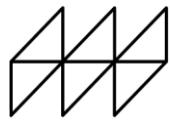
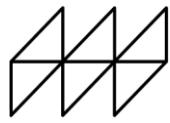


PLAN DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

CENTRE D'ESTUDIS DEMOGRÀFICS

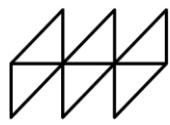
4 de febrero de 2025





ÍNDICE

1. Resumen ejecutivo	5
2. Introducción.....	7
3. Responsable del tratamiento de datos personales del CED	7
4. Persona delegada de la protección de datos personales (DPD)	8
5. Características del Protocolo	9
6. Tipos de datos sujetos a la nueva normativa	12
ANEXO: Relación de documentos del Protocolo de seguridad y privacidad del CED.....	14



1. RESUMEN EJECUTIVO

Este documento es una revisión del documento P03.3 de octubre de 2019 con fecha de enero de 2025.

El plan de protección de datos de carácter personal hace referencia a la aplicación del 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 y la libre circulación de datos personales, y de la LOPD 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, por parte del CONSORCIO CENTRE D'ESTUDIS DEMOGRÀFICS, ENTIDAD PÚBLICA DE DERECHO PRIVADO.

Los conceptos básicos que deben tenerse en cuenta según el citado Reglamento (en adelante RGPD) son los siguientes:

- **Datos personales:**

Cualquier información sobre una persona física identificada o identifiable («el interesado»). Se considera persona física identifiable 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 la persona.

- **Consentimiento del interesado:**

Cualquier manifestación de voluntad libre, específica, informada e inequívoca por la que la persona interesada acepta, mediante una declaración o una acción afirmativa clara, el tratamiento de datos personales que le conciernen.

- **Tratamiento:**

Cualquier operación o conjunto de operaciones que se apliquen a datos de carácter personal, de manera automatizada o no, es decir: recogida, registro, organización, estructuración, almacenamiento, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otro medio disponible, comparación o combinación, restricción, supresión o destrucción.

- **Encargado del tratamiento:**

La La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que trate datos personales por cuenta del responsable del tratamiento.

- **Gestión de riesgos:**

Es el conjunto de actividades y tareas que permiten controlar la incertidumbre de una amenaza mediante una secuencia de actividades que incluye la identificación y evaluación del riesgo, así como las medidas para su reducción o mitigación.

- **Medidas y protocolos para garantizar la seguridad de los datos:**

Tienen por objeto garantizar la seguridad de los datos de carácter personal, teniendo en cuenta el estado de la técnica, los costes de aplicación, el alcance, el contexto y las finalidades de los tratamientos, así como los riesgos y amenazas para los derechos y libertades de las personas, de manera que se pueda acreditar el cumplimiento y la eficacia de las medidas aplicadas en cada caso. El momento adecuado para definir las medidas de control y seguridad a aplicar es la fase de diseño de los servicios.

El CED dispone de un “**Protocolo de Privacidad y Medidas de Seguridad de los Datos de Carácter Personal del CED**”, que ha sido supervisado por una Delegada de Protección de Datos (DPD), cuya función es el seguimiento de su correcta aplicación. También cuenta con una “**Política de Protección de Datos del CED**”, firmada por la dirección del CED. Ambos documentos están actualizados a julio de 2024.

El despliegue requerido por la normativa del RGPD está detallado en el mencionado Protocolo, y el presente documento, en el marco de la estrategia HRS4R, resume sus contenidos más relevantes.

Todo el personal del CED debe tener presente esta normativa y seguir el Protocolo al diseñar o desarrollar una actividad o proyecto de investigación que implique la utilización de datos de carácter personal.

2. INTRODUCCIÓN

El 27 de abril de 2016 se aprobó el Reglamento (UE) 2016/679 del Parlamento y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de dichos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE 4.5.2016).

La novedad más destacada de la nueva legislación es el principio de responsabilidad proactiva. Esto significa que el organismo, a través de todo el personal que trabaja con datos de carácter personal, debe ser proactivo respecto a las obligaciones sobre confidencialidad y gestión de riesgos, y respecto a los derechos de las personas interesadas, mediante cláusulas y consentimientos explícitos, utilizando registros, documentación firmada, informando sobre posibles violaciones de seguridad, etc.

