COMISIÓN
EUROPEA

Bruselas, 14.10.2022
COM(2022) 530 final

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO

Primer informe sobre la aplicación del Reglamento de Protección de Datos en las instituciones, órganos y organismos de la Unión Europea (Reglamento 2018/1725)

Contenido

1 Introduction 2

2 Separate data protection rules for EU institutions, bodies, offices and agencies aligned with EU data protection legislation 3

3 Implementation of the EUDPR in EUIBs 4

3.1 EUIB's role as controllers 4

3.2 Exercise of data subjects' rights 5

3.3 Restricting data subject rights through internal rules 5

3.4 Data protection officers 6

3.5 Data protection impact assessments 7

3.6 International data transfers 8

4 EDPS activities 9

4.1 The EDPS as the data protection supervisory authority for EUIBs 9

4.2 The EDPS as adviser to the EU legislator 11

4.3 Cooperation between the EDPS and national data protection authorities 12

4.4 EDPS resources 13

5 Commission's use of empowerments to adopt delegated and implementing acts 14

6 Data protection rules for bodies and agencies dealing with police cooperation and judicial cooperation in criminal matters 14

6.1 Extending the application of the EUDPR's law enforcement chapter 15

6.2 Clarifying the applicability of certain EUDPR provisions to the processing of operational data 16

6.3 The EDPS's powers in supervising EU bodies and agencies 17

7 Way forward 17

ANNEX 20

1 Introducción

El Reglamento de protección de datos para las instituciones, órganos y organismos de la Unión Europea[1] («RPDUE») es el principal[2] marco para la protección de datos cuando las instituciones, órganos y organismos de la UE («IOUE») tratan datos personales como responsables o encargados del tratamiento. Este Reglamento constituye un pilar de buena gobernanza y buena conducta administrativa a escala de la UE. Se aplica desde el 11 de diciembre de 2018[3], fecha en que derogó y sustituyó a su predecesor, el Reglamento (CE) n.º 45/2001[4].

La presente Comunicación presenta el primer informe sobre la aplicación del RPDUE, de conformidad con el artículo 97 de dicho Reglamento. Asimismo, revisa los actos jurídicos adoptados sobre la base de los Tratados que regulan el tratamiento de datos personales operativos[5] por parte de los órganos u organismos de la UE cuando llevan a cabo actividades en el ámbito de la cooperación policial y la cooperación judicial en materia penal[6], de conformidad con el artículo 98 del RPDUE.

La Comisión ha recopilado información sobre la aplicación del RPDUE a través de una encuesta puesta en marcha en octubre de 2021, en la que se invitó a las IOUE a compartir su experiencia en lo que respecta a la aplicación del RPDUE. Un total de cincuenta y seis[7] IOUE respondieron, y las estadísticas sobre IOUE presentadas en el informe se basan en estas respuestas[8]. Se envió una solicitud de contribución separada al Supervisor Europeo de Protección de Datos («SEPD») en su calidad de autoridad de control[9]. Por último, la Comisión publicó asimismo una convocatoria de datos[10], que permitió al público formular observaciones también. Las cuestiones planteadas en las

---

[1] Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (Texto pertinente a efectos del EEE) (DO L 295 de 21.11.2018, p. 39), http://data.europa.eu/eli/reg/2018/1725/oj.

[2] Algunos organismos del ámbito de la justicia y los asuntos de interior tienen normas específicas sobre protección de datos en sus actos constitutivos que se aplican en lugar del RPDUE o lo complementan (véase la sección 6).

[3] De conformidad con el artículo 101, apartado 2, del RPDUE, solo se aplica a Eurojust desde el 12 de diciembre de 2019.

[4] Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001, p. 1), http://data.europa.eu/eli/reg/2001/45/oj.

[5] Artículo 3, apartado 2, del RPDUE.

[6] Los capítulos 4 o 5 del título V de la tercera parte del Tratado de Funcionamiento de la Unión Europea («TFUE»).

[7] La encuesta se envió a las IOUE que existían en aquel momento (lista: https://publications.europa.eu/code/es/es-5000900.htm).

[8] Los porcentajes indicados en el presente informe son siempre con respecto a las IOUE que respondieron a esa pregunta concreta de la encuesta.

[9] Supervisor Europeo de Protección de Datos, *Contribution by the European Data Protection Supervisor to the Report on the application of Regulation (EU) 2018/1725, the 'EUDPR'* [«Contribución del Supervisor Europeo de Protección de Datos al Informe sobre la aplicación del Reglamento (UE) 2018/1725, el "RPDUE"», documento en inglés], 21 de diciembre de 2021, https://edps.europa.eu/system/files/2022-04/20-12-21-contribution_edps_report_eudpr_en_0.pdf.

[10] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13256-Reglamento-de-proteccion-de-datos-para-las-instituciones-organos-organismos-y-agencias-de-la-UE-informe-sobre-la-aplicacion_es.

pocas observaciones recibidas en respuesta a la convocatoria de datos se abordan en el presente informe.

El presente informe sitúa al RPDUE en el marco de la legislación de la UE en materia de protección de datos, presenta su aplicación por parte de las IOUE y las actividades del SEPD, y analiza la aplicación del capítulo relativo a los órganos y organismos de la UE que llevan a cabo actividades en el ámbito de la cooperación policial y la cooperación judicial en materia penal. El informe concluye esbozando el camino a seguir.

2 Normas sobre protección de datos separadas para las instituciones, órganos y organismos de la UE, en consonancia con la legislación de la UE en materia de protección de datos

Los principales instrumentos de protección de datos en la UE son el Reglamento general de protección de datos («RGPD»)[11], la Directiva sobre protección de datos en el ámbito penal[12] y la Directiva sobre la privacidad y las comunicaciones electrónicas[13]. Sin embargo, no se aplican al tratamiento de datos personales por parte de las IOUE[14]. Por lo tanto, se necesitan normas sobre protección de datos separadas, aunque armonizadas, para las IOUE. El RPDUE establece dichas normas.

A fin de garantizar un enfoque coherente de la protección de los datos personales y su libre circulación en la UE, el RPDUE se ajusta, en la medida de lo posible, a las normas sobre protección de datos adoptadas para el sector público, establecidas en el RGPD y la Directiva sobre protección de datos en el ámbito penal. Cuando el RPDUE siga los mismos principios que el RGPD, debe interpretarse de la misma manera, ya que debe entenderse como equivalente al RGPD[15]. Lo mismo cabe suponer con las normas armonizadas con la Directiva sobre protección de datos en el ámbito penal.

---

[11] 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 de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1), http://data.europa.eu/eli/reg/2016/679/oj.

[12] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DO L 119 de 4.5.2016, p. 89), http://data.europa.eu/eli/dir/2016/680/oj.

[13] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (DO L 201 de 31.7.2002, p. 37), https://data.europa.eu/eli/dir/2002/58/oj.

[14] Artículo 2, apartado 3, del RGPD, y artículo 2, apartado 3, letra b), de la Directiva sobre protección de datos en el ámbito penal. La Directiva sobre la privacidad y las comunicaciones electrónicas, como tal, no se aplica, pero el artículo 37 del RPDUE obliga a las IOUE a proteger la información transmitida a los equipos terminales de los usuarios que acceden a sus sitios web y aplicaciones móviles de acceso público almacenada en dichos equipos, relacionada con ellos, tratada por ellos y recopilada de ellos, de conformidad con el artículo 5, apartado 3, de la Directiva 2002/58/CE.

[15] Véase el considerando 5 del RPDUE.

El RPDUE se adapta al contexto específico de las IOUE, tal como se describe en los puntos siguientes.

