



Código de conducta sobre la protección de datos para una investigación e innovación responsables



Esta obra está bajo una licencia de Creative Commons Atribución-NoComercial-SinObraDerivada 4.0 Internacional.



Este proyecto ha recibido financiación del programa de investigación e innovación Horizonte 2020 de la Unión Europea en virtud del acuerdo de subvención n° 788039. Este documento refleja únicamente la opinión del autor y la Agencia no es responsable del uso que pueda hacerse de la información que contiene.

Información sobre el proyecto

Título del proyecto Enfoques participativos para un nuevo marco ético y jurídico de las TIC
Acrónimo del proyecto PANELFIT
Número del convenio de subvención 788039
Coordinador de proyecto UPV/EHU

Información del documento

Número de entrega D5.4
Título del documento Código de conducta sobre la protección de datos para una investigación e innovación responsables
Versión del documento Versión 4.0
Fecha del documento 2021-08-04
Documento principal ICM-CSIC | < soacha@icm.csic.es >

Socios del proyecto que participan en el documento

Nº	Nombre de la organización participante	Acrónimo
1	Instituto de Ciencias del Mar (Consejo Superior de Investigaciones Científicas)	ICM-CSIC
2	Universidad del País Vasco / Euskal Herriko Unibertsitatea	UPV/EHU
3	Red Europea de Comités de Ética de la Investigación	EUREC
4	Unabhängiges Landeszentrum für Datenschutz AöR	ULD
5	Academia de Ciencias de Austria	OEAW
6	Fonden Teknologiradet	DBT

Historia del documento

Estado	Versión	Fecha	Autor(es)	Revisado por
Borrador	v0.5	2020-10-30	Pranesh Prakash (ICM-CSIC)	Karen Soacha (ICM-CSIC), Jaume Piera (ICM-CSIC)
Borrador	v1.0	2020-11-03	Pranesh Prakash	Julia Maria Mönig (EUREC), Johann Cas (OEAW), Bud Bruegger (ULD), Harald Zwingelberg (ULD), Bjørn Basted (DBT)
Borrador	v2.0	2020-12-06	Pranesh Prakash	Iñigo de Miguel Beriain (UPV/EHU), Karen Soacha
Borrador	v3.0	2021-01-23	Pranesh Prakash	Karen Soacha
Final	v4.0	2021-08-02	Pranesh Prakash	Karen Soacha, MLEs (Interesados, Investigadores), Iñigo de Miguel Beriain

Descargo de responsabilidad: El contenido de esta publicación es responsabilidad exclusiva del consorcio PANELFIT y no refleja necesariamente la opinión de la Unión Europea.

Tabla de Contenidos:

Tabla de Contenidos:	3
1 Preámbulo	4
1.1. RRI y protección de datos.....	5
2 Principios de protección de datos	6
2.1. Licitud, equidad y transparencia.....	6
2.2. Limitación de la finalidad.....	10
2.3. Minimización de datos.....	12
2.4. Precisión.....	13
2.5. Limitación de almacenamiento.....	14
2.6. Integridad y confidencialidad.....	14
2.7. Rendición de cuentas.....	15
3 Buenas prácticas relacionadas con los principios de protección de datos	16
3.1. Anonimización, seudonimización y cifrado.....	17
3.2. Datos agregados y gruesos.....	17
3.3. Transparencia.....	17
3.4. Múltiples bases jurídicas para el tratamiento	18
3.5. El consentimiento en la protección de datos y en la ética.....	18
3.6. Legitimidad, lealtad y aprobaciones éticas	18
3.7. Autoridades de protección de datos y comités de ética.....	19
3.8. Directrices de protección de datos y DPD	19
3.9. Evaluación del impacto de la protección de datos.....	20
4 Anexos.....	20
4.1. Anexo 1: Recursos clave.....	20
4.2. Anexo 2: Bibliografía.....	22
4.3. Anexo 3: Proceso de creación del Código de Conducta sobre Protección de Datos para la Investigación e Innovación Responsables.....	23

1 Preámbulo

Este Código de Conducta sobre Protección de Datos para la Investigación e Innovación Responsables (CCPD) es una contribución del proyecto PANELFIT a la comunidad investigadora.

PANELFIT (Enfoques participativos para un nuevo marco ético y jurídico de las TIC) es un proyecto financiado por Horizonte 2020 que elaboró normas operativas y directrices prácticas para abordar algunas de las cuestiones éticas y jurídicas que plantean las tecnologías de las TIC. Así, el proyecto PANELFIT pretende aportar claridad y orientación respecto a aspectos problemáticos ligados a la investigación e innovación responsables (EIR),¹ la ética y la protección de datos.

El CCPD tiene como objetivo proporcionar un conjunto de normas de conducta fáciles de entender que cubren los principales principios previstos en el Reglamento General de Protección de Datos (RGPD) de la UE, así como una serie de prácticas adecuadas, adaptadas específicamente a la comunidad investigadora.² Existen múltiples códigos de conducta relacionados con la investigación y la innovación responsables. Sin embargo, estos códigos de conducta existentes no pretenden ofrecer orientación sobre los principios de protección de datos, lo que constituye una laguna que este CCPD pretende cubrir. El CCPD pretende ser un texto introductorio a los principios de protección de datos, y no pretende abarcar todos los aspectos del RGPD que pueden ser de interés para los investigadores. Así, por ejemplo, el CCPD no pretende abarcar todas las obligaciones que un investigador puede tener en virtud de las leyes de protección de datos, ni todos los derechos de las personas cuyos datos personales son utilizados por los investigadores, ni los requisitos legales en torno a la puesta en común de datos personales con investigadores fuera de la UE, las leyes nacionales sobre protección de datos, etc. El proyecto PANELFIT también ha creado unas "Directrices sobre cuestiones éticas y jurídicas de protección de datos en la investigación y la innovación en materia de TIC", que pretenden ser mucho más exhaustivas en este sentido.

