formativo de un determinado segmento de la población, no tiene sentido preguntarle por sus convicciones religiosas, datos de salud, etc.

- Exactos y, si fuera necesario, actualizados (principio de exactitud).

  Ejemplo: los datos obtenidos de la propia persona se presumen exactos. En cualquier caso, si tenemos constancia de que algún dato es erróneo o se ha modificado, por ejemplo, una dirección, se deberá de proceder a la corrección y/o actualización.

- Mantenidos de forma que no se permita la identificación de los interesados durante más tiempo del necesario para los fines del tratamiento de los datos personales (limitación del plazo de conservación).

Ejemplo: todo tratamiento de datos está sujeto a un plazo de conservación en base a la finalidad. Una vez que la finalidad ha concluido, dichos datos, atendiendo a los criterios de bloqueo, se deberán de suprimir.

En la realización de encuestas, una vez finalizada y evaluada la actividad docente, los datos de carácter personal se bloquearán. Es decir, se almacenarán de tal forma que serán inaccesibles, salvo que sea necesario ante la petición de una autoridad u organismo público o para la defensa de intereses. Permanecerán bloqueados hasta que se supere el periodo legal previsto en el cual se pueda derivar cualquier tipo de responsabilidad legal. Superado el mismo, se procederá a la eliminación o anonimización total de tales datos.

- 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 (principio de integridad y confidencialidad).

  Ejemplo: la integridad y confidencialidad de los datos se garantizará a través de medidas jurídicas, organizativas y técnicas. Por ejemplo:

  - Si los datos se almacenan en una carpeta compartida, que dicha carpeta se encuentra segregada por roles.
  - Si se van a comunicar los datos en un archivo, que dicho archivo se encuentre cifrado o bloqueado por medio de una contraseña.
  - Si contamos con terceros o proveedores para la realización de la actividad, que se hayan formalizado los debidos contratos.
  - Realización de copias de seguridad.
  - Etc.

- Cumplen con la normativa en materia de protección de datos, teniendo la capacidad de demostrarlo (principio de responsabilidad proactiva).

Análisis de riesgos y evaluación de impacto

Toda actividad de tratamiento de datos de carácter personal conlleva un riesgo sobre los mismos. Dicho riesgo debe ponderarse en base a unos criterios previamente definidos. Por ejemplo, cuando se utilizan tecnologías de reciente creación, se tratan datos a gran escala o se tratan categorías especiales de datos, el riesgo es exponencialmente mayor.

Las evaluaciones de impacto analizan los tratamientos de datos para determinar si la actividad implica un perjuicio superior sobre los participantes que los beneficios que arroja, afectando a sus derechos y libertades, esto es, implicando un mayor riesgo sobre las personas. En estos supuestos, la actividad no se podrá llevar a cabo, salvo que se apliquen medidas adicionales para mitigar el riesgo.

Se deberá de proceder al análisis de riesgos y/o evaluación de impacto, siempre que se lleve a cabo una actividad del tratamiento o se modifique sustancialmente una ya existente.

Para la correcta valoración del riesgo debe acudir al delegado de protección de datos que, de conformidad a su criterio y en cumplimiento de la normativa en materia de protección de datos, procederá a participar en el asesoramiento y supervisión de los análisis de riesgos realizados o, cuando proceda, de las correspondientes evaluaciones de impacto.

Ejemplos:

En el caso de que la actividad implique el tratamiento de datos de categorías especiales, por ejemplo, datos de salud de los participantes, donde atendiendo al volumen de datos recabados, así como al ámbito geográfico, se determina que los tratamientos se realizan a gran escala (p.ej.: se recaban los datos de salud de 1.000.000 de personas de la Comunidad de Madrid). Esta información es tratada a través de herramientas que aplican técnicas de reciente creación o que implican un riesgo, con la intención de obtener un resultado específico en base a unos parámetros previamente definidos.

A priori, esta actividad requiere de la realización de una evaluación de impacto, que determinará si la actividad del tratamiento se puede llevar a cabo en base a las medidas de seguridad que se apliquen para mitigar cualquier tipo de riesgos. Por ejemplo, una medida de seguridad que se podría aplicar es que, antes de que la información sea tratada por estas herramientas, se haya procedido a realizar procesos de anonimización, que bajo ningún concepto implique que esta herramienta saque conclusiones con base en personas determinadas.