- Dado que su ámbito de aplicación se limita exclusivamente a las IOUE como organismos públicos, se han omitido varias disposiciones del RGPD que solo son pertinentes para el sector privado. Por ejemplo, el RPDUE no contempla la posibilidad de tratar los datos apoyándose en la base jurídica de los «intereses legítimos» del responsable del tratamiento[16].
- Algunas facultades de la Comisión para adoptar actos delegados o de ejecución no se repiten como tales, sino que, en su lugar, el RPDUE hace referencia al RGPD o a la Directiva sobre protección de datos en el ámbito penal. Por ejemplo, el RPDUE no contiene un mecanismo para adoptar decisiones de adecuación para las transferencias internacionales, pero las IOUE también pueden invocar las decisiones de adecuación adoptadas en virtud del RGPD o de la Directiva sobre protección de datos en el ámbito penal.
- El RPDUE también crea directamente el SEPD, y establece sus funciones, competencias y procedimientos de nombramiento. En virtud del RGPD y de la Directiva sobre protección de datos en el ámbito penal, las respectivas autoridades de control se establecen con arreglo a la legislación nacional, de conformidad con los requisitos de estos dos actos.
- El capítulo del RPDUE aplicable a los órganos y organismos de la UE en el ámbito del Derecho penal[17] es funcionalmente equivalente a la Directiva sobre protección de datos en el ámbito penal para dichos órganos y organismos. Sin embargo, al ser un Reglamento de aplicación directa, se formula de forma distinta. Establece normas generales que deben complementarse, cuando sea necesario, con disposiciones específicas recogidas en los actos constitutivos de los órganos y organismos que actúen en este ámbito. Prevé un régimen adaptado para el tratamiento de datos personales operativos que tiene en cuenta la naturaleza específica de este sector, por ejemplo las normas sobre la comunicación de información a los interesados, destinadas a garantizar la protección de la investigación.

3 Aplicación del RPDUE en las IOUE

3.1 Papel de las IOUE como responsables del tratamiento

Las observaciones generales de las IOUE demuestran que los primeros años de aplicación del RPDUE han contribuido con éxito a reforzar su cultura general de protección de datos. A este respecto, el 94 % de las IOUE afirmaron que la entrada en vigor del RPDUE mejoró en cierta o en gran medida el conocimiento por parte de su organización de las normas sobre protección de datos.

[16] Esto refleja la situación conforme a su predecesor, el Reglamento (CE) n.º 45/2001, que tampoco incluía el motivo de «interés legítimo». El considerando 22, segunda frase, del RPDUE aclara que «el tratamiento de datos personales efectuado a cargo de las instituciones y organismos de la Unión para el desempeño de funciones de interés público incluye el tratamiento de datos personales necesarios para [su] gestión y funcionamiento», lo que significa que dichas operaciones de tratamiento, por ejemplo para garantizar el control del acceso físico a las instalaciones de las IOUE, también quedan cubiertas.

[17] Capítulo IX sobre el tratamiento de datos personales operativos por los órganos y organismos de la Unión cuando llevan a cabo actividades comprendidas en el ámbito de aplicación de los capítulos 4 o 5 del título V de la tercera parte del TFUE.

En general, las IOUE indicaron que el RPDUE ha tenido una repercusión positiva en sus políticas de protección de datos y que su personal es más consciente de la responsabilidad proactiva de su organización en su calidad de responsables del tratamiento, así como de los requisitos para el tratamiento de datos personales.

Las IOUE mencionaron la realización de evaluaciones de impacto relativas a la protección de datos, la identificación y gestión de las violaciones de la seguridad de los datos y la consideración de la protección de datos desde el diseño y por defecto como los principales efectos del RPDUE en comparación con el Reglamento (UE) n.º 45/2001 derogado. El RPDUE hace más visible la posibilidad de una corresponsabilidad del tratamiento —múltiples organizaciones determinan conjuntamente los fines y medios del tratamiento de los datos personales—, al igual que el RGPD. El SEPD ha proporcionado directrices[18] sobre este tema y la Comisión ha elaborado modelos internos para los acuerdos de corresponsabilidad.

Si bien los requisitos adicionales de responsabilidad proactiva necesarios para demostrar el cumplimiento del RPDUE por parte de las IOUE fueron, en general, bien acogidos, algunas IOUE señalaron que las normas del RPDUE han dado lugar a un aumento de la carga de trabajo. También señalaron que el RPDUE establece normas relativamente complejas que requieren más conocimientos especializados en el seno de las IOUE, también por parte de sus delegados de protección de datos (DPD), así como en las redes de coordinadores de la protección de datos (CPD) de las IOUE que dispongan de ellas.

Todas las IOUE, excepto dos de ellas, mantienen sus registros de las operaciones de tratamiento en un registro central. Aunque no se trata de un requisito específico conforme al RPDUE, constituye una buena práctica que también recomienda el SEPD[19]. Además, el 72 % de las IOUE han convertido en registros todas sus notificaciones al DPD con arreglo al Reglamento anterior[20]. Aquellas que aún no hayan realizado esta tarea deben revisar y actualizar la documentación de sus operaciones de tratamiento para garantizar que esté completa y actualizada.

3.2 Ejercicio de los derechos de los interesados

El RPDUE otorga a los interesados un amplio conjunto de derechos sobre el tratamiento de sus datos personales, en consonancia con el RGPD. Las IOUE, en su calidad de responsables del tratamiento, tienen la obligación específica de facilitar el ejercicio de estos derechos[21]. Como

[18] *Concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725* [«Conceptos de responsable y encargado del tratamiento y de corresponsabilidad con arreglo al Reglamento (UE) 2018/1725», documento en inglés], https://edps.europa.eu/data-protection/our-work/publications/guidelines/concepts-controller-processor-and-joint.

[19] *Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies* [«Responsabilidad sobre el terreno: Orientaciones sobre la documentación de las operaciones de tratamiento para las instituciones, órganos y organismos de la UE», documento en inglés] — Parte I: Registros y análisis del umbral, p. 7, https://edps.europa.eu/sites/default/files/publication/19-07-17_accountability_on_the_ground_part_i_en.pdf.

[20] Artículo 25 del Reglamento (CE) n.º 45/2001.

[21] Artículo 14 del RPDUE.

consecuencia de ello, el 96 % de las IOUE indicaron que habían llevado a cabo actividades de sensibilización, como la actualización de la información públicamente disponible sobre sus operaciones de tratamiento, mensajes informativos o guías para los interesados.

Varias IOUE, como la Comisión, el Banco Central Europeo y el Servicio Europeo de Acción Exterior, informaron de un claro aumento de las solicitudes recibidas de particulares entre 2018 y 2021[22]. Sin embargo, en el caso de otras, como el Tribunal de Justicia de la Unión Europea, el Comité Económico y Social Europeo y la Agencia de Asilo de la Unión Europea, las cifras se mantuvieron estables o fluctuaron sin una tendencia clara. Aún no es posible discernir una tendencia clara en el número de solicitudes por parte de interesados tras la entrada en vigor del RPDUE, dada la forma en que el registro de los distintos tipos de solicitudes varía de una IOUE a otra.

3.3 Limitación de los derechos de los interesados mediante normas internas

Al igual que el RGPD, el RPDUE[23] prevé la posibilidad de limitar determinados derechos de los interesados. Esto puede hacerse mediante actos legislativos y a través de normas internas[24], a las que se aplican criterios estrictos. Estas normas deben ser claras y precisas y su aplicación debe ser previsible para las personas sujetas a ellas. Deben publicarse en el Diario Oficial y cumplir los requisitos establecidos en la Carta de los Derechos Fundamentales y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales[25].

Las limitaciones basadas en normas internas solo pueden referirse al funcionamiento de las IOUE. Deben respetar los derechos fundamentales, constituir medidas necesarias y proporcionadas en una sociedad democrática y tener por objeto salvaguardar uno de los objetivos enumerados de forma específica en el RPDUE[26]. Todo interesado cuyos derechos hayan sido limitados tiene derecho a presentar una reclamación ante el SEPD[27].

Una gran mayoría (el 84 %) de las IOUE han adoptado normas internas. Por ejemplo, se han introducido normas de este tipo para permitir el aplazamiento de la comunicación de información a una persona interesada en una investigación administrativa interna[28]. En otras, el objetivo de dichas normas ha sido garantizar una cooperación continua y eficaz con los Estados miembros en aquellos ámbitos en los que las actividades de las IOUE se basan en la información recibida de las autoridades competentes de los Estados miembros. Por ejemplo, las normas internas adoptadas por

[22] Esto incluye solicitudes de información general y solicitudes de ejercicio de los derechos de los interesados en virtud del capítulo II del RPDUE, como el derecho de acceso a sus datos personales en poder de una IOUE.
[23] Artículo 25 del RPDUE.
[24] Esto equivale a las posibilidades de limitar los derechos de los interesados a escala nacional en algunos Estados miembros, por ejemplo, mediante decretos ministeriales.
[25] Artículo 25, apartado 5, y considerando 24 del RPDUE.
[26] Artículo 25, apartado 1, del RPDUE.
[27] Artículo 25, apartado 6, del RPDUE.
[28] Véase por ejemplo la Decisión n.º 59/2021 del Secretario General del Consejo de la Unión Europea por la que se establecen normas de aplicación relativas a la aplicación del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo y a la limitación de los derechos de los interesados a efectos de las investigaciones administrativas y los procedimientos disciplinarios y judiciales 2022/C 25/02 (DO C 25 de 18.1.2022, p. 2).

la Comisión para el tratamiento de datos personales en sus actividades de competencia, lucha contra el fraude y auditoría interna prevén la posibilidad de introducir limitaciones de los derechos de los interesados cuando los datos personales se obtienen de las autoridades competentes de los Estados miembros[29]. Dichas normas establecen la posibilidad de imponer restricciones similares cuando las autoridades nacionales hayan impuesto limitaciones basadas en una medida legislativa posible en virtud del RGPD[30] o de la Directiva sobre protección de datos en el ámbito penal[31].