A finales de 2017, el CED inició los trabajos de adaptación a la nueva normativa europea, que cambiaba de manera fundamental las gestiones relacionadas con el tratamiento de datos personales, así como los derechos de las personas respecto a la legalidad que entraría en vigor el 25 de mayo de 2018, fecha límite para la aplicación de la normativa.

A principios de 2018, el CED creó un equipo de trabajo que se formó en los conceptos y procedimientos requeridos por la nueva normativa.

En diciembre de 2018, la normativa española completó las disposiciones sobre este tema con la LOPD 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.

En marzo de 2019, el CED contrató a una Delegada de Protección de Datos, quien se integró en el equipo para asesorar en la redacción final del **"Protocolo de Privacidad y Medidas de Seguridad de los Datos de Carácter Personal del CED"**. Este documento se actualiza siempre que es necesario, y la última versión data de julio de 2024.

Desde 2020, la DPD del CED actualiza y realiza el seguimiento de los protocolos de protección de datos desarrollados en el CED mediante una auditoría, que da lugar a un informe de verificación anual. Además, la DPD asesora al CED en todos los contenidos relacionados con nuestra política; por ejemplo, en 2024 se desarrolló el **"Protocolo de desconexión digital del CED"**.

Todo el despliegue requerido está detallado en el mencionado Protocolo, y el presente documento, en el marco de la estrategia HRS4R, resume sus contenidos más relevantes.

3. RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES

Nombre: CONSORCIO CENTRE D'ESTUDIS DEMOGRÀFICS, ENTIDAD PÚBLICA DE DERECHO PRIVADO

Actividad: investigación, formación y transferencia en el campo de la demografía

CIF: Q5855973C

Mail de contacto: personaldata@ced.uab.cat

Teléfono: 935813060

* Este Protocolo contiene todo el detalle de las acciones que es obligatorio realizar, así como los diferentes tipos de documentos que deben utilizarse para cada una de las acciones de protección de la privacidad y seguridad de los datos de carácter personal. Véase, en el anexo, la relación completa.

Dirección: Edificio E2, Campus UAB, 08193, Cerdanyola del Vallès

Web: <https://ced.cat/>

3.1. Obligaciones

El responsable del tratamiento es la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o junto con otros, determina las finalidades y los medios del tratamiento.

El tratamiento de datos personales se define 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, el registro, la organización, la estructuración, la conservación, la adaptación o modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, confrontación o interconexión, limitación, supresión o destrucción”.

3.2. Corresponde al responsable del Tratamiento de los datos:

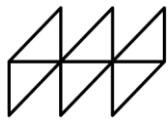
- Aplicar los principios del Reglamento (RGPD) en el tratamiento de datos personales para garantizar y poder demostrar que el tratamiento se ajusta a las previsiones del RGPD, tanto en el momento de determinar los medios del tratamiento como durante el mismo.
- Garantizar que solo sean objeto de tratamiento los datos personales que sean necesarios.
- Aplicar las medidas de seguridad adecuadas en relación con las actividades de tratamiento para garantizar la confidencialidad e integridad de los datos.
- Seleccionar encargados del tratamiento que garanticen la aplicación de las medidas técnicas y organizativas apropiadas.
- Cooperar con la autoridad de control que lo solicite.
- Comunicar las violaciones de seguridad que se hayan producido: el encargado al responsable, y el responsable a la autoridad de control y al interesado.
- Designar un delegado de protección de datos cuando sea necesario.

4. PERSONA DELEGADA DE LA PROTECCIÓN DE DATOS PERSONALES (DPD)

El Reglamento introduce la figura del delegado de protección de datos cuando el tratamiento lo lleva a cabo una autoridad u organismo público, como es el caso del CED. La persona designada para esta función en el CED es: **Maria Company Jiménez**, abogada especializada en Derecho Digital y Protección de Datos.

El delegado de protección de datos tiene, entre otras, las siguientes funciones:

- Informar y asesorar al responsable o al encargado y a los trabajadores sobre las obligaciones que impone la normativa de protección de datos.
- Supervisar que se cumple la normativa.
- Asesorar respecto a la evaluación de impacto relativa a la protección de datos.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto para cuestiones relativas al tratamiento.