¹ La Investigación e Innovación Responsables (EIR) es un componente importante del programa "Ciencia con y para la Sociedad" de Horizonte 2020 (H2020) de la UE. "La EIR es el proceso continuo de adaptación de la investigación y la innovación a los valores, las necesidades y las expectativas de la sociedad." (Declaración de Roma sobre Investigación e Innovación Responsables en Europa). La Comisión Europea señala que "la EIR es un enfoque inclusivo de la investigación y la innovación (I+I), para garantizar que los actores sociales trabajen juntos durante todo el proceso de investigación e innovación... En términos generales, la EIR implica anticipar y evaluar las posibles implicaciones y las expectativas de la sociedad con respecto a la investigación y la innovación." (Comisión Europea, "Ciencia con y para la sociedad")

² Aunque no existe una definición única y universalmente aceptada de investigación, es útil tener en cuenta las palabras del Supervisor Europeo de Protección de Datos en un informe reciente: "Las definiciones reputadas de investigación tienden a hacer hincapié en la actividad sistemática, incluida la recopilación y el análisis de datos, que incrementa el acervo de comprensión y conocimiento y su aplicación". La Comisión Europea ha definido los objetivos de la investigación y las políticas de la UE como "abrir el proceso de innovación a personas con experiencia en ámbitos distintos del académico y el científico", "difundir los conocimientos tan pronto como estén disponibles utilizando la tecnología digital y de colaboración" y "promover la cooperación internacional en la comunidad investigadora". " (Supervisor Europeo de Protección de Datos, "A Preliminary Opinion on Data Protection and Scientific Research", 9-10)

1.1. RRI y protección de datos

La actividad investigadora, ya sea la realización de investigaciones o su difusión, a menudo implica el tratamiento de datos personales.³ Por lo tanto, la ética de los datos es un componente necesario de la investigación y la innovación responsables, y eso incluye la protección de los datos personales. En la UE, la protección de los datos personales es un derecho fundamental en virtud de la Carta de los Derechos Fundamentales de la Unión Europea, y el Reglamento General de Protección de Datos desarrolla ese derecho.¹

Los investigadores están sujetos a la normativa de protección de datos personales, y consiguientemente están obligados a cumplir las disposiciones del RGPD, y a adoptar buenas prácticas que reviertan en la protección de los derechos de los interesados.

El CCPD pretende ayudar a los investigadores a comprender los principios básicos que subyacen a la protección de datos en el cumplimiento de esta tarea.

Por tanto, el objetivo es que los investigadores sepan cómo aplicar en la práctica estos principios en el marco de la investigación y la innovación responsables. La comprensión de la investigación en el marco del RGPD es amplia, ya que abarca las actividades destinadas a proporcionar conocimientos que puedan "mejorar la calidad de vida de una serie de personas y mejorar la eficiencia de los servicios sociales", e incluye "el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado"⁴

³ Los datos personales son cualquier información relativa a una persona física identificada o identificable. El término es una categoría muy amplia, e incluye el nombre de una persona, su número de identificación, sus datos de localización, un identificador en línea o factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de esa persona.

⁴ Reglamento general de protección de datos, Reglamento de la UE 2016/679, considerando 159.

2 Principios de protección de datos

La protección de los datos personales según el RGPD se basa en una serie de principios:

- Licitud, equidad y transparencia¹
- Limitación de la finalidad²
- Minimización de datos³
- Exactitud⁴
- Limitación del plazo de conservación⁵
- Integridad y confidencialidad⁶
- Responsabilidad proactiva⁷

2.1. Licitud, equidad y transparencia

Para cumplir con los requisitos del principio de legalidad, transparencia y equidad, los investigadores deben

- Determinar las finalidades de la recogida y utilización de los datos personales.
- Asegurarse de que identifican un motivo válido (al menos uno de los seis motivos ("bases jurídicas") previstos en el RGPD) para la recogida y el uso de los datos.
- Garantizar que todo uso de los datos es legítimo y cumple con todas las leyes y directrices éticas aplicables, incluidas las relativas a los ensayos clínicos, la propiedad intelectual, los derechos humanos, los contratos, etc.
- Determinar las expectativas de los individuos en cuanto al uso que los investigadores podrían hacer de sus datos y lo que considerarían razonable.
- Anticipar los posibles daños que pueden ocasionarse al titular de los datos.
- Recoger y utilizar los datos de forma abierta y transparente.
- Informar a las personas en un lenguaje claro sobre quién recoge u obtiene los datos, bajo qué fundamento jurídico se recogen/obtienen, por qué se recogen/obtienen, durante cuánto tiempo se conservarán, cómo se utilizarán y por quién, y cuáles son sus derechos.
- Utilizar los datos de manera justa, en consonancia con las expectativas de las personas, y de forma que no suponga un perjuicio injustificado para ellas.

¹ [Reglamento general de protección de datos, Reglamento de la UE 2016/679](#), art. 5(1)(a).

² [Reglamento general de protección de datos, Reglamento de la UE 2016/679](#), art. 5(1)(b).

³ [Reglamento general de protección de datos, Reglamento de la UE 2016/679](#), art. 5(1)(c).

⁴ [Reglamento general de protección de datos, Reglamento de la UE 2016/679](#), art. 5(1)(d).

⁵ [Reglamento general de protección de datos, Reglamento de la UE 2016/679](#), art. 5(1)(e).

⁶ [Reglamento general de protección de datos, Reglamento de la UE 2016/679](#), art. 5(1)(f).

⁷ [Reglamento general de protección de datos, Reglamento de la UE 2016/679](#), art. 5(2).

- Comprobar si los datos que deben recopilarse están relacionados con "categorías especiales de datos personales" (definidos en el art 9.1 del RGPD). En ese caso, se requieren requisitos adicionales para tratar esos datos, como contar con el consentimiento explícito del interesado, o basarse en una ley que permita dicha recogida para fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.
- Comprobar si los datos que deben recogerse están relacionados con "condenas e infracciones penales", en cuyo caso se aplicarán leyes especiales.

Antecedentes

De acuerdo con la legislación europea, todo tratamiento de datos personales debe realizarse con un fin lícito y una finalidad legítima. Mientras que los demás principios establecen limitaciones sobre cómo pueden tratarse los datos personales, este principio impone restricciones a los fines para los que pueden tratarse los datos personales.

Base legal

El RGPD establece seis bases⁸ jurídicas para el tratamiento legal de los datos personales. Así, para que el tratamiento de datos personales sea considerado lícito debe reunir una de las siguientes condiciones:

- Medie el consentimiento del individuo
- El tratamiento sea necesario para la ejecución de un contrato
- Sea necesario para el cumplimiento de una obligación legal.
- Sea necesario para proteger los intereses vitales de una persona.
- El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
- Sea necesario para perseguir intereses legítimos del responsable del tratamiento, siempre que esos intereses no prevalezcan sobre los intereses del titular de los datos.

