El Manual del DPD

(Delegado de Protección de Datos)

Guía para los Delegados de Protección de Datos en los sectores públicos y semi-públicos sobre cómo garantizar el cumplimiento del Reglamento General de Protección de Datos de la Unión Europea

(Reglamento (UE) 2016/679)

Elaborado para el proyecto "T4DATA" financiado por la UE

(Acuerdo de subvención número: 769100 — T4DATA — REC-DATA-2016/REC-DATA-2016-01)

por

Douwe Korff

Profesor Emérito de Derecho Internacional, London Metropolitan University
Profesor Asociado Oxford Martin School, Universidad de Oxford

&

Marie Georges

Experta internacional europea en protección de datos (CNIL, EU, Consejo de Europa, etc.)

Miembros del Grupo de Expertos Europeos de Derechos Fundamentales (Fundamental Rights Experts Europe - FREE)

Aprovechando las principales contribuciones de la Agencia Italiana de Protección de Datos & los socios del proyecto

Aprobado por la Comisión, julio de 2019

Sobre este Manual:

Este manual ha sido preparado como parte de los materiales para el programa de formación de formadores "T4DATA" financiado por la UE, destinado a formar al personal de varias agencias de protección de datos (APD) de los Estados miembros de la UE en la formación de delegados de protección de datos (DPD), especialmente en el sector público, en sus nuevas obligaciones bajo el Reglamento General de Protección de Datos de la UE (Reglamento 2016/679, RGPD). El proyecto se lleva a cabo bajo la iniciativa de la agencia italiana de protección de datos, la *Garante per la protezione dei dati personali* (en lo sucesivo, *'Garante' o 'Garante della Privacy'*), y administrado por la Fondazione Basso, con la ayuda de dos expertos del Grupo de Expertos en Derechos Fundamentales de Europa (FREE), la Sra. Marie Georges y el Prof. Douwe Korff.

El Manual está basado en contribuciones importantes de *Garante della Privacy* y de otros socios de DPA que enviaron ejemplos prácticos muy útiles y copias de sus propias notas de orientación sobre el RGPD.

Cabe señalar que cuando un tema hace referencia al trabajo anterior de uno de los dos expertos, aparecerá su nombre en un pie de página relacionado solo cuando se trate de recursos disponibles de forma pública. Esto raramente ocurre en el caso de Marie Georges debido a razones de institucionalidad o confidencialidad relacionadas con su trabajo sobre protección de datos para organismos gubernamentales nacionales e internacionales.

Para obtener información sobre el programa, los socios y los expertos pueden acceder a:
http://www.fondazionebasso.it/2015/wp-content/uploads/2018/04/T4Data_Brochure.pdf

Aunque se creó para el programa T4DATA, se espera que el Manual sea útil también para cualquier otra persona interesada en la aplicación del Reglamento y, en particular, para otros RPD (del sector público o privado), poniéndose a disposición del público con una licencia "Creative Commons" (CC).

Nota: Dado que el manual tiene por objeto apoyar la formación de los responsables de la protección de datos (RPD) en sus nuevas funciones en el marco del GDPR, está centrado en la legislación de la UE en materia de protección de datos y, más concretamente, en la legislación de protección de datos en relación con lo que antes se denominaban cuestiones del "Primer Pilar" o del "mercado interior". Sin embargo, las secciones 1.3.4 - 1.3.6 y 1.4.3 - 1.4.5 introducen brevemente las normas e instrumentos de protección de datos que se aplican o se aplican a otras cuestiones cubiertas por la legislación de la UE, a saber asuntos relacionados con el ámbito de lo que antes se denominaba "Justicia y Asuntos de Interior" (JAI) o "Tercer Pilar" -ahora denominado "Espacio de Libertad, Seguridad y Justicia" (FSJ); asuntos relacionados con la denominada Política Exterior y de Seguridad Común (PESC) - el anterior "Segundo Pilar"; y las actividades de las propias instituciones de la UE; y la sección 1.4.6 trata de las transferencias de datos entre los diferentes regímenes de la UE. Tampoco está cubierta la protección de datos fuera de la UE/EEE, aunque creemos que los RPD deberían adquirir al menos cierto conocimiento de la gran influencia que las normas de la UE han tenido, y siguen teniendo, en la protección de datos en todo el mundo.
Esperamos poder añadir estas cuestiones en una segunda edición posterior de este manual, en la que también podremos actualizar la información sobre cuestiones pendientes en el momento de redactar esta primera edición, como, en particular, los avances en relación con el Reglamento sobre la privacidad electrónica, que en el momento de redactar este documento todavía está en proceso legislativo.
El manual también está disponible en italiano, croata, búlgaro, polaco, español (es decir, todos los idiomas de los socios). Estamos estudiando la posibilidad de realizar otras traducciones (en particular, una traducción al francés) (dependiendo de la financiación).