Puede consultar la lista de tipos de tratamientos de datos que requieren una evaluación de impacto en el siguiente enlace: https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf.

Bases legales que legitiman el tratamiento

Los datos solo podrán ser tratados cuando exista una base legal que lo permita. La normativa en materia de protección de datos contempla las siguientes:

- Consentimiento del interesado.
- El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte u opera la aplicación de medidas precontractuales.
- El tratamiento es necesario para el cumplimiento de una obligación legal.
- El tratamiento es necesario para proteger intereses vitales.
- El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos.
- El tratamiento es necesario para la satisfacción de un interés legítimo (base legitimadora particularmente concurrente para universidades privadas, empresas y otras entidades privadas).

Habitualmente, la base de legitimación aplicable a estas actividades es el consentimiento, puesto que no suelen concurrir el resto de las bases aludidas.

El consentimiento tiene que cumplir una serie de requisitos para que se considere válido:

- Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos.

- Cuando el tratamiento tenga varios fines, debe darse el consentimiento para cada uno de ellos.
- Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.
- Tiene que ser una manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa (no se permiten casillas premarcadas, oraciones en negativo o la inactividad como consentimiento) el tratamiento de datos personales que le conciernen.

Adicionalmente, es una práctica bastante extendida la de firmar con las personas intervinientes lo que se denomina "Consentimiento informado". Este consentimiento informado, por norma general, informa a la persona de las implicaciones que conlleva que forme parte de la actividad, no siendo un consentimiento en los términos comprendidos en la normativa en materia de protección de datos, sino que actúa como un eximente de responsabilidad. El entendimiento de dicho consentimiento suele limitarse a cuestiones éticas, médicas o de otro tipo sobre la participación en un estudio o proyecto (tiempo invertido, esfuerzo de reflexión, molestias por asistencia...). Sin embargo, hace falta un consentimiento específico en materia de protección de datos, concretamente concerniente al tratamiento de datos personales.

El tratamiento de los datos de carácter personal, a priori, podrá estar basado en las siguientes bases de legitimación:

- Consentimiento del interesado (art. 6.1.a) del RGPD): cuando no resulte otra base de legitimación aplicable.
- Datos necesarios para la ejecución de un contrato (art. 6.1.b) del RGPD): cuando la participación del interesado esté sujeta a unas condiciones particulares, como podrían ser características propias del interesado, cumplimiento de exigencias, plazos, etc.
- Cuando se traten categorías especiales de datos, con base en alguna de las bases de legitimación anteriormente indicadas, la circunstancia que levanta la prohibición del tratamiento será el consentimiento explícito del interesado (art. 9.2.a) del RGPD) o la realización de una actividad de investigación científica o histórica o fines estadísticos (art.9.2.j) del RGPD).

En cualquier caso, el responsable del tratamiento revisará las bases jurídicas que resulten aplicables, pudiendo apreciarse, además de las señaladas, la realización de una misión en interés público (art.6.1.e) del RGPD) o la satisfacción de intereses legítimos en el caso de las universidades privadas (art.6.1.f) del RGPD).

Principio de información

Facilitar la información adecuada es un deber de vital importancia a la hora de gestionar la protección de datos de carácter personal.

- Cuando la información provenga del propio interesado se le tendrá que informar del tratamiento de sus datos de carácter personal en el mismo momento en el que se obtengan y de forma previa a su tratamiento.

- Cuando la información no provenga del propio interesado se le tendrá que informar del tratamiento de sus datos de carácter personal conforme a las previsiones del artículo 14.3 del RGPD.

Independientemente del medio por el cual se lleve a cabo la información, se tendrá que hacer a través de un lenguaje claro y sencillo, de forma concisa, transparente, inteligible y de fácil acceso.

Esta información se puede ofrecer a través de un sistema multicapa o multinivel que garantice la comprensión de los participantes. En este sentido se establecerá:

- **Primera capa**: recogerá la información básica de primer nivel, de forma resumida, que se facilitará en el mismo momento y en el mismo medio en el que se recojan los datos de carácter personal. Deberá contener:

  - La identidad del responsable o persona que va a tratar los datos.
  - La finalidad del tratamiento, es decir, de la actividad que se va a llevar a cabo.
  - La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del RGPD.
  - La posibilidad de acceder a información adicional.
  - Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar.