Cabe señalar que, a diferencia de las instituciones privadas, las autoridades públicas no están autorizadas a utilizar el "interés legítimo" como finalidad, a menos que el tratamiento quede fuera del ámbito de las tareas de la autoridad pública. Además, la "necesidad" y el "interés público" implican una "necesidad social apremiante", en contraposición a las ventajas ampliamente privadas o comerciales.⁹

Si se utiliza el "consentimiento" como base, es importante que la finalidad se especifique de forma clara y explícita, y que revele, explique o exprese de forma fácilmente comprensible por qué se recogen y tratan los datos. El propio consentimiento

debe ser libre, específico, informado e inequívoco, y la persona tiene derecho a retirarlo en cualquier momento.

⁸ Reglamento general de protección de datos, Reglamento de la UE 2016/679, art. 6.

⁹ Supervisor Europeo de Protección de Datos, "A Preliminary Opinion on Data Protection and Scientific Research",23 .

El RGPD reconoce que "Con frecuencia no es posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida. Por consiguiente, debe permitirse a los interesados dar su consentimiento para determinados ámbitos de investigación científica que respeten las normas éticas reconocidas para la investigación científica. Los interesados deben tener la oportunidad de dar su consentimiento solamente para determinadas áreas de investigación o partes de proyectos de investigación, en la medida en que lo permita la finalidad perseguida"¹⁰

El Supervisor Europeo de Protección de Datos (SEPD) señala que "el consentimiento específico que normalmente se exige en el marco del RGPD puede resultar menos apropiado en el caso de los datos recogidos e inferidos y, especialmente, en el caso de las categorías especiales de datos en las que se basa gran parte de la investigación científica", y, por tanto, "cuando los fines de la investigación no pueden especificarse plenamente, se espera que un responsable del tratamiento haga más para garantizar la esencia de los derechos del interesado a un consentimiento válido, incluso mediante la mayor transparencia posible y otras salvaguardias".¹¹

Lealtad

La forma en que se realiza el tratamiento debe ser justa y transparente. Incluso si el tratamiento que se realiza tiene una base legal, puede ser injusto y, por tanto, violar este principio. La lealtad es un concepto amplio: requiere que los investigadores sólo traten los datos personales de la manera que la gente esperaría razonablemente, y que no hagan nada que pueda perjudicar a los interesados.

Transparencia

La transparencia exige que se informe a las personas sobre los fines previstos para la recogida y el uso de los datos personales, los fundamentos jurídicos del tratamiento, etc. Esto es necesario tanto si hay una recogida de datos personales de los individuos afectados (ya sean proporcionados conscientemente por el individuo, o recogidos a través de la observación del individuo), u obtención de datos personales de alguna otra fuente (como un tercero al que se le han confiado los datos, fuentes públicas, intermediarios de datos, o de otros individuos). ¹² La información que debe proporcionarse, como mínimo, incluye:¹³

¹⁰ Reglamento general de protección de datos, Reglamento de la UE 2016/679, considerando 33.

¹¹ Supervisor Europeo de Protección de Datos, "A Preliminary Opinion on Data Protection and Scientific Research",19 .

¹² Reglamento general de protección de datos, Reglamento de la UE 2016/679, Art. 12(1), (5), (7), Art. 13, Art. 14, Considerandos 58-6239.

¹³ Comisión Europea, "¿Qué información debe darse a las personas cuyos datos se recogen?".

- quién es su empresa/organización (sus datos de contacto y los de su DPO, si lo hay);
- por qué su empresa/organización utilizará sus datos personales (fines);
- las categorías de datos personales tratados;
- la justificación legal para el tratamiento de sus datos;
- durante cuánto tiempo se conservarán los datos;
- quién más podría recibirlo;
- si sus datos personales serán transferidos a un destinatario fuera de la UE;
- que tienen derecho a una copia de los datos (derecho de acceso a los datos personales) y otros derechos básicos en el ámbito de la protección de datos (véase la lista completa de derechos);
- su derecho a presentar una reclamación ante una Autoridad de Protección de Datos (APD);
- su derecho a retirar el consentimiento en cualquier momento;
- en su caso, la existencia de una toma de decisiones automatizada y la lógica que conlleva, incluidas sus consecuencias.

En caso de que haya obtenido datos personales de una fuente distinta a las personas afectadas, tiene que informarles en un plazo razonable, y como máximo en un mes desde que tuvo acceso a sus datos personales.

Las obligaciones de transparencia no se aplican cuando, y en la medida en que, el interesado ya dispone de la información.¹⁴ En el caso de los datos personales recogidos de una tercera fuente, hay tres situaciones adicionales en las que no se aplican las obligaciones de transparencia:¹⁵

Categorías especiales de datos personales / Datos sensibles

Las categorías especiales de datos personales, o datos sensibles, ¹⁶son datos que se refieren al:

- origen racial o étnico,
- opiniones políticas,

- creencias religiosas o filosóficas,
- la afiliación sindical;
- 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 a la orientación sexual de una persona física.

Estos datos sensibles no pueden ser recogidos a menos que la recogida se enmarque en uno de los diez motivos legítimos previstos en el RGPD.¹⁷ Entre ellos se incluyen el consentimiento explícito del interesado, así como que la recogida de los datos se utilice para fines de archivo, investigación científica o histórica, y este tratamiento observe ciertas garantías que se indican en el RGPD.¹⁸ No obstante, existen diferencias nacionales en las leyes que regulan los datos sensibles, y especialmente los datos genéticos, biométricos y de salud. Consiguientemente, es recomendable que los ¹⁹investigadores consulten al responsable de protección de datos de su institución, o a su autoridad local de protección de datos para informarse con más detenimiento a la hora de tratar este tipo de datos.

Además, aunque los datos relativos a las condenas e infracciones penales no están clasificados como "sensibles" en el marco del RGPD, el reglamento exige que todo uso de estos datos por parte de los investigadores esté además autorizado por una ley nacional o de la UE, y siga las salvaguardias previstas en dicha ley.²⁰

¹⁶ Reglamento general de protección de datos, Reglamento de la UE 2016/679, art. 9(1), considerandos 51-56.