Los responsables y los encargados deben hacer pública la designación del delegado de protección de datos y sus datos de contacto, y comunicarlos a las autoridades de supervisión competentes.

La posición del DPD en las organizaciones debe cumplir los requisitos que el RGPD establece expresamente: total autonomía en el ejercicio de sus funciones, la necesidad de que se relacione con el nivel superior de la dirección, y la obligación de que el responsable o encargado le faciliten todos los recursos necesarios para desarrollar su actividad.

5. CARACTERÍSTICAS DEL PROTOCOLO

El **Protocolo de Privacidad y Medidas de Seguridad de los Datos de Carácter Personal del CED**, contiene la definición de los conceptos básicos, las bases jurídicas y los diferentes ámbitos de aplicación del reglamento, con la siguiente información en la que se desarrollan los aspectos que aquí se resumen, tales como:

5.1. Ámbito de aplicación

El Reglamento amplía el ámbito de aplicación territorial a los responsables y encargados del tratamiento establecidos en la UE, así como cuando las actividades de los no establecidos en la UE están relacionadas con la oferta de bienes o servicios o con el control del comportamiento de las personas que se encuentran en la UE.

5.2. Principios

La mayor innovación del RGPD para los responsables la constituyen dos elementos de carácter general:

5.2.1. El principio de “responsabilidad proactiva”

El RGPD describe este principio como la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas, con el fin de garantizar y poder demostrar que el tratamiento es conforme al Reglamento.

Este principio requiere que las organizaciones analicen qué datos tratan, con qué fines lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. A partir de este conocimiento, deben determinar de manera explícita cómo aplicarán las medidas que prevé el RGPD. Asimismo, deben asegurarse de que estas medidas son adecuadas para cumplirlo y que pueden demostrar su cumplimiento ante las personas interesadas y ante las autoridades de supervisión.

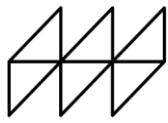
En síntesis, este principio exige que las organizaciones adopten una actitud consciente, diligente y proactiva frente a todos los tratamientos de datos personales que lleven a cabo.

5.2.2. El principio del “enfoque de riesgo”

Las medidas dirigidas a garantizar su cumplimiento deben tener en cuenta la naturaleza, el alcance, el contexto y las finalidades del tratamiento, así como el riesgo para los derechos y libertades de las personas.

Estos dos elementos se proyectan sobre todas las obligaciones de las organizaciones. Se trata de una privacidad desde el diseño y de una privacidad por defecto.

El responsable debe aplicar, tanto en el momento de determinar los medios de tratamiento como durante el propio tratamiento, las medidas técnicas y organizativas adecuadas,



concebidas para aplicar de manera efectiva los principios de protección e integrar las garantías necesarias en el tratamiento para cumplir los requisitos del Reglamento.

Asimismo, debe aplicar las medidas técnicas y organizativas adecuadas para garantizar que, por defecto, solo se traten los datos personales necesarios para cada finalidad específica del tratamiento.

5.3. Categorías especiales de datos

Datos genéticos: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física, que proporcionan información única sobre la fisiología o la salud de dicha persona, obtenidos en particular del análisis de una muestra biológica.

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 permiten o confirman la identificación única de dicha persona (imágenes faciales, datos dactiloscópicos, etc.).

Las entrevistas en profundidad que se realizan en el marco de algunos proyectos de investigación también se incluyen en esta categoría de datos especiales, dado que en ellas se manifiestan opiniones, se describen comportamientos y, por tanto, hay información relativa a la ideología, la orientación sexual u otros datos sensibles.

5.4. El consentimiento

El RGPD requiere que el interesado otorgue su consentimiento mediante una declaración inequívoca o una acción afirmativa clara. A los efectos del nuevo Reglamento, las casillas ya marcadas, el consentimiento tácito o la inacción no constituyen un consentimiento válido.

El consentimiento por omisión no es compatible con el RGPD, ya que se basa en la inacción de la persona interesada.