En los casos en que las IOUE han adoptado normas internas que permiten limitar los derechos de los interesados, estas suelen aplicarse caso por caso, según exijan sus respectivas normas internas. Sin embargo, el 69 % de las IOUE que han adoptado normas conforme al artículo 25 declaran que todavía no las han utilizado. Las que sí lo han hecho han notificado menos de diez casos de limitaciones, salvo el Parlamento Europeo y la Comisión. La necesidad de limitaciones ha surgido con mayor frecuencia en el caso de las actividades de la OLAF, en particular para aplazar la comunicación de información a los interesados sobre el tratamiento de sus datos personales cuando una investigación se encuentra todavía en una fase temprana a fin de no perjudicar la recogida de pruebas. La OLAF también aplicó varias limitaciones relativas a solicitudes de acceso de los interesados a sus propios datos personales que se rechazaron únicamente con el fin de proteger los derechos y libertades de terceros[32], por ejemplo, cuando la divulgación de los datos podría poner a un informador en riesgo de sufrir represalias.

Por lo general, las normas internas de las IOUE les obligan a informar a sus DPD de las limitaciones aplicadas y a facilitar a los DPD acceso al registro y a los documentos sobre dichas limitaciones[33].

3.4 Delegados de protección de datos

La obligación de que cada IOUE cuente con un delegado de protección de datos (DPD) ya se contemplaba en el anterior Reglamento (CE) n.º 45/2001. El RPDUE ha dado más visibilidad a esta función mediante la introducción del principio de responsabilidad proactiva. Esto significa que el responsable del tratamiento asume la responsabilidad por el cumplimiento de las normas sobre protección de datos y debe poder demostrarlo.

En el 46 % de las IOUE, sus DPD están respaldados por redes de coordinadores de protección de datos (CPD) o estructuras similares[34]. Las IOUE de mayor tamaño tienen más probabilidades de disponer de este tipo de redes [(por ejemplo, el Parlamento Europeo, la Secretaría General del

[29] Decisión (UE) 2018/1961 de la Comisión (DO L 315 de 12.12.2018, p. 35); Decisión (UE) 2018/1962 de la Comisión (DO L 315 de 12.12.2018, p. 41); Decisión (UE) 2018/1927 de la Comisión (DO L 313 de 10.12.2018, p. 39).
[30] Artículo 23 del RGPD.
[31] Artículo 13, apartado 3, artículo 15 o artículo 16 de la Directiva sobre protección de datos en el ámbito penal.
[32] Véase el artículo 2, apartado 2, de la Decisión 2018/1962 de la Comisión, relativo a la protección de terceros, tal como se menciona en el artículo 25, apartado 1, letra h), del RPDUE.
[33] Así se recomienda también en las orientaciones sobre el artículo 25 del RPDUE publicadas por el SEPD, que pueden consultarse en el siguiente enlace: https://edps.europa.eu/data-protection/our-work/publications/guidelines/guidance-art-25-regulation-20181725_en.
[34] Por ejemplo, la Comisión Europea tiene un delegado de protección de datos adscrito a la Secretaría General que cuenta con el apoyo de coordinadores de protección de datos en todas las direcciones generales.

Consejo, la Comisión y el Servicio Europeo de Acción Exterior (SEAE)]. El SEAE también organiza y mantiene una red de corresponsales de protección de datos en las delegaciones de la UE.

Varias IOUE señalaron el aumento de las responsabilidades y la carga de trabajo de sus DPD (y, por ende, de sus CPD). Reconocieron la necesidad de dotar a los DPD (y a los CPD) de más recursos para garantizar que puedan aplicar eficazmente las políticas de protección de datos de sus IOUE. También se mencionó la necesidad de velar por la independencia de los DPD.

En este contexto, existen dos tendencias: Por una parte, el RPDUE hace mayor hincapié en la responsabilidad proactiva del responsable del tratamiento, por ejemplo, al eliminar el procedimiento de control previo que existía en el marco del anterior Reglamento (UE) n.º 45/2001, con lo que se reduce la carga administrativa. Por otra parte, los responsables del tratamiento solicitan a los DPD/CPD una mayor orientación sobre la mejor manera de dar cumplimiento al RPDUE. En este sentido, se observó que la red de DPD de las IOUE ha proporcionado un foro importante para debatir y aclarar determinados aspectos jurídicos y técnicos específicos del tratamiento de datos por parte de las IOUE. Esta red proporciona una plataforma para los intercambios entre los DPD y el SEPD y entre los propios DPD. Coopera de forma continua y suele reunirse dos veces al año.

Más de la mitad (el 54 %) de las IOUE han proporcionado más recursos a sus DPD y, de manera más general, a su personal con funciones de protección de datos. La mayoría (el 84 %) de las IOUE han adaptado sus procesos internos para garantizar que su personal informe y consulte a los DPD sobre las nuevas operaciones de tratamiento de datos personales. Esto suele hacerse, por ejemplo, incluyendo a los DPD en los procesos de gestión de cambios o en los comités de dirección de proyectos.

3.5 Evaluaciones de impacto relativas a la protección de datos

El Banco Central Europeo, el Banco Europeo de Inversiones y la Comisión fueron quienes realizaron el mayor número de evaluaciones de impacto relativas a la protección de datos (EIPD). En comparación con el anterior sistema de «control previo»[35] con arreglo al Reglamento (CE) n.º 45/2001, el número de casos enviados al SEPD ha disminuido considerablemente. Esta fue la consecuencia prevista de este cambio y redujo las consultas del SEPD sobre operaciones de tratamiento administrativo como las evaluaciones del personal.

[35] Artículo 27 del Reglamento (CE) n.º 45/2001. En el marco de dicho sistema, las operaciones de tratamiento, por ejemplo las que conllevaban un tratamiento de datos personales relativos a la salud, así como a sospechas, infracciones, condenas penales o medidas de seguridad o estaban destinadas a evaluar aspectos de la personalidad del interesado, como su competencia, rendimiento o conducta, tenían que ser «controladas previamente» por el SEPD. Esto generó un gran número de notificaciones (y los correspondientes dictámenes del SEPD) sobre operaciones de tratamiento muy similares, por ejemplo, los procedimientos de selección y evaluación del personal entraban en el ámbito de aplicación de esta disposición.

El cuadro 1 del anexo ofrece una visión general de las EIPD realizadas por las IOUE entre 2019 y 2021.

Casi todas las IOUE (el 94 %) estuvieron de acuerdo en que los criterios del RPDUE[36] sobre cuándo tienen que llevar a cabo las EIPD cubren adecuadamente las operaciones de tratamiento de alto riesgo. Aquellas que no estuvieron de acuerdo subrayaron la necesidad de que el SEPD tuviera en cuenta el desarrollo tecnológico a la hora de interpretar estos criterios. Por ejemplo, la computación en la nube ya no es una tecnología «nueva», lo que debe tenerse en cuenta a la hora de valorar si deben llevarse a cabo EIPD. Las IOUE que plantearon esta cuestión por lo general consideran que el texto jurídico es suficientemente claro en sí mismo, y que se trata de una cuestión de interpretación por parte del SEPD.

El RPDUE no contiene ninguna obligación específica de publicar los resultados de las EIPD. Una gran mayoría (el 84 %) de las IOUE no publican las EIPD que han llevado a cabo, mientras que el 14 % las publican parcialmente o en forma de resumen, eliminando información que pudiera comprometer las garantías de seguridad adoptadas. Solo una IOUE indicó que publica íntegramente sus EIPD. La publicación de las EIPD, eliminando en caso necesario la información que pudiera poner en peligro la seguridad de las operaciones de tratamiento, mejora la transparencia en cuanto al cumplimiento de las normas del RPDUE por parte de las IOUE y constituye una buena práctica recomendada por el SEPD[37].