¹⁷ Reglamento general de protección de datos, Reglamento de la UE 2016/679, art. 9(2)(a).

¹⁸ Reglamento general de protección de datos, Reglamento de la UE 2016/679, art. 89.

¹⁹ Reglamento general de protección de datos, Reglamento de la UE 2016/679, art. 9(4).

²⁰ Reglamento general de protección de datos, Reglamento de la UE 2016/679, art. 10.

2.2. Limitación de la finalidad

Para cumplir con el principio de limitación de la finalidad, los investigadores deben:

- Documente en términos claros y específicos los propósitos de la recopilación y el uso de los datos personales.
- Proporcionar a los individuos información sobre los propósitos que justifican la recolección y uso de sus datos.
- Limitar el tratamiento de los datos personales a los fines especificados o a fines compatibles.
- Garantizar que se notifica a las personas del tratamiento de sus datos en aquellas situaciones en las que los datos se recogieron a partir de una base legal distinta al consentimiento. Esto debe hacerse con una antelación razonable al nuevo uso de

los datos personales, para que la persona tenga la oportunidad de oponerse al tratamiento.

- Asegurarse de que solicitan un nuevo consentimiento en aquellas situaciones en las que el motivo original para el uso de los datos personales era el consentimiento, y ahora esos datos se destinan a cualquier otro uso (independientemente de que el nuevo uso sea "compatible").
- Asegurarse de que cuentan con el consentimiento o con una clara obligación/función prevista en el interés público en una ley si desean utilizar los datos personales para fines distintos de los especificados o compatibles.
- Asegúrese de que el nuevo uso es justo, legal y transparente.

Antecedentes

La finalidad con la que se tratan los datos debe ser "específica, explícita y legítima".²¹ El Grupo de Trabajo del Artículo 29 señala que "una finalidad vaga o general, como por ejemplo ... 'investigación futura', sin más detalles

— normalmente no cumplen los criterios de ser "específicos". Dicho esto, el grado de detalle con el que debe especificarse una finalidad para el tratamiento depende del contexto particular en el que se recojan los datos y la naturaleza de dichos datos. En algunos casos claros, un lenguaje sencillo será suficiente para proporcionar una especificación adecuada, mientras que en otros casos puede ser necesario un mayor detalle."²²

Solo se pueden procesar datos atendiendo a las siguientes finalidades:

- los fines legítimos que se especificaron explícitamente al recoger los datos, u
- otros fines que sean compatibles con los fines iniciales.

La compatibilidad puede juzgarse utilizando los siguientes criterios:

²¹ [Reglamento general de protección de datos, Reglamento de la UE 2016/679](#), art. 5(1)(b).

²² [Artículo Grupo de Trabajo de 29 Protección de Datos, "Dictamen 03/2013 sobre la limitación de la finalidad"](#), 15-16.

- a) el vínculo entre los fines iniciales y los fines adicionales que se están considerando;
- b) el contexto en el que se han recogido los datos personales, en particular en lo que respecta a la relación entre los interesados y el responsable del tratamiento;
- c) la naturaleza de los datos personales, en particular si incluyen categorías especiales de datos personales (es decir, sensibles) o se tratan datos personales relacionados con condenas e infracciones penales
- d) las posibles consecuencias del tratamiento posterior previsto para los interesados;
- e) la existencia de garantías adecuadas, que pueden incluir la seudonimización.

Algunos de los fines que se presumen compatibles, si se siguen las salvaguardas adecuadas y legalmente establecidas, son:

- archivo de interés público,
- investigación científica o histórica, y
- estadísticos

Sin embargo, como señala el SEPD, "la presunción no es una autorización general para seguir tratando datos en todos los casos con fines históricos, estadísticos o científicos. Cada caso debe considerarse según sus propios méritos y circunstancias. Pero, en principio, los datos personales recogidos en el contexto comercial o sanitario, por ejemplo, pueden seguir utilizándose con fines de investigación científica, por el responsable original o por un nuevo responsable, si se establecen las garantías adecuadas... para garantizar el respeto de los derechos del interesado, la prueba de compatibilidad prevista en el artículo 6.4 debe seguir considerándose antes de la reutilización de los datos con fines de investigación científica, en particular cuando los datos se recogieron originalmente con fines muy diferentes o fuera del ámbito de la investigación científica."²³

2.3. Minimización de datos

Para estar en consonancia con el principio de minimización de datos, los investigadores deben:

- Asegurarse de que sólo recogen datos personales si son adecuados, pertinentes y necesarios para la finalidad que han especificado.
- Abstenerse de recoger más datos personales de los necesarios.
- Abstenerse de recopilar tipos de datos personales más detallados o granulares de lo necesario.

²³ Supervisor Europeo de Protección de Datos, "A Preliminary Opinion on Data Protection and Scientific Research", 22-23.

- Asegurarse de que no almacenan los datos personales durante más tiempo del necesario.
- Revisar los datos personales que almacenan periódicamente para comprobar si siguen cumpliendo con los requisitos anteriores, y eliminar los datos en caso contrario.

Antecedentes

La adecuación, la pertinencia y la necesidad son tres requisitos para el tratamiento de datos personales según el RGPD. Así, los datos inadecuados, es decir, no aptos para la finalidad especificada, no pueden recogerse ni tratarse; los datos también deben ser pertinentes, es

decir, deben servir para la finalidad especificada. Y la limitación de la necesidad tiene tres aspectos:

- cantidad de datos;
- la granularidad de los datos, y
- la duración del almacenamiento (que se trata con más detalle en el principio de "limitación del almacenamiento" más adelante)

Así, resumidamente, los investigadores deben tratar de recoger, almacenar y procesar la menor cantidad de datos personales que sea necesaria, y durante el menor tiempo posible para lograr el propósito especificado. Esto, al igual que otros principios, se consigue mediante la implementación de medidas técnicas y organizativas.

La minimización de los datos figura como una preocupación especial en el RGPD para aquellos que procesan datos personales con fines de archivo en el interés público, fines de investigación científica o histórica, o fines estadísticos, ya que estos operan bajo un régimen ligeramente relajado en lo que respecta al principio de limitación de la finalidad. Entre las medidas que pueden adoptarse para la minimización de los datos figura la seudonimización, siempre que sea factible.