El consentimiento puede ser inequívoco o bien otorgarse de forma implícita, por ejemplo, cuando se deduce de una acción de la persona interesada que decide continuar navegando por una página web, aceptando así que se utilicen cookies para monitorizar su navegación.

Se requiere un consentimiento explícito para el tratamiento de categorías especiales de datos, en la adopción de decisiones automatizadas y para realizar transferencias internacionales de datos.

5.5. Derecho de información

La información es un derecho de las personas afectadas y debe incluir los siguientes aspectos: los datos de contacto del delegado de protección de datos; la base jurídica del tratamiento; los intereses legítimos perseguidos en los que se fundamenta el tratamiento, si procede; la intención de transferir los datos a un tercer país o a una organización internacional y la base para hacerlo, si procede; el plazo durante el cual se conservarán los datos; el derecho a solicitar la portabilidad; el derecho a retirar en cualquier momento el consentimiento prestado; si la comunicación de datos es un requisito legal o contractual, o un requisito necesario para suscribir un contrato; el derecho a presentar una reclamación ante una autoridad de control; la existencia de decisiones automatizadas, incluida la lógica aplicada y sus consecuencias.

El RGPD establece que la información a los interesados debe proporcionarse de forma concisa, transparente, inteligible y de fácil acceso, y en un lenguaje claro y sencillo.

5.6. Principales derechos

El RGPD incorpora el derecho al olvido, el derecho a la limitación del tratamiento y el derecho a la portabilidad, además de mantener los derechos previstos en la normativa anterior. Por tanto, se deberán tener en cuenta todos los derechos que se relacionan a continuación:

- Acceso: permite al interesado conocer y obtener información sobre el tratamiento de sus datos personales de forma gratuita.
- Rectificación: derecho para garantizar la certeza de la información tratada. Permite corregir y modificar los datos inexactos o incompletos.
- Supresión: permite la eliminación de los datos que resulten inadecuados o excesivos sin interferir con el deber de bloqueo.
- Oposición: derecho a exigir el cese o a que no se lleve a cabo el tratamiento de los datos del interesado.
- Limitación: derecho a suspender las operaciones de tratamiento de los datos personales del interesado.
- Portabilidad: complemento del derecho de acceso. Permite obtener los datos proporcionados a una organización o transmitirlos directamente a otra entidad.
- Olvido: es la manifestación de los derechos de cancelación y oposición aplicados a los buscadores de internet. Permite impedir la difusión de datos personales a través de internet si no se cumplen ciertos requisitos.

5.7. Procedimiento para ejercer los derechos

El RGPD no establece una forma concreta para ejercer los derechos, pero sí exige a los responsables que los procedimientos sean visibles, accesibles y sencillos, y que las solicitudes se presenten por medios electrónicos, especialmente cuando el tratamiento se realiza por estos medios.

El ejercicio de los derechos debe ser gratuito para la persona interesada.

El responsable puede contar con la colaboración de los encargados para atender el ejercicio de los derechos de los interesados.

5.8. Registro de actividades de tratamiento

Los responsables y encargados deben documentar un registro de las actividades de tratamiento que realizan. Este registro debe contener, respecto de cada actividad, la información que establece el RGPD:

- Nombre y datos de contacto del responsable y, en su caso, del corresponsable, así como del delegado de protección de datos, si lo hubiera.
- Finalidades del tratamiento.
- Descripción de las categorías de interesados y de las categorías de datos personales tratados.
- Transferencias internacionales de datos.
- Cuando sea posible, los plazos previstos para suprimir los datos.
- Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

5.9. Medidas de seguridad

El Reglamento no establece un listado de las medidas de seguridad que son de aplicación según la tipología de datos objeto de tratamiento, sino que establece que el responsable y

el encargado del tratamiento deben aplicar medidas técnicas y organizativas adecuadas al riesgo que comporta el tratamiento.

Las medidas concretas a aplicar deben 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 manera rápida en caso de incidente físico o técnico.
- La existencia de un proceso para verificar y evaluar regularmente la eficacia de las medidas técnicas y organizativas establecidas para garantizar la seguridad del tratamiento.

Si se produce una violación de la seguridad, el responsable debe notificarla a la autoridad de control en un plazo máximo de 72 horas, salvo que sea improbable que constituya un riesgo para los derechos y libertades de las personas.