3.6 Transferencias internacionales de datos

Casi todas las IOUE (el 91 %) informaron de que sus actividades conllevan transferencias internacionales de datos personales. Esto incluye las transferencias de datos a países no pertenecientes a la UE ni al EEE, así como a organizaciones internacionales. Sin embargo, varias IOUE mencionaron que estas transferencias son escasas o solo afectan a una cantidad limitada de datos personales. Por lo que se refiere a las herramientas de transferencia utilizadas, las IOUE hicieron principalmente referencia a decisiones de adecuación (adoptadas en virtud del RGPD[38] o de la Directiva sobre protección de datos en el ámbito penal[39]) y a instrumentos contractuales, por ejemplo para las transferencias de datos a empresas privadas. En el caso de las transferencias de datos a organismos públicos, también se utilizan otras herramientas, como acuerdos jurídicamente vinculantes y disposiciones administrativas. Además, el 51 % de las IOUE mencionaron que llevan a cabo transferencias limitadas y ocasionales, por ejemplo para organizar formaciones, amparándose en los motivos legales para las transferencias de datos (las «excepciones»)[40].

En la práctica, las transferencias de datos no suelen ser realizadas directamente por las IOUE, sino por sus encargados del tratamiento (que no son IOUE) que actúan en su nombre. Por consiguiente,

[36] Artículo 39 del RPDUE.
[37] Aunque la publicación de informes de las EIPD (o sus resúmenes) no constituye una obligación en virtud del RPDUE, es una buena práctica recomendada por el SEPD; véase *Accountability on the ground*, Parte II, p. 18/19, https://edps.europa.eu/node/4582_en.
[38] Artículo 45, apartado 3, del RGPD.
[39] Artículo 36, apartado 3, de la Directiva sobre protección de datos en el ámbito penal.
[40] Artículo 50 del RPDUE.

la Comisión abordó específicamente este supuesto en las cláusulas contractuales tipo adoptadas en virtud del RGPD en junio de 2021[41] para ayudar a los responsables y encargados del tratamiento a cumplir los requisitos tanto del RGPD como del RPDUE. En particular, los encargados del tratamiento del Espacio Económico Europeo (EEE) tienen la posibilidad de incluir estas cláusulas contractuales tipo para las transferencias internacionales de datos en los contratos con sus subencargados en terceros países[42]. Esto garantiza el cumplimiento de las normas del RPDUE[43] relativas a la contratación de subencargados en nombre de las IOUE, siempre que las obligaciones en materia de protección de datos sean uniformes en los contratos entre: i) la IOUE y el encargado del tratamiento; y ii) el encargado del tratamiento y su subencargado[44]. Concretamente, las IOUE pueden garantizar dicha armonización utilizando las cláusulas contractuales tipo adoptadas por la Comisión para la relación entre los responsables y los encargados del tratamiento[45].

Con el fin de proporcionar herramientas adicionales que ofrezcan garantías adecuadas para las transferencias directas de datos de IOUE a terceros países (es decir, sin la participación de un encargado del tratamiento de la UE o del EEE), la Comisión está elaborando actualmente cláusulas contractuales tipo con arreglo al artículo 48, apartado 2, letra b), del RPDUE. Estas cláusulas se ajustarán, en la mayor medida posible, a las cláusulas existentes adoptadas en virtud del RGPD.

Por último, habida cuenta de las cuestiones específicas que surgen cuando se transfieren datos personales a organizaciones internacionales (por ejemplo, debido al estatuto de las organizaciones internacionales y a los privilegios e inmunidades aplicables), la Comisión colabora con los DPD de las IOUE para desarrollar herramientas específicas (por ejemplo, acuerdos administrativos) que se adapten a dichas transferencias.

4 Actividades del SEPD

4.1 El SEPD como autoridad de control de la protección de datos para las IOUE

El SEPD es la autoridad independiente de control de la protección de datos para las IOUE[46] que refleja el papel de las autoridades nacionales de control de la protección de datos establecidas en

[41] Decisión de Ejecución (UE) 2021/914 de la Comisión de 4 de junio de 2021 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.
[42] Utilizando el «módulo 3» de las cláusulas contractuales tipo.
[43] Artículo 29, apartado 4, del RPDUE.
[44] Véase el considerando 8 de la Decisión de Ejecución 2021/914 de la Comisión y la nota a pie de página n.º 1 del anexo de dicha Decisión.
[45] Decisión de Ejecución (UE) 2021/915 de la Comisión de 4 de junio de 2021 relativa a las cláusulas contractuales tipo entre responsables y encargados del tratamiento contempladas en el artículo 28, apartado 7, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo y en el artículo 29, apartado 7, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo.
[46] A excepción del Tribunal de Justicia de la Unión Europea cuando actúa en el ejercicio de sus funciones jurisdiccionales; véanse el artículo 57, apartado 1, letra a), y el considerando 74, del RPDUE. En estos casos, el control se lleva a cabo mediante mecanismos específicos, creados por la Decisión del Tribunal de Justicia, de 1 de octubre de 2019, por la que se establece un mecanismo interno de supervisión en materia de tratamiento de datos personales

los Estados miembros en virtud del RGPD y de la Directiva sobre protección de datos en el ámbito penal.

El cuadro 2 del anexo ofrece una visión general de las actividades de control del SEPD entre 2018 y 2021. Desde que el RPDUE entró en vigor, el 11 de diciembre de 2018[47], las cifras de 2018 constituyen la base de referencia para la comparación con la situación con arreglo al anterior Reglamento (UE) n.º 45/2001.

El SEPD observó que, desde que comenzó a aplicarse el RPDUE, los temas de las consultas recibidas de las IOUE pasaron a centrarse en su actividad principal. Esto conlleva un cambio hacia preguntas sobre el tratamiento de datos personales para el desempeño de las tareas asignadas a las IOUE en aras del interés público, alejándose de los temas «administrativos», como la gestión del personal.

El número de reclamaciones inadmisibles recibidas por el SEPD ha aumentado entre 2019 y 2021[48]. La mayoría de las reclamaciones que se consideraron inadmisibles iban dirigidas contra responsables del tratamiento de los Estados miembros que no están supervisados por el SEPD, sino por sus autoridades nacionales de protección de datos. Las cifras de 2018 fueron más elevadas, muy probablemente porque comenzó a aplicarse el RGPD. Esto dio lugar a un mayor conocimiento de las normas sobre protección de datos entre la población, pero también a un aumento de las reclamaciones inadmisibles. El SEPD también puede archivar las reclamaciones admisibles cuando se haya llegado a una solución amistosa.

En cuanto a las inspecciones y auditorías, en 2019 se registró un aumento con respecto a la base de referencia de 2018, seguido de una disminución en 2020 y 2021. Esto puede deberse a la pandemia de COVID-19, que dificultó los controles *in situ* y obligó a sustituirlos por auditorías a distancia. El SEPD evalúa los riesgos a la hora de decidir qué IOUE deben inspeccionarse. Para ello se tiene en cuenta, por ejemplo, el número de consultas presentadas, especialmente cuando se tratan categorías especiales de datos como parte de la actividad principal de la IOUE. El SEPD también podrá decidir llevar a cabo investigaciones por propia iniciativa, por ejemplo, sobre el uso de proveedores de servicios en la nube por parte de la IOUE.

efectuado en el marco de las funciones jurisdiccionales del Tribunal de Justicia (DO C 383, 2019, p. 2), y por la Decisión del Tribunal General, de 16 de octubre de 2019, por la que se establece un mecanismo interno de supervisión en materia de tratamiento de datos personales efectuado en el marco de las funciones jurisdiccionales del Tribunal General (DO C 383, 2019, p. 4). Además, sigue existiendo la Autoridad de Supervisión Común del Sistema de Información Aduanero creada en virtud de la Decisión 2009/917/JAI del Consejo.

[47] Una excepción a este respecto es Eurojust, a la que se aplica el RPDUE desde el 12 de diciembre de 2019; véase el artículo 101, apartado 2, del RPDUE.

[48] Véase el cuadro 2 del anexo.

En cuanto a las violaciones de la seguridad de los datos, el SEPD informó de que, en la mayoría de los casos, la causa subyacente fue un error humano, seguido de errores técnicos y ataques externos[49].

El SEPD ha hecho uso de la mayoría de sus potestades en virtud del RPDUE, entre otras, por ejemplo, la imposición de prohibiciones temporales a las operaciones de tratamiento[50]. Hasta la fecha, no ha utilizado su nueva potestad para imponer multas administrativas, que constituye una medida de último recurso con arreglo al RPDUE[51].