2.4. Precisión

Para cumplir con el principio de precisión, los investigadores deben:

- Garantizar que los datos personales que tienen son correctos.
- Asegurarse de que los datos personales que tienen están actualizados.
- Establezca procesos para comprobar la exactitud de los datos, con plazos para comprobar la actualidad.
- Corrija cualquier dato incorrecto o engañoso tan pronto como lo descubra.
- Registre los errores que deban conservarse como tales, junto con el motivo de su conservación.
- Cumplir con las solicitudes de rectificación de los particulares.

Antecedentes

El principio de exactitud tiene dos aspectos: la corrección de los hechos y la actualización. Está prohibido utilizar datos personales inexactos, ya que podrían ser inadecuados para el fin para el que se recogieron. Además, los datos inexactos podrían perjudicar a los interesados, por lo que podrían violar el principio de equidad. Así pues, los investigadores tienen la obligación de borrar o corregir los datos personales inexactos.

Para garantizar la exactitud de sus datos personales, los interesados tienen derecho a solicitar la rectificación de los mismos.

2.5. Limitación de almacenamiento

Para garantizar el cumplimiento del principio de limitación del almacenamiento, los investigadores deben:

- Garantizar que no se almacenan los datos personales durante más tiempo del necesario para los fines que se recogieron.
- Asegurarse de que eliminan o anonimizan los datos personales que ya no son necesarios.
- Documente la finalidad para la que se recogieron los datos personales y el tiempo que es necesario conservar los datos para lograr esa finalidad.
- Documente la justificación del período de conservación.
- Revisar la necesidad de conservación cuando finaliza el periodo de conservación preestablecido.
- Identificar y documentar el archivo de interés público, la investigación científica o histórica, o la finalidad estadística para la que se almacenan los datos durante más tiempo del estrictamente necesario, en caso de que los datos se almacenen en virtud de la excepción para este tipo de investigación, junto con el cumplimiento de las garantías adecuadas, según lo prescrito legalmente en el artículo. 89 del RGPD.

Antecedentes

Los investigadores no deben conservar los datos personales durante más tiempo del necesario para los fines especificados para los que fueron recogidos. Los datos deben destruirse tan pronto como dejen de ser necesarios para los fines especificados.

Una de las formas de lograrlo es la anonimización de los datos siempre que sea posible, convirtiendo los datos personales en datos que ya no permiten la identificación directa o indirecta de los sujetos a los que pertenecen.

Los investigadores están autorizados a conservar los datos personales durante más tiempo del estrictamente necesario si los datos personales se van a utilizar únicamente con fines de archivo en el interés público, con fines de investigación científica o histórica o con fines estadísticos, y si además cumplen las condiciones establecidas en el artículo 89 del RGPD y establecen garantías adecuadas en forma de medidas técnicas y organizativas apropiadas para salvaguardar los derechos del interesado. Además, los investigadores deben asegurarse de que no utilizan estos datos personales como base para ninguna medida o decisión relativa a una persona concreta.²⁴

2.6. Integridad y confidencialidad

Para cumplir con el principio de integridad y confidencialidad, los investigadores deben

- Garantizar que los datos personales se conservan de forma segura, protegiéndolos contra el tratamiento no autorizado o ilegal, y contra la pérdida, destrucción o daño accidentales, utilizando tanto medidas técnicas como organizativas.
- Documentar las medidas técnicas y organizativas que se aplican para garantizar la seguridad.

Contexto:

Los investigadores están obligados a garantizar la seguridad de los datos personales, es decir, a asegurar la confidencialidad, la integridad y la disponibilidad de los datos y, por lo tanto, a protegerlos contra el tratamiento no autorizado o ilegal y contra la pérdida, la destrucción o el daño accidentales, utilizando tantos medios técnicos como organizativos.

Por lo tanto, la seguridad de los datos es una parte fundamental de la protección de los datos personales. A la hora de determinar si se han cumplido la confidencialidad y la integridad, es importante analizarlo desde la perspectiva de los interesados, y no desde la perspectiva de los investigadores. En otras palabras, aunque los investigadores no hayan sufrido ningún daño a causa del tratamiento no autorizado, eso no puede llevarnos a presuoner que no se haya derivado un daño que afecte a los interesados.

Esto significa que los investigadores tienen que haber designado claramente las funciones y responsabilidades para que quede claro quiénes tienen autorizado el acceso a los datos personales, especificando también investigaciones concretas.

²⁴ Artículo Grupo de Trabajo de 29Protección de Datos, "Dictamen 03/2013 sobre la limitación de la finalidad",28 .

2.7. Rendición de cuentas

Para cumplir con el principio de rendición de cuentas (responsabilidad proactiva), los investigadores deben:

- Asegurarse de que cumplen con la ley de protección de datos de forma proactiva y organizada.
- Conozca las obligaciones que se les imponen y los derechos que tienen las personas ante la ley.
- Establecer políticas, procesos y medidas técnicas claras que garanticen el cumplimiento de los principios anteriores y de la ley.
- Garantizar que se sigue el enfoque de "privacidad por diseño y por defecto".

- Asegúrese de que su organización cuenta con un delegado protección de datos en caso de que sea una autoridad u organismo público; si realiza un seguimiento regular y sistemático de las personas a gran escala; o si trata una gran cantidad de datos sensibles.
- Llevar a cabo una evaluación de impacto sobre la protección de datos si el tipo de tratamiento de datos que desean llevar a cabo puede suponer un riesgo elevado, y en particular si tienen previsto utilizar la elaboración sistemática y extensa de perfiles con efectos significativos; tratar datos de categoría especial o de delitos penales a gran escala; o controlar sistemáticamente lugares de acceso público a gran escala.
- Notificar a las personas, normalmente a través del delegado de la protección de datos de su institución, de una violación de datos a más tardar en el plazo de 72 horas, si es probable que la violación suponga un riesgo para los derechos y libertades de las personas cuyos datos personales hayan sido violados.
- Responder inmediatamente a cualquier ejercicio de los derechos de las personas sobre sus datos.
- Documentar el cumplimiento de todos los principios anteriores.

Contexto:

Quienes recogen y utilizan datos personales, como los investigadores, son responsables del cumplimiento de los principios mencionados. Y lo que es más importante, deben ser capaces de demostrar que los cumplen.