El CED mantiene actualizados los siguientes documentos:

- Relación del personal
- Relación de las personas que acceden a los datos
- Relación de los ordenadores/servidores
- Dominio
- Programas informáticos
- Lista de externos que tienen acceso a los datos del Centro
- Lista de empresas que acceden al CED

Realiza el seguimiento y establece un control de:

- Las copias de seguridad
- Las posibles violaciones de seguridad
- Los derechos de los usuarios
- El registro de soportes
- El almacenamiento
- La destrucción

6. TIPOS DE DATOS SUJETOS A LA NUEVA NORMATIVA

- Datos personales: Todos aquellos que permiten identificar a una persona: nombres y apellidos; DNI, NIE, pasaporte; foto, vídeo; dirección de correo electrónico; dirección postal, etc.
- Datos sensibles: Toda información que pueda vulnerar el derecho a la intimidad: datos de salud; raza; orientación sexual; estado civil y familiar; discapacidad; opiniones, etc.

Para organizar las gestiones relacionadas con la normativa de protección de datos, es necesario definir las diferentes actividades en las que se realiza un tratamiento de este tipo de información. En el CED se han definido las siguientes:

1. INVESTIGACIÓN. Datos: relaciones con instituciones; entrevistas en profundidad
2. FORMACIÓN. Candidatos/as; predoc; postdoc
3. DOCENCIA. Profesores/as; alumnos/as; candidatos/as

4. CURSOS, SEMINARIOS Y ESCUELA DE VERANO. Profesores/as; alumnos/as; candidatos/as
5. CONFERENCIAS: Quién da la conferencia; qué condiciones ha establecido (derechos de imagen...); informar a los asistentes de que pueden ser filmados.
6. ESTANCIAS: Tutores; residentes; candidatos/as.
7. CONTACTOS: Correo electrónico, acceso al dominio o a impresoras.
8. RECURSOS HUMANOS: Secretaría y funcionamiento del CED; administración y gobernanza; contabilidad y presupuestos; investigación y formación.

Se debe distinguir si los datos son responsabilidad del CED o si son datos cuyo tratamiento realiza por encargo.

El acceso a la información en cada una de las actividades del CED puede ser transversal y de distinta naturaleza, como por ejemplo un tratamiento directo de la información o un simple conocimiento de la información por formar parte de una comisión. En todo caso, el compromiso de confidencialidad debe registrarse igualmente.

Los recursos del CED también se administran de manera controlada, por ejemplo, mediante el dominio del CED o el acceso a las carpetas en servidores. La información en papel se guarda en mobiliario cerrado con llave y en despachos determinados, que también deben permanecer cerrados.

ANEXO: Relación de los documentos del Protocolo de seguridad y privacidad del CED.

1. Anexo a: Registro de actividades de tratamiento
2. Anexo b: Recursos protegidos
3. Anexo c: Cláusulas para los interesados
4. Anexo d: Encargados del tratamiento
5. Anexo e: Funciones y obligaciones de las personas con acceso a los datos personales del responsable
6. Anexo f: Política de privacidad para los empleados
7. Anexo g: Modelo de comunicación interna de violación de seguridad
8. Anexo h: Análisis de violación de seguridad y necesidad de comunicación a la autoridad de control y al interesado
9. Anexo i: Relación de personal y usuarios
10. Anexo j: Registro de entrada y salida de soportes
11. Anexo k: Autorización de entrada y salida de soportes
12. Anexo l: Modelos para el ejercicio de los derechos de los ciudadanos
13. Anexo m: Cláusula de confidencialidad
14. Anexo n: Sistema de realización de las copias de seguridad
15. Anexo p: Verificación mensual del control de accesos para los tratamientos de categorías especiales de datos
16. Anexo q: Aplicaciones informáticas
17. Anexo r: Identificación y autenticación
18. Anexo s: Responsable de seguridad
19. Anexo t: Borrado y destrucción de la documentación
20. Anexo u: Almacenamiento de la documentación
21. Anexo v: Inventario de soportes informáticos
22. Anexo w: Aviso legal para la página web
23. Anexo x: Código de buenas prácticas en investigación