El SEPD también señaló en su contribución al presente informe que había invertido en actividades de sensibilización, como formaciones, alcanzando un máximo de aproximadamente más de 4 600 participantes en 2019, tras la entrada en vigor del RPDUE. Aunque el número de participantes en 2020 y 2021 ha disminuido con respecto a este máximo, sigue siendo considerablemente superior a la base de referencia de unos 1 000 participantes en 2018.

Las IOUE hicieron comentarios en gran parte positivos sobre las interacciones con el SEPD y las orientaciones recibidas de este, y un 86 % indicó que las respuestas eran siempre o casi siempre fáciles de entender. Las IOUE también valoraron positivamente el aumento de los contactos del SEPD con la red de DPD.

No obstante, algunas IOUE observaron que, en ocasiones, el asesoramiento del SEPD llegó demasiado tarde[52]. Destacaron la importancia de recibir un apoyo y asesoramiento constantes del SEPD y pidieron orientaciones prácticas y oportunas sobre determinadas cuestiones relativas a la protección de datos. Entre estas cuestiones están la aplicación del enfoque basado en el riesgo para los responsables del tratamiento, las transferencias internacionales y la relación entre los responsables (en particular los corresponsables) y sus encargados del tratamiento.

[49] En 2020 (el último año con estadísticas completas): el 52 % de las violaciones de la seguridad de los datos se debieron a errores humanos; el 21 %, a errores técnicos; el 17 %, a ataques externos; y el resto se debió a otros motivos, como el uso indebido de cuentas con privilegios.

[50] Por ejemplo, a las operaciones de tratamiento para el seguimiento de las redes sociales por parte de la entonces Oficina Europea de Apoyo al Asilo (EASO): https://edps.europa.eu/sites/default/files/publication/19-11-12_reply_easo_ssm_final_reply_en.pdf. En respuesta a ello, la antigua EASO suspendió las operaciones de tratamiento en cuestión.

[51] En virtud del RGPD, pueden imponerse multas directamente por una violación, por ejemplo, cuando un responsable del tratamiento no informa adecuadamente a los interesados sobre el tratamiento de sus datos personales (artículos 12 a 14 del RGPD). En virtud del RPDUE, el SEPD solo puede imponer multas por incumplimiento de una orden, por ejemplo, para subsanar que no se haya informado adecuadamente a los interesados con arreglo a los artículos 14 a 16 del RPDUE.

[52] El 67 % de las IOUE declararon que recibieron asesoramiento del SEPD a tiempo o generalmente a tiempo, mientras que el 33 % se mostraron neutrales o afirmaron que (generalmente) había llegado demasiado tarde.

4.2 El SEPD como asesor del legislador de la UE

La Comisión consulta oficialmente[53] al SEPD, en particular sobre las propuestas legislativas que repercuten en el tratamiento de datos personales, tras su adopción por el Colegio[54]. El SEPD responde a estas consultas con dictámenes u observaciones[55]. El SEPD también emite dictámenes de iniciativa, como su dictamen preliminar sobre el Espacio Europeo de Datos Sanitarios[56]. Cuando una propuesta reviste especial importancia para la protección de datos, la Comisión también puede consultar al Comité Europeo de Protección de Datos (CEPD). En ese caso, el SEPD y el CEPD deben emitir un dictamen conjunto[57] para garantizar que el legislador de la UE obtenga un asesoramiento coherente.

La Comisión también consulta al SEPD de manera oficiosa antes de que el Colegio adopte actos sujetos a requisitos de consulta. En respuesta a dichas consultas, el SEPD formula observaciones informales a la Comisión. Esta posibilidad contribuye a garantizar que los actos de la Comisión se ajusten plenamente a las normas sobre protección de datos antes de su adopción. Las consultas oficiosas se utilizan, en particular, para los actos sensibles o que tienen un impacto más significativo en la protección de datos.

La actividad del SEPD como asesor del legislador de la UE depende del número de nuevas propuestas elaboradas por la Comisión. Tras la disminución de las cifras durante el último año de la Comisión saliente, el marcado aumento de las observaciones formales en 2021 se debe al mayor número de propuestas legislativas y a los esfuerzos de la Comisión por garantizar una aplicación coherente de la obligación de consultar al SEPD[58]. Esto incluye los actos delegados y de ejecución que conllevan el tratamiento de datos personales. Tras la entrada en vigor del RPDUE, la Secretaría General de la Comisión elaboró procedimientos y concienció a los servicios sobre la obligación de consultar al SEPD. Esto ha dado lugar a una consulta más sistemática, también para los actos delegados y de ejecución. A efectos de planificación, el SEPD y los servicios de la Comisión celebran reuniones anuales sobre el próximo programa de trabajo y las propuestas que requerirán consulta.

---

[53] Artículo 42 del RPDUE.

[54] En el caso de los actos delegados y de ejecución, la consulta formal puede tener lugar en paralelo al período de consulta pública sobre los proyectos de actos de ejecución y delegados.

[55] El SEPD se refiere a las respuestas sobre propuestas legislativas y recomendaciones con arreglo al artículo 218 del TFUE como «dictámenes». Las respuestas relativas a actos delegados o de ejecución se denominan «observaciones»; véase también la Decisión del Supervisor Europeo de Protección de Datos, de 15 de mayo de 2020, por la que se adopta el Reglamento interno del SEPD (DO L 204 de 26.6.2020, p. 49), http://data.europa.eu/eli/proc_rules/2020/626/oj.

[56] *EDPS Preliminary Opinion 8/2020 on the European Health Data Space* [«Dictamen preliminar 8/2020 del SEPD sobre el Espacio Europeo de Datos Sanitarios», documento en inglés], https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-82020-european-health-data-space_en.

[57] Artículo 42, apartado 2, del RPDUE.

[58] Artículo 42 del RPDUE.

4.3 Cooperación entre el SEPD y las autoridades nacionales de protección de datos

El SEPD es miembro del CEPD para el cual ejerce las funciones de secretaría. También coopera con las autoridades nacionales de control en el ejercicio de sus respectivas funciones de otras maneras[59]. Entre los ejemplos cabe citar la remisión de reclamaciones a la autoridad de control competente en materia de protección de datos o casos en los que intervienen proveedores de servicios externos que son utilizados tanto por las IOUE como por responsables del tratamiento sujetos al RGPD. El SEPD también contribuye activamente a la labor del CEPD asumiendo funciones, por ejemplo, de ponente principal o coponente para las directrices, o contribuyendo de otro modo a su labor.

Varios sistemas informáticos a gran escala y organismos creados en virtud del Derecho de la UE exigen que el SEPD y las autoridades nacionales de control, cada uno en el ámbito de sus competencias respectivas, cooperen de forma activa para garantizar una supervisión coordinada[60]. En el pasado, los actos constitutivos de cada sistema u organismo contenían disposiciones específicas a tal fin. El RPDUE[61] crea un sistema armonizado para esta coordinación de la supervisión que puede mencionarse en otros actos. Esto es lo que ocurre en el caso del Sistema de Información del Mercado Interior[62], el ECRIS-TCN[63], Eurojust[64] y, más recientemente, Europol[65].

---

[59] De conformidad con el artículo 61 del RPDUE, el SEPD también coopera con la Autoridad de Supervisión Común creada por el artículo 25 de la Decisión 2009/917/JAI del Consejo.

[60] Algunos ejemplos son el Sistema de Información de Schengen, el Sistema de Información de Visados y Eurodac. Véanse el Reglamento (UE) 2018/1862 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de la cooperación policial y de la cooperación judicial en materia penal, por el que se modifica y deroga la Decisión 2007/533/JAI del Consejo, y se derogan el Reglamento (CE) n.º 1986/2006 del Parlamento Europeo y del Consejo y la Decisión 2010/261/UE de la Comisión (DO L 312 de 7.12.2018, p. 56); el Reglamento (CE) n.º 767/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros (DO L 218 de 13.8.2008, p. 60); y el Reglamento (UE) n.º 603/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del Reglamento (UE) n.º 604/2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida, y a las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de aplicación de la ley, y por el que se modifica el Reglamento (UE) n.º 1077/2011, por el que se crea una Agencia europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia (DO L 180 de 29.6.2013, p. 1).

[61] Artículo 62 del RPDUE.

[62] Reglamento (UE) 2018/1724 del Parlamento Europeo y del Consejo, de 2 de octubre de 2018, relativo a la creación de una pasarela digital única de acceso a información, procedimientos y servicios de asistencia y resolución de problemas y por el que se modifica el Reglamento (UE) n.º 1024/2012 (DO L 295 de 21.11.2018, p. 1).