Por lo tanto, el cumplimiento de estos principios debe planificarse y documentarse. Por ejemplo, los investigadores deben poder justificar por qué necesitan determinados datos personales con la granularidad con la que los recogen y la duración de su almacenamiento. Muchos aspectos de la rendición de cuentas se beneficiarían de la aplicación de medidas técnicas automatizadas.

3 Buenas prácticas relacionadas con los principios de protección de datos

Las buenas prácticas para los principios de protección de datos abarcan prácticas que van más allá del mínimo legalmente exigido por el RGPD y las leyes nacionales. Aunque no son legalmente obligatorias, ayudarán a los investigadores a cumplir con los principios de protección de datos ya señalados en este documento.

3.1. Anonimización, seudonimización y cifrado

Los diversos requisitos del RGPD no se aplican si los investigadores no manejan *datos personales*. Siempre que sea posible compruebe si los datos que se necesitan para la investigación tengan la capacidad de identificar a una persona, y, por tanto, entren dentro de la categoría de datos personales. Asimismo, debe tener en cuenta que el RGPD distingue entre datos seudonimizados y datos anonimizados. La simple eliminación de todos los identificadores personales no convierte automáticamente los datos en "anónimos".

Los datos personales seudónimos se refieren a los datos personales que ya no pueden atribuirse a un sujeto de datos específico sin el uso de información adicional.

En el caso de los datos anonimizados, no solo no se debe poder identificar a ninguna persona en particular sobre la base de los datos que se han recogido y procesado, sino que también hay que tener en cuenta todos los medios que otros pueden encontrar "razonablemente probables para ser utilizados, como la identificación ... para identificar a la persona física directa o indirectamente". Para ver qué medios "es razonablemente probable que se utilicen para identificar a la persona física", el RGPD señala que "deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta la tecnología disponible en el momento del tratamiento y la evolución tecnológica". "Por lo tanto, si es posible en la práctica acceder a indicadores que revelen la identidad de la persona, no se puede considerar que se trata de datos anonimizados, sino de datos seudonimizados que siguen siendo datos personales.

El RGPD sugiere la seudonimización y el cifrado como dos medios para garantizar una mayor seguridad de los datos personales. Ambas técnicas ayudarían a cumplir los requisitos del principio de integridad y confidencialidad. La seudonimización también ayudaría a cumplir el principio de minimización de los datos. En el caso de algunos tipos de tratamiento de datos para la investigación científica, para los que el principio de limitación de la finalidad está ligeramente relajado, el RGPD exige que los investigadores traten de minimizar los datos, y que lo hagan utilizando la seudonimización siempre que sea posible o anonimizando los datos si eso es factible.²

3.2. Datos agregados y gruesos

Siempre que sea posible, prefiera los datos agregados a los datos a nivel individual, y prefiera los datos gruesos a los granulares. Por ejemplo, si se necesitan datos sobre la edad, opte por recogerlos en forma de número en lugar de la fecha de nacimiento. Mejor aún, si basta con un rango de edad, opte por recogerlo en lugar de una edad precisa. Por último, si se puede agregar la fecha de varias personas y destruir los datos a nivel individual, opte por hacerlo.

3.3. Transparencia

Si los datos personales se recogen en un contexto en línea, proporcione un enlace destacado a la declaración o aviso de privacidad, o asegúrese de que la información esté disponible en la misma página en la que se encuentran los datos personales

¹ Reglamento general de protección de datos, Reglamento de la UE 2016/679, considerando 26.

² Reglamento general de protección de datos, Reglamento de la UE 2016/679, art. 89(1).

recogidos.³ Si se producen cambios en el tratamiento de los datos personales, debe proporcionarse de nuevo toda la información al interesado, facilitando al mismo tiempo que se sepa qué información de la misma es nueva.⁴

3.4. Múltiples bases jurídicas para el tratamiento

El RGPD parece permitir la posibilidad de utilizar múltiples bases legales para el tratamiento de los mismos datos personales. Sin embargo, esto podría llevar a una situación en la que se utilicen dos bases jurídicas (como el consentimiento del interesado y el interés legítimo del), pero uno de ellos acabe por desaparecer (por ejemplo, por la revocación del consentimiento). En tal caso, no está claro qué exige la ley, y no existe una opinión unánime entre las autoridades de protección de datos. Es preferible resolver esta incertidumbre mediante una comprensión conservadora de la ley, y dejar de procesar cualquier dato cuando desaparezca alguna de las causas jurídicas que permitieron su procesamiento. Para evitar esta situación se sugiere no combinar el consentimiento con ninguna otra base jurídica. En estos casos, puede ser preferible optar por tratar los datos únicamente en virtud del motivo más adecuado.

3.5. El consentimiento en la protección de datos y en la ética

El consentimiento como base legal para el tratamiento de datos en virtud de la ley de protección de datos es diferente del "consentimiento informado" como principio ético para la investigación con seres humanos.⁵ Por lo tanto, siempre es preferible proporcionar formularios de consentimiento separados y obtener cada tipo de consentimiento por separado. Incluso si la institución obtiene ambos mediante un único formulario de consentimiento, debe mantenerse un registro claro de lo que cada participante ha consentido en relación con la investigación.

Téngase en cuenta que en los casos en los que el consentimiento no se utiliza como motivo en virtud del RGPD, "el *consentimiento informado* como participante en una investigación humana podría servir como una "salvaguardia adecuada" de los derechos del sujeto de los datos."⁶

3.6. Legitimidad, lealtad y aprobaciones éticas

La legitimidad de la recopilación de datos a veces estará determinada por leyes que prescriben requisitos éticos (como en el caso de los ensayos clínicos). Pero incluso cuando una investigación específica no está cubierta por los requisitos legales de autorización ética,

es mejor trabajar con la presunción de que la recopilación o el uso de datos no éticos también se considerará un propósito ilegítimo para la base del GDPR, así como el incumplimiento del principio de lealtad. Así, por ejemplo, los investigadores deben abstenerse de realizar cualquier tratamiento de datos que un comité de revisión ética desapruébe.

3.7. Autoridades de protección de datos y comités de ética

Dada la creciente interrelación entre las cuestiones éticas y las relativas a la privacidad y la protección de datos, sería provechoso que los comités de revisión ética se comprometieran más con los responsables y autoridades de la protección de datos.⁷ Hay muchos casos (como en el de los datos genéticos) en los que el uso de los datos personales de un individuo en la investigación afectaría no sólo a ese individuo, sino también a otros. El marco de la protección de datos por sí solo puede ser inadecuado para captar esas preocupaciones del modo en que podría hacerlo un marco combinado de ética de la investigación y protección de datos. Esto exige una mayor colaboración entre los que trabajan en cuestiones éticas y quienes son expertos en materia de protección de datos.

