

Guía básica para investigadores sobre protección de datos personales

En el marco de las actividades de I+D+I desarrolladas por la Universidad Politécnica de Cartagena resulta indispensable tener en cuenta los requerimientos de la **normativa de protección de datos de carácter personal**. Para ello, todo investigador deberá considerar las siguientes directrices contando con el apoyo del Delegado de Protección de Datos de la UPCT (DPD) con el que deberá contactar por correo electrónico: dpd@upct.es.

1. **Si podemos evitarlo, no utilizaremos datos personales.** Así, por ejemplo, emplearemos encuestas anónimas, evitando preguntas que permitan identificar a la persona que dio las respuestas. Si se trata de datos audiovisuales se preverán técnicas que posibiliten obtenerlos anonimizados, tales como modificadores de la voz y de la imagen de la persona que hagan imposible identificarla.
2. Se recomienda diseñar la investigación para evitar al máximo recoger **datos personales especialmente protegidos**. En caso de que sea imprescindible hacerlo, se deberá realizar una evaluación del impacto que supone sobre los derechos y las libertades de las personas el hecho de que la Universidad trate esos datos. En estos casos, el DPD le asesorará sobre cómo tratarlos.
3. **Si tratamos datos personales debemos ponerlo en conocimiento del DPD de la Universidad.** El tratamiento debe quedar reflejado en el Registro de Actividades del Tratamiento que se publica en la Sede electrónica de la UPCT.
4. **Utilizaremos siempre los mínimos datos personales posibles para cumplir con el principio de minimización de datos:** los datos personales que se recogen en el marco de una actividad de I+D+I deben estar limitados a lo estrictamente necesario para la consecución de los objetivos de dicha actividad.

Así, por ejemplo:

- a. Si sólo nos interesa tener control de quien responde un cuestionario evitando respuestas duplicadas, mantendremos por separado las respuestas obtenidas y un listado con la identificación de quién ha respondido, sin que las respuestas queden vinculadas a la persona que las dio.
- b. Si es relevante la edad de la persona solicitaremos que indique su edad o el año en que nació, pero no la fecha completa de nacimiento.



5. **Siempre que sea posible realizaremos un proceso de seudonimización de los datos personales que dificulte conocer a qué persona pertenecen.** Así, por ejemplo, si disponemos de muestras biológicas humanas debemos codificarlas de manera tal que con el solo nombre de la muestra no pueda identificarse a quién pertenece. El vínculo del código de la muestra con la persona a quien corresponden se guardará en un lugar seguro con acceso sólo al personal autorizado.
6. **Los datos personales se recogerán con el consentimiento de la persona entendido como una clara declaración afirmativa** y que se tendrá que poder demostrar más adelante si resultase necesario. Hay que verificar la identidad de la persona para comprobar que efectivamente quien presta el consentimiento es quien dice ser. En el caso de cuestionarios en línea, es necesario adjuntar una pregunta obligatoria, junto con la cláusula de protección de datos, que se marque en una casilla conforme se acepta haberla leído y siempre que sea posible se requerirá la autenticación de la persona en el Campus Virtual.
7. **En caso de menores de 14 años el consentimiento deberá ser obtenido de la persona que ostenta la patria potestad o su tutor legal.** Si se trata de datos de menores de otros países de la Unión Europea la edad puede moverse entre los 13 y los 16 años, pues los Estados miembros han regulado específicamente este requerimiento dentro del rango permitido.
8. **Siempre, incluso cuando los datos no provengan de la propia persona, se debe informar a la persona de lo siguiente:**
 - a. Quién tratará los datos y a quién se cederán.
 - b. En su caso, de dónde se han obtenido los datos si no provienen de la misma persona.
 - c. Qué datos se tratarán y bajo qué medidas de seguridad
 - d. Para qué fin se tratarán. Resulta importante identificar:
 - i. Si en el futuro se les querrá dar otros usos diferentes al del propio estudio. Esto se debe informar en el momento de recoger los datos ya que, de lo contrario, no se podrán utilizar si no se obtiene un nuevo consentimiento de la persona.
 - ii. Si con los datos se realizarán perfiles de la persona, bajo qué criterios y procedimientos que permitirían llegar a conclusiones sobre más información la misma y si se tomarán decisiones automatizadas a partir de este perfil, tal como invitarle a participar en otros estudios.
 - e. Durante cuánto tiempo se tratarán teniendo en cuenta la normativa aplicable y la probabilidad de otros requerimientos como pueden ser auditorías posteriores. Superado este tiempo los datos deberán ser eliminados de forma segura.



- f. Cuáles son sus derechos respecto al tratamiento de los datos y cómo pueden ejercerlos. Indicar que los derechos son de acceso, rectificación, supresión, portabilidad, limitación u oposición al tratamiento.
- g. Quién es el Delegado de Protección de Datos y cómo se puede contactar.

En la página web del Comité de Ética en la Investigación encontrará modelos de **Consentimiento informado** y **Hoja informativa** que podrá utilizar como guía adaptándolos a las características específicas que requiere su actividad de I+D+I (<https://www.upct.es/vicerrectoradoinvestigacion/es/etica/modelos-y-formularios>).