EXENCION DE RESPONSABILIDADES:

La información y las opiniones expuestas en este manual son las de sus autores y no reflejan necesariamente la opinión oficial de la Unión Europea. Ni las instituciones y organismos de la Unión Europea, ni ninguna persona que actúe en su nombre podrá ser considerada responsable del uso que pueda hacerse de la información que contiene dicho manual.

Prólogo

Esta primera edición del *"Manual"* elaborado como parte del proyecto *"T4Data - Formación para Protección de Datos"*, financiado por la Unión Europea, es, a nuestro parecer, algo más que *"otro manual"* sobre el RGPD.

Es una verdadera guía práctica que ha sido posible en primer lugar, gracias al trabajo arduo y el compromiso demostrado por los dos expertos seleccionados para este cometido, la Sra. Marie Georges y el Catedrático Douwe Korff, quienes están enormemente familiarizados con los derechos humanos, las cuestiones relacionadas con las TIC y la protección de datos, tanto conceptualmente como en la práctica, y en segundo lugar, gracias a la contribución de los funcionarios y miembros de las cinco autoridades de supervisión participantes, quienes han confiado en su práctica y experiencia diarias para proporcionar valiosas aportaciones a la orientaciones contenidas en el manual.

Es, sobre todo, una obra en evolución, ley viva, no es letra muerta. Está destinado a traducir las nuevas y sin duda más exigentes tareas de **responsabilidad activa** establecidas en el nuevo marco legal de la UE – que tienen como objetivo garantizar la eficiencia de la protección de datos en un mundo donde el tratamiento de datos está abarcando todas las dimensiones de la vida – en una guía de orientaciones prácticas, sólidas y documentadas, que se ajustarán y ampliarán aún más gracias a las actividades nacionales de capacitación y difusión que se desarrollarán a lo largo de 2019 sobre los fundamentos de este manual. Los destinatarios de esta guía son los Delegados de Protección de Datos (DPDs), y especialmente los DPDs que trabajan en el sector público, quienes podrán utilizarla como una especie de trampolín para fortalecer y mejorar su competencia en el manejo de los asuntos de protección de datos en beneficio de todos los interesados: los responsables, los afectados y el público en general.

Esta es la razón por la cual nuestras cinco autoridades nacionales de protección de datos decidieron unir fuerzas para llevar a cabo el Proyecto T4Data, y también por ello nos complace especialmente presentar este valioso fruto del proyecto, en inglés y traducido a nuestros respectivos idiomas nacionales, y esperamos que también al francés en un futuro, conscientes de que supondrá un fortalecimiento del conjunto de herramientas de cooperación que estamos forjando día a día a nivel europeo y mundial.

Doctora Edyta Bielak – Jomaa, Presidenta de la Oficina de Protección de Datos de Polonia.

Mar España Martí, Directora de la Agencia Española de Protección de Datos.

Ventsislav Karadjov, Presidente de la Comisión de Protección de Datos de la República de Bulgaria.

Anto Rajkovača, Director de la Agencia Croata de Protección de Datos.

Antonello Soro – Presidente de la Autoridad Italiana de Protección de Datos.