³ Artículo Grupo de Trabajo de 29Protección de Datos, "Directrices sobre la transparencia en el marco del Reglamento 2016/679",8 .

⁴ Artículo Grupo de Trabajo de 29Protección de Datos, 27-28.

⁵ Supervisor Europeo de Protección de Datos, "A Preliminary Opinion on Data Protection and Scientific Research", 19-20.

⁶ Supervisor Europeo de Protección de Datos,20 .

⁷ Supervisor Europeo de Protección de Datos,25 .

3.8. Directrices de protección de datos y DPD

Muchas instituciones de investigación han publicado directrices de protección de datos, además de las directrices éticas. Los investigadores deben familiarizarse con las directrices de su institución. Muchas veces, los financiadores también tienen requisitos especiales en materia de protección de datos. Todos los proyectos financiados por Horizonte 2020, por ejemplo, requieren la participación de un delegado de protección de datos si se ha designado uno, e incluso en los casos en que no se requiere legalmente un DPD, es necesario elaborar ⁸una política de protección de datos.

Hay algunas cuestiones a las que se aplica la legislación de los Estados miembros, y no sólo el RGPD. Es importante señalar el régimen especial de protección de datos para el tratamiento con fines de archivo en interés público, de investigación científica o histórica, o con fines estadísticos, puede ser menos exigente para el investigador, si las leyes nacionales así lo permiten. El tratamiento de datos personales para cualquiera de estos fines requiere de las garantías adecuadas. Los investigadores deben respetar los principios mencionados anteriormente y prestar especial atención a las medidas

técnicas y organizativas para garantizar la minimización de los datos.⁹ Dado que los detalles de las obligaciones de los investigadores en virtud de la ley no son uniformes, los investigadores deben consultar al delegado de protección de datos de su institución y las directrices de protección de datos, si es posible, ya que podrán ayudar a orientar a los investigadores sobre las normas legales y extralegales aplicables.

3.9. Evaluación del impacto de la protección de datos

Si un proyecto va a tratar una gran cantidad de datos personales, o los datos personales de personas vulnerables, sería beneficioso discutir dicho proyecto con el DPD y realizar una evaluación de impacto sobre la protección de datos (EIPD), incluso cuando no sea legalmente obligatorio hacerlo. El SEPD señala que "la EIPD es obligatoria para las operaciones de tratamiento de datos que presenten riesgos elevados para los interesados, como cuando se dan dos de los criterios siguientes":¹⁰ 1. Se realicen evaluaciones sistemáticas y/o se generen perfiles. 2. Se realicen toma de decisiones automatizada 3. Se de una vigilancia o supervisión sistemática 4. Se traten datos sensibles 5. El Tratamiento se dé una gran escala 6. Se combinen un conjunto de datos con fines diferentes. 7. Los interesados sean vulnerables. 8. Se utilicen nuevas tecnologías 9. El tratamiento pueda impedir que las personas ejerzan sus derechos o suscriban un servicio/contrato.

⁸ Reglamento general de protección de datos, Reglamento de la UE 2016/679, art. 38.

⁹ Reglamento general de protección de datos, Reglamento de la UE 2016/679, art. 89.

¹⁰ Supervisor Europeo de Protección de Datos, "Decisión del Supervisor Europeo de Protección de Datos de julio16 sobre las listas de 2019EIPD emitidas en virtud del artículo 39, apartados 4 y 5, del Reglamento (UE) 2018/1725", anexo 1.

4 Anexos

4.1. Anexo 1: Recursos clave

El proyecto PANELFIT ha elaborado un conjunto detallado de directrices sobre protección de datos y cuestiones éticas y jurídicas en la investigación e innovación en el ámbito de las TIC, así como un análisis crítico del marco regulador de la protección de datos en el ámbito de las TIC. El CCDP se basa en gran medida en esos dos documentos. Aquellos que deseen comprender mejor las cuestiones planteadas en el CCDP o que quieran entender los aspectos de la protección de datos que no se trataron en el CCDP, deben consultar las Directrices, que ofrecen muchos más detalles.

Ambos estarán disponibles en <https://www.panelfit.eu/deliverables/>.

A continuación se presentan otros recursos importantes para los investigadores que deseen saber más sobre la protección de datos y la investigación e innovación responsables.

- Supervisor Europeo de Protección de Datos. "A Preliminary Opinion on Data Protection and Scientific Research" (Dictamen preliminar sobre la protección de datos y la investigación científica), enero https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_2020_research_en.pdf.
- Artículo Grupo de Trabajo de 29Protección de Datos. "Opinion 03/2013 on Purpose Limitation", abril2,2013. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.
- Artículo Grupo de Trabajo de 29Protección de Datos. "Dictamen 05/2014 sobre técnicas de anonimización", abril https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/10_2014/wp216_en2014.pdf *.
- Artículo Grupo de Trabajo de 29Protección de Datos. "Guidelines on Transparency under Regulation 2016/679", noviembre h29,2017. <https://ec.europa.eu/newsroom/article29/items/622227>.
- Consejo Europeo de Protección de Datos. "Directrices 03/2020 sobre el tratamiento de datos relativos a la salud con fines de investigación científica en el contexto del brote de COVID-19. " Directrices, abril 30, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2020_healthdatascientificresearchcovid19_en202003.pdf.
- Consejo Europeo de Protección de Datos. "Directrices /20194 sobre el artículo Protección 25de datos por diseño y por defecto. " Directrices, noviembre https://edpb.europa.eu/sites/edpb/files/consultation/13_edpb_guidelines_201904_dataprotection_by_design_and_by_default2019..pdf.
- Consejo Europeo de Protección de Datos. "Directrices 04/2019 sobre el artículo 25: Protección de datos por diseño y por defecto. " Directrices, octubre https://edpb.europa.eu/sites/edpb/files/files/file1/20_edpb_guidelines_201904_dataprotection_by_design_and_by_default_v22020.0_en.pdf.
- Supervisor Europeo de Protección de Datos. "Directrices del SEPD sobre la evaluación de la proporcionalidad de las medidas que limitan los derechos fundamentales a la intimidad y a la protección de los datos personales", diciembre https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_19_proportionality_guidelines2_en2019..pdf.