9. **Con carácter previo al tratamiento de datos hay que definir las medidas de seguridad con las que se tratarán los datos para cumplir así con el principio de seguridad desde el diseño.** En caso de tratarse de datos especialmente protegidos hay que extremar las medidas de seguridad. En este ámbito el DPD, en conjunción con el Responsable de Seguridad de la UPCT, asesorarán sobre los sistemas de información más idóneos a utilizar y las medidas a aplicar. Los investigadores deberán informar sobre el tipo de soporte en el que se recogerán los datos (documentos escritos, formularios web, grabaciones de voz, vídeos, seguimiento mediante geolocalizadores, etc.)

Ejemplos de tratamientos que pueden implicar un alto riesgo:

- Elaboración de perfiles sobre cuya base se tomen decisiones que produzcan efectos jurídicos o afecten significativamente a los interesados.
- Tratamientos a gran escala de datos especialmente protegidos.
- Observación sistemática a gran escala de una zona de acceso público.

10. **Se deben utilizar siempre que sea posible los sistemas propios de la Universidad a los que se aplican centralizadamente las medidas de seguridad pertinentes.** En caso de ser necesario utilizar otros sistemas, estos deberán ser configurados de forma segura cumpliendo así con el **principio de seguridad por defecto**. Deberán diseñarse para evitar errores conocidos, tales como contraseñas por defecto del usuario administrador. Además, se bloquearán funcionalidades y campos de información del programa que no sea necesario utilizar y se mantendrá actualizado a la última versión con sus respectivos parches de seguridad.
11. **Durante el tratamiento de datos** todo el que participe en la realización del estudio estará advertido de las medidas de seguridad que deberá tener en cuenta y saber que los datos se deben utilizar única y exclusivamente para la finalidad para la que se recogieron, evitando cualquier acceso no autorizado a los mismos.
12. **En caso de que un proveedor participe en la realización del estudio, éste es considerado Encargado del Tratamiento** de los datos, que seguirán siendo responsabilidad de la UPCT. En ese caso, hay que suscribir un contrato que limite al proveedor, indicando claramente,



entre otros, qué datos tratará, para qué finalidad y bajo qué medidas de seguridad, así como lo que deberá realizar con los datos a la finalización del contrato.

13. **En caso de que los datos sean tratados por un proveedor o una entidad que participe en el estudio y se encuentre fuera del espacio europeo hay que exigir que los datos se traten bajo las premisas de la normativa europea** que se encuentra ente las más exigentes en la materia en todo el mundo. El DPD le asesorará sobre las exigencias a suscribir mediante contrato o convenio de colaboración. En la medida de lo posible, los datos se mantendrán en territorio europeo y se facilitará a la otra parte el acceso a los mismos sin que pueda extraerlos.
14. En atención a la función pública de la Universidad de promover la investigación **resulta posible invitar a la comunidad universitaria a participar en estudios de investigación**. No obstante, los miembros de la Comunidad Universitaria deberán disponer de un mecanismo sencillo para darse de baja de recibir este tipo de comunicados, lo que habrá que respetar para no enviar solicitudes adicionales.

ANEXO

Marco legislativo de aplicación: <https://privacidad.upct.es/container/normativa-vinculada-a-la-proteccion-de-datos>

Actores implicados en el proceso

1. **Interesado:** persona física identificada o identificable. Se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente a partir de determinada información.
2. **Responsable del tratamiento de datos:** cuando los investigadores de la UPCT recaban datos personales en el marco de actividades de I+D+I, el responsable del tratamiento será la Universidad Politécnica de Cartagena.
3. **Encargado del tratamiento de datos:** persona física o jurídica, autoridad pública, servicio u otro organismo que trate los datos personales por cuenta del responsable del tratamiento. El Investigador Responsable de la actividad de I+D+I será el encargado del tratamiento.
4. **Corresponsable del tratamiento de datos:** Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento de datos personales serán considerados corresponsables del tratamiento, por ejemplo, en proyectos de investigación realizados en cooperación con otras Universidades.
5. **Delegado de protección de datos de la UPCT (DPD).**
6. **Responsable de Seguridad de la UPCT.**

Glosario de términos utilizados en la presente guía (de acuerdo a la legislación vigente para la protección de datos de carácter personal)

Dato personal: aquel relativo a una persona física identificada o identificable “el interesado”. Por lo tanto, aunque no tengamos el nombre o el DNI de una persona, si tenemos un conjunto de datos que permitirían determinar a quién pertenecen, entonces son considerados igualmente datos personales.

Datos personales especialmente protegidos: aquellos que revelan el origen étnico o racial, las opiniones políticas, la religión o las creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual o las condenas e infracciones penales, administrativas o medidas de seguridad conexas.



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.

Elaboración de perfiles, toda forma de tratamiento automatizado de datos personales consistente en utilizar los 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 (muy importante este punto en la aplicación de la Inteligencia Artificial (IA) que desarrolla perfiles automatizados para la predicción.

Seudonimización: Es 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.

Anonimización: Es la disociación definitiva e irreversible de los datos personales.

Consentimiento del interesado: En aquellos supuestos en los que la base jurídica del tratamiento sea el consentimiento, la citada manifestación de voluntad ha de prestarse de forma libre, específica, informada e inequívoca por la que se acepte, mediante una declaración o clara acción afirmativa, el tratamiento de datos que le conciernan al que lo presta. Una de las vías de acreditarlo puede ser mediante la marcación registrada de una casilla de verificación. En cualquier caso, el tratamiento estará limitado a la finalidad para la que se solicita el mismo.