[63] Reglamento (UE) 2019/816 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, por el que se establece un sistema centralizado para la identificación de los Estados miembros que poseen información sobre condenas de nacionales de terceros países y apátridas (ECRIS-TCN) a fin de complementar el Sistema Europeo de Información de Antecedentes Penales, y por el que se modifica el Reglamento (UE) 2018/1726 (DO L 135 de 22.5.2019, p. 1).

[64] Artículo 42, apartado 2, del Reglamento (UE) 2018/1727 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, sobre la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust) y por el que se sustituye y deroga la Decisión 2002/187/JAI del Consejo (DO L 295 de 21.11.2018, p. 138).

[65] Véanse los cambios en el artículo 44, apartado 2, del Reglamento de Europol, introducidos por el Reglamento (UE) 2022/991 del Parlamento Europeo y del Consejo, de 8 de junio de 2022, por el que se modifica el Reglamento (UE)

Otros sistemas siguen teniendo grupos de coordinación de la supervisión con normas detalladas en sus actos constitutivos, o referencias detalladas a reuniones como parte del CEPD[66].

El SEPD también contribuye al mecanismo de evaluación de Schengen establecido por el Reglamento (UE) n.º 1053/2013 del Consejo[67]. En virtud de dicho Reglamento, la Comisión puede invitar al SEPD a designar a un observador para que participe en una visita *in situ* que afecte a un ámbito que cubra su mandato, es decir, evaluaciones de la protección de datos[68]. Esto equivale a la posibilidad de que Frontex y Europol designen observadores para las evaluaciones de la gestión de fronteras y la cooperación policial, respectivamente. En opinión de la Comisión, la experiencia de los observadores del SEPD es un activo valioso para las evaluaciones de la protección de datos.

4.4 Recursos del SEPD

El número de miembros del personal del SEPD (incluida la Secretaría del CEPD[69]) ha aumentado constantemente durante el período de referencia[70], lo que refleja la tendencia general de las autoridades nacionales de control de la protección de datos. Las actividades de la Secretaría han aumentado con el tiempo, con una producción cada vez mayor de directrices, recomendaciones, dictámenes y otros documentos del CEPD a los que contribuye la Secretaría. Es fundamental dotar a la Secretaría del CEPD de recursos suficientes, puesto que se espera que desempeñe un mayor papel en la aplicación efectiva del RGPD. Esto afecta, en particular, al objetivo del CEPD de desarrollar una cooperación más estrecha en materia de trabajo estratégico y de utilizar nuevas herramientas de apoyo a la cooperación entre las autoridades de protección de datos[71]. En particular, contar con una Secretaría sólida y dotada de recursos suficientes para apoyar la labor del CEPD resulta fundamental para garantizar que este pueda realizar su trabajo según sea

2016/794 en lo que se refiere a la cooperación de Europol con entidades privadas, el tratamiento de datos personales por Europol en apoyo de investigaciones penales y el papel de Europol en materia de investigación e innovación (DO L 169 de 27.6.2022, p. 1).

[66] Artículo 57 del Reglamento (UE) 2018/1861 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de las inspecciones fronterizas, por el que se modifica el Convenio de aplicación del Acuerdo de Schengen y se modifica y deroga el Reglamento (CE) n.º 1987/2006 (DO L 312 de 7.12.2018, p. 14); y artículo 71 del Reglamento (UE) 2018/1862 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de la cooperación policial y de la cooperación judicial en materia penal, por el que se modifica y deroga la Decisión 2007/533/JAI del Consejo, y se derogan el Reglamento (CE) n.º 1986/2006 del Parlamento Europeo y del Consejo y la Decisión 2010/261/UE de la Comisión (DO L 312 de 7.12.2018, p. 56).

[67] Reglamento (UE) n.º 1053/2013 del Consejo, de 7 de Octubre de 2013, por el que se establece un mecanismo de evaluación y seguimiento para verificar la aplicación del acervo de Schengen, y se deroga la Decisión del Comité Ejecutivo de 16 de septiembre de 1998 relativa a la creación de una Comisión permanente de evaluación y aplicación de Schengen (DO L 295 de 6.11.2013, p. 27).

[68] Artículo 10, apartado 5, del Reglamento (UE) n.º 1053/2013 del Consejo, de 7 de octubre de 2013.

[69] Artículo 57, apartado 1, letra l), del RPDUE.

[70] Véase el cuadro 4 del anexo.

[71] Declaración del CEPD sobre una cooperación más estrecha en los expedientes estratégicos, 29 de abril de 2022: DPAs decide on closer cooperation for strategic files | Comité Europeo de Protección de Datos (europa.eu).

necesario, especialmente en el contexto del mecanismo de coherencia[72], cuyo uso se espera que siga aumentando.

En su contribución al presente informe, el SEPD consideró, en particular, que, en caso de que se le confíen funciones adicionales, por ejemplo, como autoridad de vigilancia del mercado conforme a la propuesta legislativa sobre inteligencia artificial[73], debería dotársele de los recursos adicionales correspondientes.

5 Uso por parte de la Comisión de facultades para adoptar actos delegados y actos de ejecución

El RPDUE incluye varias facultades para que la Comisión adopte actos de ejecución y establezca cláusulas tipo, así como referencias cruzadas a facultades concedidas con arreglo al RGPD[74].

El RPDUE[75] contiene disposiciones que la facultan para establecer cláusulas contractuales tipo de protección de datos para los contratos entre responsables y encargados del tratamiento, correspondientes a la facultad concedida en el RGPD[76]. La Comisión utilizó esta facultad y, en junio de 2021, adoptó cláusulas contractuales tipo que cubrían las relaciones entre responsable y encargado del tratamiento[77] y abarcaban tanto el RGPD como el RPDUE. Estas cláusulas proporcionan herramientas fáciles de utilizar para que los responsables puedan gestionar eficazmente las relaciones con sus encargados del tratamiento.

El RPDUE[78] también faculta a la Comisión para adoptar cláusulas contractuales tipo de protección de datos con el fin de ofrecer garantías adecuadas para la transferencia de datos personales fuera de la UE o del EEE. La Comisión está preparando actualmente dichas cláusulas.

6 Normas sobre protección de datos para los órganos y organismos que se ocupan de la cooperación policial y la cooperación judicial en materia penal

El capítulo IX del RPDUE contiene normas para las IOUE que tratan datos personales operativos cuando llevan a cabo actividades en el ámbito de la cooperación policial y la cooperación judicial en materia penal (el «capítulo del ámbito penal»). El objetivo es reducir la fragmentación:

[72] Capítulo VII del RGPD.
[73] COM(2021) 206 final.
[74] Véase el artículo 47 del RPDUE que permite a las IOUE basarse en las decisiones de adecuación adoptadas en virtud del RGPD y de la Directiva sobre protección de datos en el ámbito penal, y el artículo 14, apartado 8, del RPDUE, relativo a los actos delegados sobre los iconos en virtud del artículo 12, apartado 8, del RGPD.
[75] Artículo 29, apartado 7, del RPDUE.
[76] Artículo 28, apartado 7, del RGPD.
[77] Decisión de Ejecución (UE) 2021/915 de la Comisión de 4 de junio de 2021 relativa a las cláusulas contractuales tipo entre responsables y encargados del tratamiento contempladas en el artículo 28, apartado 7, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo y en el artículo 29, apartado 7, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo (Texto pertinente a efectos del EEE) (DO L 199 de 7.6.2021, p. 18), https://eur-lex.europa.eu/legal-content/AUTO/?uri=CELEX:32021D0915.
[78] Artículo 48, apartado 2, letra b), del RPDUE.

- entre los regímenes de protección de datos aplicables al tratamiento de datos operativos por parte de los organismos de la UE en este ámbito;
- con el régimen de protección de datos aplicable a las actividades policiales y judiciales nacionales en el marco de la Directiva sobre protección de datos en el ámbito penal.

A tal fin, el capítulo del ámbito penal del RPDUE dispone un conjunto de normas horizontales basadas en la Directiva sobre protección de datos en el ámbito penal. Estas normas pueden complementarse, en caso necesario, con normas específicas recogidas en los actos constitutivos de los organismos, en función de sus respectivos mandatos y de la naturaleza concreta de sus tareas y operaciones de tratamiento de datos.