- Supervisor Europeo de Protección de Datos. "Diagramas de flujo y listas de comprobación sobre la protección de datos." 2020. <https://doi.org/10.2804/823679>.
- Comisión Europea (Dirección General de Investigación e Innovación). "Ethics and Data Protection", noviembre 2018. https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf.
- ALLEA. *Código europeo de conducta para la integridad de la investigación*. 2ª ed., 2017. https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020-ethics_code-of-conduct_en.pdf.
- Proyecto RESPECT. "Código de prácticas de RESPECT para la investigación socioeconómica." Instituto de Estudios Laborales, 2004. http://www.respectproject.org/code/respect_code.pdf
- EFAMRO y ESOMAR. "Guidance Note for the Research Sector: Appropriate Use of Different Legal Bases under the GDPR." Junio 2017. https://www.esomar.org/uploads/public/government-affairs/position-papers/EFAMRO-ESOMAR_GDPR-Guidance-Note_Legal-Choice.pdf.
- Wilford, Sara, Malcolm Fisk y Bernd Stahl. "Directrices para la investigación e innovación responsables." Proyecto GREAT, 2016. <https://www.great-project.eu/Deliverables10>.
- El Consejo Europeo de Protección de Datos ha declarado que "tiene la intención de publicar orientaciones sobre las condiciones "horizontales y complejas" para la aplicabilidad de la "presunción de compatibilidad" del tratamiento posterior con fines de archivo en interés público, investigación científica e histórica o fines estadísticos, según lo dispuesto en el artículo 5.1.b del RGPD. "Esto será útil para los investigadores cuando se publique.

4.2. Anexo 2: Bibliografía

Grupo de Trabajo del Artículo 29 Protección de Datos. Directrices sobre la transparencia en el marco del Reglamento 2016/679"29, noviembre 2017. <https://ec.europa.eu/newsroom/article29/items/622227>.

---. "Dictamen 03/2013 sobre la limitación de la finalidad"2, abril 2013. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

Comisión Europea. Ciencia con y para la sociedad". Horizonte Noviembre 2020, 112013. <https://ec.europa.eu/programmes/horizon2020/en/h2020-section/science-and-society>.

---. ¿Qué información debe darse a las personas cuyos datos se recogen? ! Texto. Principio del RGPD - ¿Qué información debe darse a las personas cuyos datos se recogen?, enero 2018. <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business->

[and-organisations/_____principles-gdpr/what-information-must-be-given-individuals-whose-data-collected_en.](#)

Consejo Europeo de Protección de Datos. Dictamen del Consejo (art. 70.I.b)".
Dictamen, enero
23h2019.https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_en.pdf.

Supervisor Europeo de Protección de Datos. Dictamen preliminar sobre la protección de datos y la investigación científica", enero
h2020.https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.

---. 'Decisión del Supervisor Europeo de Protección de Datos de julio16 sobre las listas de 2019EIPD emitidas en virtud de los apartados 4 y 5 del artículo 39 del Reglamento (UE) 2018/1725', julio https://edps.europa.eu/162019.sites/default/files/publication/19-07-16_edps_dpia_list_en.pdf.

Reglamento General de Protección de Datos, Reglamento UE 2016/679 (2016).
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504>.

"Declaración de Roma sobre Investigación e Innovación Responsables en Europa",
noviembre212014. https://ec.europa.eu/research/swafs/pdf/rome_declaration_RRI_final_21_November.pdf.

4.3. Anexo 3: Proceso de creación del Código de Conducta sobre Protección de Datos para la Investigación e Innovación Responsables

Hemos tratado de involucrar a múltiples partes interesadas en la revisión del CCDP y de obtener el mayor número posible de comentarios. El proceso de consulta se describe a continuación.

El primer borrador del CCDP se distribuyó en octubre y 2020 la versión final se consolidó en agosto. Se generaron cinco versiones en diferentes etapas del proceso, incorporando los comentarios en cada paso. Las siguientes secciones resumen el proceso de retroalimentación del CCDP, recogen los comentarios más significativos recibidos y los pasos dados para responder en cada caso.

A continuación, se describe el alcance de cada una de las etapas de retroalimentación:

¹ Consejo Europeo de Protección de Datos, "Dictamen del Consejo (Art. 70.I.b)".

- Consulta de expertos internos (PANELFIT): la primera versión del CCDP generada en octubre fue 2020revisada por el consorcio del Proyecto PANELFIT que incluye expertos en ciberseguridad, gobernanza, privacidad y protección de datos, entre otros.

- Consulta de expertos externos (partes interesadas): esta consulta se realizó a través del Encuentro de Aprendizaje Mutuo para partes interesadas organizado por el proyecto. En este evento online celebrado en abril se reunieron personas 202021, 13 de las siguientes organizaciones ALLEA, Grupo Europeo de Ética (EGE) de la Comisión Europea, Universidad de Vilnius, NEC Laboratories Europe, Tech Uni Cluj-Napoca, Museum for Naturkunde, COCIR, Universidad Babes-Bolyai, Research Centre for Data Science y Senior Lecturer, School of Computing, Electronics and Mathematics at Coventry University, Uni Babes Bolyai, European Commission, Open Science (DG RTD), Tilburg University, School of Computing, Electronics and Mathematics at Coventry University, University of Copenhagen.

- Consulta de investigadores externos: investigadores de diversas disciplinas participaron en el Encuentro de Aprendizaje Mutuo para investigadores organizado por el proyecto. El evento en línea se celebró en junio 242021.

- Consulta pública: el PDC se publicó en el sitio web de PANELFIT con un formulario disponible para recibir comentarios de cualquier persona interesada. Se promovió la participación en los comentarios a través de las redes sociales y las listas de correo. El documento estuvo disponible de marzo a agosto en 2021 el siguiente enlace: <https://www.panelfit.eu/a-code-of-conduct-on-data-protection-for-responsible-research-and-innovation-ccdp/>

- Encuesta a los investigadores: la encuesta formaba parte del proceso de cierre de la información del CCDP. Se distribuyó antes, durante y después de la EML para los investigadores. Los comentarios contribuyeron a mejorar la sección de buenas prácticas.