  Cuando los datos provengan de un tercero, la información básica indicada anteriormente, se le deberá de añadir:

  - Las categorías de datos objeto de tratamiento.
  - Las fuentes de las que procedieran los datos. Es decir, quién nos ha facilita los datos.

- **Segunda capa**: recogerá la información adicional de segundo nivel, donde se detallará de forma pormenorizada el resto de información que no se ha presentado en la primera capa. En términos generales, la información que deberá de aparecer será la siguiente:

  - Los datos identificativos y de contacto del responsable del tratamiento.
  - Los datos de contacto del delegado de protección de datos en su caso.
  - Las finalidades por las que dichos datos de carácter personal van a ser tratados.
  - La base jurídica que permita dicho tratamiento.
  - Los destinatarios a los que se van a facilitar tales datos.
  - La existencia de transferencias internacionales de los datos.
  - El plazo de conservación de los datos personales.
  - En el caso de que la base de legitimación se base en el interés legítimo, se especificará dicho interés.

- El ejercicio de los derechos de los interesados, así como el derecho a retirar el consentimiento en cualquier momento y a presentar una reclamación ante la autoridad de control (AEPD, APDCAT, AVPD y CTPDA).
- La fuente de procedencia de los datos y la categoría de estos.
- La existencia de decisiones automatizadas, incluida la elaboración de perfiles.

Registro de actividades del tratamiento

El registro de actividades del tratamiento (RAT) es un listado de tratamientos que se llevan a cabo por los responsables del tratamiento. Cada universidad organizará ese registro bajo su propio criterio, inventariando los tratamientos de modo que cumplan el RGPD con el grado de generalidad o especificidad que se determine.

Las universidades registrarán todo tratamiento de datos personales que tenga lugar con ocasión de la realización de tesis doctorales y trabajos de fin de estudios. Los estudiantes, de forma conjunta con los directores o tutores académicos, facilitarán la información pertinente para que la Universidad mantenga actualizado el correspondiente registro de las referidas actividades de tratamiento de datos.

Dicho RAT debe de contar con la siguiente información:

- El nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos.

- Los fines del tratamiento.

- Una descripción de las categorías de interesados y de las categorías de datos personales.

- Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales.

- 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 y, en su caso, la documentación de garantías adecuadas.

- Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos.

- Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad, en su caso, tienen que incluir:

    - La seudonimización y el cifrado de datos personales.
    - La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
    - La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

- Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Este RAT, tendrá que llevarse a cabo por escrito y en formato electrónico. Debiendo de estar a disposición de la autoridad de control. En el caso de las universidades públicas, el RAT será público, conforme al artículo 6.bis de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

IV. Personas intervinientes y responsabilidades

Se debe llevar a cabo una **correcta identificación de personas intervinientes, así como las responsabilidades que asumen cada una de ellas**. A continuación, debiendo atender al caso concreto y siendo necesaria la valoración del delegado de protección de datos, se establecen una serie de ejemplos. La información mostrada a continuación solo se puede tener en cuenta a efectos ejemplificativos:

Universidad

La Universidad es el responsable de todos aquellos tratamientos de datos de carácter personal relacionados con la realización del servicio público de la educación superior, que presta mediante la investigación, la docencia y el estudio. En base a esta responsabilidad, la Universidad debe velar por el cumplimiento de la normativa en la elaboración de tesis y trabajos académicos, que supongan un tratamiento de datos personales.

Por tanto, podemos definir a la Universidad como el responsable del tratamiento, en base a que determina los fines y medios de la actividad, con el objetivo de velar por el correcto desarrollo, valoración y evaluación de las actividades llevadas a cabo.

Directores y tutores de la actividad

Los directores o tutores son garantes de que la actividad se lleva a cabo de conformidad a los fines y medios determinados por la Universidad, con la intención de velar por la correcta ejecución de estas.

Por tanto, podemos considerar a los directores y tutores como una extensión de la Universidad, en su calidad de empleados a servicio del responsable del tratamiento. La Universidad debe de garantizar que las actividades o acciones que lleva a cabo son acordes a la normativa. Asimismo, el director o tutor debe comprometerse a cumplirlas y velar por su cumplimento por parte del alumno o doctorando.