El RPDUE establece la necesidad de garantizar una protección uniforme y coherente de las personas físicas al tratar sus datos personales[79]. A tal fin, señala explícitamente el objetivo de ampliar la aplicación del capítulo del ámbito penal del RPDUE a los organismos que tenían marcos de protección de datos separados en sus actos constitutivos cuando se adoptó el RPDUE, a saber, Europol y la Fiscalía Europea. También hace referencia a una posible modificación del capítulo del ámbito penal, en caso necesario.

6.1 Ampliación de la aplicación del capítulo del ámbito penal del RPDUE

En el momento de redactar el presente documento, el capítulo del ámbito penal del RPDUE se aplica al tratamiento de datos personales operativos por parte de:

- Eurojust[80], complementado con normas específicas recogidas en el Reglamento de Eurojust;
- Europol[81], complementado con normas específicas recogidas en el Reglamento de Europol, que ha sido modificado[82] desde la entrada en vigor del RPDUE;
- Frontex, para la pequeña parte de sus actividades comprendidas en el ámbito penal[83].

[79] Artículo 98, apartado 2, del RPDUE.
[80] Artículo 26 del Reglamento (UE) 2018/1727 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, sobre la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust) y por el que se sustituye y deroga la Decisión 2002/187/JAI del Consejo (DO L 295 de 21.11.2018, p. 138).
[81] Artículo 28 del Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo (Reglamento de Europol posteriormente modificado).
[82] Reglamento (UE) 2022/991 del Parlamento Europeo y del Consejo, de 8 de junio de 2022, por el que se modifica el Reglamento (UE) 2016/794 en lo que se refiere a la cooperación de Europol con entidades privadas, el tratamiento de datos personales por Europol en apoyo de investigaciones penales y el papel de Europol en materia de investigación e innovación (DO L 169 de 27.6.2022, p. 1).
[83] Véanse los artículos 10, apartado 1, letra q), y 90 del Reglamento (UE) 2019/1896 del Parlamento Europeo y del Consejo, de 13 de noviembre de 2019, sobre la Guardia Europea de Fronteras y Costas y por el que se derogan los Reglamentos (UE) n.º 1052/2013 y (UE) 2016/1624 (DO L 295 de 14.11.2019, p. 1), https://eur-lex.europa.eu/eli/reg/2019/1896/oj.

Sin embargo, el capítulo del ámbito penal del RPDUE aún no se aplica a la Fiscalía Europea, cuyo Reglamento constitutivo se adoptó antes que el RPDUE. El Reglamento de la Fiscalía Europea establece un régimen independiente para el tratamiento de datos operativos. Esto tiene dos consecuencias: en primer lugar, algunas disposiciones del Reglamento de la Fiscalía Europea difieren en cuanto al fondo del capítulo del ámbito penal del RPDUE, por ejemplo, en lo que respecta al tratamiento «limitado» de datos personales[84]. En segundo lugar, algunas disposiciones del Reglamento de la Fiscalía Europea, a pesar de ser similares en cuanto al fondo, están redactadas de manera diferente a la del capítulo del ámbito penal del RPDUE, lo que podría dar lugar a interpretaciones distintas.

En aras de la coherencia y en consonancia con el objetivo general de minimizar la fragmentación de las normas sobre protección de datos, debe seguirse un enfoque similar al adoptado para Eurojust y Europol en el caso de la Fiscalía Europea. El objetivo es garantizar la aplicabilidad directa del capítulo del ámbito penal del RPDUE a la Fiscalía Europea, manteniendo únicamente las especificaciones necesarias en el Reglamento de la Fiscalía Europea. Al mismo tiempo, dado que la Fiscalía Europea solo lleva un año en funcionamiento, a corto plazo sigue siendo necesario recabar más información sobre la aplicación práctica del régimen de protección de datos de la Fiscalía Europea, lo que permitirá definir con precisión dichas especificaciones, teniendo en cuenta la naturaleza de fiscalía independiente de la UE que tiene la Fiscalía Europea[85].

6.2 Aclaración de la aplicabilidad de determinadas disposiciones del RPDUE al tratamiento de datos operativos

El RPDUE[86] establece que «[s]olo el artículo 3 [definiciones] y el capítulo IX [capítulo del ámbito penal] del presente Reglamento serán aplicables al tratamiento de datos personales operativos».

El capítulo del ámbito penal contiene disposiciones sustantivas que se corresponden con la mayoría de las disposiciones de los capítulos II a V del RPDUE (principios generales, derechos del interesado, determinadas obligaciones de los responsables y encargados del tratamiento y transferencias internacionales de datos), con algunas diferencias para tener en cuenta la naturaleza específica del ámbito penal (por ejemplo, las normas sobre la comunicación de información a los interesados y sobre el derecho de acceso a sus datos).

Es importante aclarar, mediante una modificación del RPDUE, que el capítulo del ámbito penal establece normas específicas únicamente para las disposiciones correspondientes de otros

[84] El artículo 61, apartado 4, del Reglamento de la Fiscalía Europea prevé un tratamiento «limitado» de los datos «con excepción de la conservación, solo […] con fines de protección de los derechos del interesado o de cualquier otra persona física o jurídica que sea parte en los procedimientos de la Fiscalía Europea, o a los fines [probatorios]». El correspondiente artículo 82, apartado 3, del RPDUE, establece que «los datos objeto de una limitación solo se tratarán para los fines que impidieron su supresión», lo que incluye la conservación de los datos a efectos probatorios, pero no hace referencia a la protección de los derechos del interesado o de terceros.

[85] La experiencia adquirida con Eurojust y Europol no es directamente aplicable a la Fiscalía Europea, dado que el mandato de la Fiscalía Europea no consiste en apoyar y mejorar la cooperación entre las autoridades nacionales, sino en investigar y enjuiciar los delitos que afectan a los intereses financieros de la UE.

[86] Artículo 2, apartado 2, del RPDUE.

capítulos del RPDUE que tengan un equivalente directo en el capítulo del ámbito penal. De este modo, si el legislador no incluye normas específicas en el acto constitutivo de un organismo, las disposiciones de los capítulos distintos al capítulo del ámbito penal que no tienen equivalente directo en este último[87] se aplicarán al tratamiento de datos operativos.

Esta modificación mejoraría la seguridad jurídica y proporcionaría un marco completo (por ejemplo, sobre la posición de los DPD y la cooperación con las autoridades nacionales de control de la protección de datos), también para cualquier futuro organismo en este ámbito[88]. Contar con un marco completo de este tipo reduciría también los riesgos de fragmentación.

6.3 Potestades del SEPD en la supervisión de los órganos y organismos de la UE

En la actualidad, los Reglamentos por los que se crean la Fiscalía Europea, Eurojust y Europol contienen disposiciones concretas sobre las competencias del SEPD[89].

El Reglamento de Europol actualizado otorga al SEPD potestades que se ajustan a las previstas en el artículo 58 del RPDUE[90]. Este es el caso, en particular, de la potestad para imponer multas administrativas y la potestad para ordenar al responsable o al encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones pertinentes, cuando proceda, de una determinada manera y dentro de un plazo especificado.

Sin embargo, en el caso de la Fiscalía Europea, las potestades del SEPD se formulan de un modo diferente al del RPDUE. El SEPD no tiene las dos potestades mencionadas[91].

El Reglamento Frontex, por lo que se refiere a la pequeña parte de las actividades de Frontex sujetas al capítulo del ámbito penal[92], no contiene ninguna disposición específica sobre las potestades del SEPD, lo que da lugar a incertidumbres sobre dichas potestades.

Siguiendo los dos pasos siguientes, podría conseguirse dotar al SEPD de todas las potestades establecidas en el artículo 58 del RPDUE.

---

[87] Por ejemplo, en relación con la obligación de los responsables del tratamiento de cooperar en virtud del artículo 32 del RPDUE, las normas sobre los delegados de protección de datos establecidas en los artículos 43 a 45 del RPDUE, el artículo 31 sobre el registro de las actividades de tratamiento, y sobre la cooperación con otras autoridades de control en virtud del artículo 61 del RPDUE.

[88] No obstante, el marco jurídico específico de estos organismos tendría que establecerse en consonancia con los requisitos del RPDUE, por ejemplo, el artículo 72 sobre la definición de los plazos de conservación. Pero no sería necesario regular los derechos de los interesados ni las potestades del SEPD, a menos que el legislador decidiera específicamente apartarse del enfoque del RPDUE.

[89] Artículo 85 del Reglamento de la Fiscalía Europea, artículo 40 del Reglamento de Eurojust y artículo 43 del Reglamento de Europol.

[90] Algunas funciones del SEPD que no son pertinentes para Europol, como la aprobación de cláusulas contractuales tipo, no se repiten.

