

DECÁLOGO

BUENAS PRÁCTICAS DE PROTECCIÓN DE DATOS PARA PROYECTOS DE INVESTIGACIÓN

La Universidad de Jaén está muy concienciada en el cumplimiento de la normativa de protección de datos. En muchos proyectos de investigación, actualmente, se requiere el tratamiento de datos para cumplir con la finalidad pretendida. Todo el personal investigador debe cumplir con la normativa de protección de datos y de confidencialidad. Para cumplir con las obligaciones en materia de protección de datos, el Servicio de Información, Registro y Administración electrónica (SIR@) en coordinación con el Delegado de Protección de datos (DPO) y el Comité de Ética de la Universidad de Jaén publican el siguiente decálogo de obligado cumplimiento.

1

COMUNICACIÓN

Comunicar al SIR@ la intención de efectuar una investigación que implique el tratamiento de datos personales a través del formulario de investigación con tratamiento de datos de carácter personal (<https://forms.gle/9acjLqAgYorsA3jS9>). No es necesario comunicar aquellos proyectos que no vayan a implicar el tratamiento de datos personales. Si tienes dudas, contacta con el SIR@ (<https://cau.ujaen.es/otrs/customer.pl>) y se te prestará toda la ayuda a nuestro alcance.

2

DEBER DE INFORMACIÓN

Garantizar que se informa a los participantes en el Proyecto de Investigación acerca del tratamiento de datos personales facilitando el derecho de información, y en su caso, se obtienen los consentimientos necesarios. Se responsabiliza también de custodiar las evidencias relacionadas con el suministro de información y la obtención de los consentimientos.

3

DERECHOS ARSOPL

Remitir cualquier ejercicio de derechos de protección de datos (ARSOPL) al SIR@ de los que se tenga noticia y colaborar en su resolución. Puede hacerlo remitiendo email a dpo@ujaen.es.

4

PRINCIPIOS

Cumplir con los principios de protección de datos. El personal investigador deberá cumplir con los principios de protección de datos: transparencia, licitud, lealtad, limitación de la finalidad, minimización, exactitud, limitación del plazo de conservación, e integridad y confidencialidad.

5

INCIDENTES DE SEGURIDAD

Informar de cualquier incidente de seguridad. Deberá comunicarse cualquier incidente que afecte a datos de carácter personal en el plazo máximo de 24 horas desde que tenga conocimiento del evento. Deberá comunicarlo al SIR@; sin perjuicio de las obligaciones de notificar los incidentes al Servicio de Informática.

6

ENCARGOS DE TRATAMIENTO

Establecer los contratos de protección de datos adecuados con los proveedores y requerir la declaración responsable a los proveedores que tengan la consideración de encargados de tratamiento.

7

SEGURIDAD

Cumplir con las medidas de seguridad de la información de la Universidad de Jaén.

8

TRANSFERENCIA INTERNACIONAL

Comunicar la necesidad de transmitir información que incluya datos personales a entidades radicadas fuera de la Unión Europea al SIR@.

9

COLABORACIÓN

Colaborar con el SIR@, Delegado de Protección de Datos o la Autoridad de Control en aquellos requerimientos que se le formulen

10

ANONIMIZACIÓN/SEUDONIMIZACIÓN

Siempre que sea posible deben tratarse los datos personales de forma anonimizada o seudonimizada. "Anonimizado" supone que los datos se han convertido en anónimos de tal forma que el interesado no podría ser identificado.

"Seudonimizado" significa que en los datos se separan los identificadores directos para que solamente se pueda identificar a una persona con información adicional que se mantiene de forma segura por separado.



Universidad
de Jaén



MÁS