Alumno o doctorando

Esta figura puede adquirir una doble connotación en base a las actividades que pretenda realizar sobre los datos de carácter personal:

- Con carácter general, considerando que la Universidad ha determinado los fines y medios del tratamiento mediante las instrucciones y directrices de los directores o tutores, el alumno o doctorando deberá realizar la actividad académica conforme al compromiso adquirido de cumplimento de las citadas instrucciones y directrices.

- De manera adicional, el alumno o doctorando, respecto de la actividad realizada, desde el momento inicial o en un momento posterior, podría querer utilizar los datos de carácter personal para finalidades propias, como podrían ser:

- Investigaciones propias o independientes que quiera llevar a cabo o proseguir en el futuro.
- La publicación de la actividad.
- Compartir los resultados con otras Universidades, empresas o terceros.
- Etc.

En estos supuestos, procederá analizar, en función de las circunstancias concurrentes, qué condición, de entre las explicitadas a posteriori, adquiere el alumno o doctorando:

- **Corresponsable del tratamiento**: si desde el inicio de la actividad ya se preveía este tipo de tratamientos. Se deberá de informar a los participantes de esta situación y de las finalidades para las cuales van a tratar los datos cada una de las partes: Universidad y alumno/doctorando.

  La relación entre el alumno o doctorando con la Universidad, se deberá de regular de forma específica mediante un contrato por escrito. Esta circunstancia supone asunción de responsabilidad también por parte del alumno.

- **Responsable del tratamiento**: si en un momento posterior el alumno o doctorando pretende hacer uso de la información con datos de carácter personal. En este punto, la Universidad deberá de informar a los participantes de esta situación, solicitando su consentimiento para que esa información pueda ser utilizada nuevamente por el alumno o doctorando. A su vez, sobre las personas que hayan consentido, el alumno o doctorando deberá de informar sobre el nuevo tratamiento de los datos de los participantes.

  ***Nota**: en caso de duda sobre el tipo de responsabilidad aplicable en cada supuesto, consúltese al delegado de protección de datos.

Terceros proveedores

Cuando se cuenta con la participación de terceros proveedores que traten datos de carácter personal, estaremos ante una relación entre el responsable y encargo de tratamiento. Dicha relación se debe de regular contractualmente.

En el caso de que este proveedor se encuentre fuera del Espacio Económico Europeo, nos encontraremos ante una transferencia internacional de datos, la cual, deberá de cumplir con unas garantías mínimas de cumplimiento. En este caso concreto, el delegado de protección de datos deberá ser informado sobre la definición del flujo transfronterizo de datos, así como de las exigencias que se deben de garantizar.

Ejemplos:

Nos encontraremos ante un supuesto de encargo de tratamiento cuando, por ejemplo, podemos solicitar a un tercero que:

a) Nos facilite datos de carácter personal.

b) Realice encuestas por nuestra cuenta.

c) Realice funciones de clasificación o procesamiento de la información.

d) Realice una valoración o desarrollo.

e) Etc.

Comités éticos o semejantes (director o tutor académicos)

Es importante señalar la función y responsabilidad de estos órganos que, como garantes de que se cumple con la normativa en materia de protección de datos, contando con el apoyo del delegado de protección de datos, la cual, realizará labores de asesoramiento y garantía de cumplimiento.

¡Aviso!

En el caso de que no se cumplan los principios y garantías en materia de protección de datos que velan por los derechos y libertades de los interesados, no debería llevarse a cabo la actividad principal o actividades ulteriores no contempladas en origen. Si la actividad se ha iniciado o finalizado sin cumplir las exigencias normativas, no podrá hacer uso de los resultados obtenidos e incluso, en ocasiones, proceder a la eliminación de estos.

Un ejemplo de lo previamente descrito lo podemos encontrar en la debida exigencia interna de cumplimiento legal de las revistas científicas, las entidades financiadoras y las entidades que facilitan acceso a datos o contacto con personas de interés. Estas entidades u organizaciones requieren, cada vez más frecuentemente, la acreditación de haber cumplido con la protección de datos. Cuando no se ha cumplido debidamente con la normativa en materia de protección de datos, en ocasiones resultará imposible garantizar el cumplimiento exigido.


crue
Universidades
Españolas
Secretarías
Generales