[91] De conformidad con el artículo 85, apartado 3, letra b), del Reglamento de la Fiscalía Europea, y el artículo 40, apartado 3, letra b), del Reglamento de Eurojust, en caso de presunta infracción de las disposiciones que rigen el tratamiento de datos personales operativos, el SEPD solo puede remitir el asunto a la Fiscalía Europea o a Eurojust y, en su caso, formular propuestas encaminadas a corregir dicha infracción y a mejorar la protección de los interesados.

[92] Véanse el artículo 10, apartado 1, letra q), y el artículo 90 del Reglamento Frontex.

1. Aclarar que el RPDUE, como opción por defecto, encomienda al SEPD la supervisión del capítulo del ámbito penal y le confiere las facultades que le otorga el artículo 58 del RPDUE[93], lo que requiere modificar el RPDUE tal como se propone en la sección anterior,
   y también colmaría la laguna del Reglamento Frontex.

2. Al suprimir las disposiciones sobre las potestades del SEPD de los actos constitutivos de los órganos y organismos, todo el conjunto de potestades del SEPD en virtud del RPDUE modificado se aplicaría directamente a Eurojust y a la Fiscalía Europea. El objetivo es armonizarlos lo máximo posible para reducir la fragmentación de las normas sobre protección de datos.

7 Próximos pasos

En términos generales, el RPDUE funciona bien y se adecua a su finalidad. En este punto, la Comisión no va a proponer modificaciones para aquellas partes que son equivalentes a las normas correspondientes del RGPD, manteniendo así la armonización más estrecha posible entre el RPDUE y el RGPD[94]. Las posibles modificaciones que se consideran en el presente informe afectan a otras partes, en particular a la relación del capítulo del ámbito penal del RPDUE con las demás disposiciones de este Reglamento.

En la primavera de 2022, la Comisión propuso normas para reforzar la seguridad de la información en las IOUE[95], lo que tendrá una repercusión positiva en la seguridad de la información, especialmente en la protección de los datos personales. Esta propuesta aspira a seguir mejorando la resiliencia y la capacidad de las IOUE para responder a incidentes cuando se enfrenten a amenazas relacionadas con la ciberseguridad.

La Comisión también tomará las medidas descritas en los puntos siguientes:

- al actualizar los actos constitutivos de los sistemas informáticos a gran escala que todavía incluyan normas detalladas sobre un modelo de supervisión coordinada, se asegurará de que se aplique el modelo de supervisión coordinada[96] del RPDUE con el fin de racionalizar los procedimientos;

- estudiará posibles modificaciones del RPDUE con el fin de:

[93] El artículo 1, apartado 3, del RPDUE encomienda al SEPD la labor de «[supervisar] la aplicación de las disposiciones del presente Reglamento a todas las operaciones de tratamiento realizadas por las instituciones y organismos de la Unión». Aunque puede interpretarse que esta disposición se aplica también a las actividades comprendidas en el capítulo del ámbito penal, sería útil explicitarlo para garantizar la seguridad jurídica.
[94] En caso de que el RGPD se modificara en una fase posterior, la Comisión estudiará las modificaciones necesarias del RPDUE para que ambos textos queden armonizados.
[95] Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen medidas destinadas a garantizar un elevado nivel común de ciberseguridad en las instituciones, los órganos y los organismos de la Unión [COM(2022) 122 final].
[96] Artículo 62 del RPDUE.

- mejorar la seguridad jurídica y completar el marco para el tratamiento de datos operativos aclarando en el artículo 2, apartado 2 que las disposiciones generales del RPDUE también se aplican al tratamiento de datos personales operativos, a menos que el capítulo del ámbito penal contenga disposiciones específicas (por ejemplo, sobre el derecho de acceso). Esto también proporcionaría un marco ya definido para los futuros organismos en los ámbitos de la cooperación judicial en materia penal y la cooperación policial;
- garantizar la participación del SEPD en calidad de observador en todas las evaluaciones de la protección de datos en el marco del mecanismo de evaluación de Schengen;

- posteriormente, estudiará la posibilidad de modificar los Reglamentos de la Fiscalía Europea y de Eurojust en una futura revisión para garantizar la plena aplicación de las normas sobre el tratamiento de datos personales operativos del RPDUE modificado, teniendo en cuenta la naturaleza específica de dichos organismos. Esto también propiciará la armonización de las potestades del SEPD sobre estos órganos y organismos con las que tiene sobre las demás IOUE;
- propondrá cláusulas contractuales tipo para las transferencias internacionales de datos personales[97] de las IOUE;
- proseguirá la estrecha cooperación con el SEPD (y, cuando proceda, el CEPD) para garantizar una consulta oportuna y específica sobre nuevas propuestas[98], además de seguir consultando de manera oficiosa al SEPD sobre textos importantes antes de su adopción.

[97] De conformidad con el artículo 48, apartado 2, letra b), del RPDUE.
[98] De acuerdo con el artículo 42 del RPDUE.

Se invita al SEPD a:

- proporcionar orientaciones prácticas adicionales y oportunas a las IOUE, en particular en lo que respecta a las transferencias internacionales de datos;
- seguir concienciando a los responsables y encargados del tratamiento sobre sus obligaciones en virtud del RPDUE y asesorando a los DPD;
- intensificar los esfuerzos para aplicar eficazmente el RPDUE con vistas a garantizar la plena protección de los interesados.

Se invita a las instituciones, órganos y organismos de la UE a:

- proseguir y, cuando sea necesario, intensificar los esfuerzos de sensibilización para garantizar que haya un nivel suficiente de conocimientos especializados a nivel interno sobre las normas del RPDUE;
- considerar la posibilidad de publicar las EIPD, excluyendo la información que pudiera comprometer las garantías de seguridad adoptadas en caso necesario;
- velar por que los DPD (así como los CPD) gocen de recursos suficientes y de una posición dentro de las IOUE que les permitan desempeñar sus funciones de manera eficiente e independiente;
- acabar de convertir en registros de protección de datos las notificaciones pendientes conforme al anterior Reglamento de protección de datos.

ANEXO

Cuadro 1: evaluaciones de impacto relativas a la protección de datos y consultas previas llevadas a cabo por las IOUE

	2019	2020	2021
Riesgo residual aceptado	30	50	77
Consulta previa del SEPD	3	3	5
Proyecto abandonado	2	2	0

Cuadro 2: actividades de control del SEPD

	2018	2019	2020	2021
Consultas	50[99]	75	59	52
Consultas previas	0	0	1	4
Autorizaciones de transferencia	0	1	0	4
Reclamaciones admisibles recibidas	58	59	43	44[100]
Decisiones[101] sobre reclamaciones admisibles	23	48	35	22
Reclamaciones inadmisibles recibidas	240	151	203	269
Inspecciones / auditorías realizadas	5	9	4	4
Investigaciones formales llevadas a cabo	0	4	1	2
Notificaciones de violaciones de la seguridad	7	95	121	82[102]

[99] Dos de ellas fueron posteriores a la entrada en vigor del RPDUE.
[100] Hasta el 15 de noviembre de 2021.
[101] Incluidos los casos cerrados tras llegar a una solución amistosa, remitirlos al DPD o por otros medios.
[102] Hasta mitad de noviembre de 2021.

de los datos recibidas				

Cuadro 3: actividades consultivas del SEPD

	2018	2019	2020	2021
Observaciones	13	3	19	72
Dictámenes	7	6	8	12
Dictámenes de iniciativa	1	1	2	0
Dictámenes conjuntos con el CEPD	0	1	0	5
Observaciones informales	33[103]	16	13	25

Cuadro 4: recursos del SEPD

	2018	2019	2020	2021	2022 (estimación)
Número total de miembros del personal del SEPD (incluida la Secretaría del CEPD)	98	100	118	126	139
Personal del SEPD en la Secretaría del CEPD	19	22	27	34	38
Presupuesto [104]	13 539 302 EUR (ejecutado)	15 301 687 EUR (ejecutado)	14 211 719 EUR (ejecutado)	16 761 285 EUR (ejecutado)	20 202 000 EUR (proyecto)

[103] De conformidad con el anterior Reglamento (CE) n.º 45/2001, el SEPD contabilizaba las consultas sobre actos delegados o de ejecución como observaciones «informales». Una parte de las observaciones que figuran como observaciones informales en 2018 se habría contabilizado como «observaciones formales» en años posteriores.

[104] Estas cifras se han actualizado con respecto a las cifras proporcionadas por el SEPD en su contribución al presente informe.