CONTENIDO

Continúa en la siguiente página

Contenido (continuación):

- o – O – o -

Douwe Korff & Marie Georges

EL Manual del DPD

Manual para delegados de protección de datos sobre cómo garantizar el cumplimiento del Reglamento general de protección de datos de la UE en sectores públicos y semipúblicos

(Reglamento (EU) 2016/679)

Introducción

El 25 de mayo de 2018, entró en vigor el nuevo Reglamento General de Protección de Datos de la UE (RGPD o "el Reglamento")[1], que sustituye a la Directiva de 1995 sobre protección de datos ("Directiva de 1995")[2]. Adoptada en respuesta a la expansión masiva del proceso de datos personales desde la introducción de la Directiva de 1995, y al desarrollo de tecnologías cada vez más intrusivas, el Reglamento se basa en la Directiva y en la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE). Al hacerlo, expande de manera significativa el contenido de la Directiva y de esta manera, refuerza considerablemente el principal régimen de protección de datos de la UE. Trae consigo muchos cambios en términos de una armonización mucho mayor, derechos de los sujetos de los datos más sólidos, una cooperación transfronteriza más estrecha entre las autoridades de protección de datos (APD) etc.

Entre los cambios más importantes se encuentran la introducción de un nuevo principio, el principio de "rendición de cuentas" y la institución de los delegados de protección de datos designados por el controlador (DPD). Los dos están vinculados: los DPD serán las personas que en la práctica deberán garantizar el cumplimiento del principio de responsabilidad por y dentro de las organizaciones a las que pertenecen. Este Manual busca apoyar a los nuevos DPD en el sector público en ese esfuerzo.

Este Manual consta de tres partes:

- La Primera Parte introduce los conceptos de "confidencialidad", "privacidad" y "protección de datos" y las primeras leyes de protección de datos, principios e instrumentos internacionales (en particular el Convenio de Protección de Datos del Consejo de Europa de 1981), antes de discutir los datos de "Primer Pilar" directivas de protección de la década de la UE de 1990 y principios de la de 2000, e introducir los instrumentos de protección de datos recientemente adoptados y pendientes para el futuro (el RGPD, el Reglamento de privacidad electrónica propuesto y el Convenio "modernizado" del Consejo de Europa).[3] La Primera Parte no aborda los instrumentos del "Tercer Pilar" creados por la UE de la década de 1990 ni la regulación sobre protección de datos para las propias instituciones de la UE y sus sucesoras.*
  *Se espera que en el futuro se pueda elaborar una segunda edición más detallada de este Manual en la que también se traten estos instrumentos.

- La Segunda Parte proporciona una visión general de todos los elementos clave del Reglamento General de Protección de Datos, antes de centrarse en el nuevo y principal principio de "responsabilidad" y el concepto y las reglas del RGPD relacionadas con el Delegado de Protección de Datos; y

- La Tercera Parte proporciona una guía práctica sobre cómo los DPD del sector público pueden y

[1] Título completo: Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y sobre la libre circulación de dichos datos, y por la que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), DOUE. L 119 del 4.5.2016, p. 1 et seq., disponible en: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
Obsérvese que, aunque el Reglamento se adoptó en 2016 y entró legalmente en vigor el vigésimo día siguiente al de su publicación en el Diario Oficial de la Unión Europea, es decir, el 25 de mayo de ese año (artículo 99, apartado 1), no entró en vigor hasta el 25 de mayo de 2018 (artículo 99, apartado 2).

[2] Título completo: Directiva 95/46 / CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, DO L 281 de 23.11. 1995, p. 31ff, disponible en:
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[3] Ver la nota del recuadro "Acerca de este Manual" en la pág. 1 sobre las limitaciones de los asuntos tratados

deben cumplir con sus numerosas tareas, con ejemplos de la vida real, que se relacionan en particular con las tres áreas de enfoque: educación, finanzas y cuidado de la salud, y ejercicios.

Además de extensas referencias y enlaces a materiales en las notas a pie de página, un segundo volumen por separado (Volumen Dos) del Manual contiene materiales extensos adicionales que están disponibles para los participantes en los ejercicios de formación "T4DATA".

Página web:

La mayor cantidad posible de los materiales y enlaces mencionados anteriormente también estarán disponibles en la página web de acceso público que acompaña este Manual (que también está disponible de forma gratuita bajo una licencia de "Creative Commons" del sitio web):

http://www.fondazionebasso.it/2015/t4data-training-data-protection-authorities-and-data- protection-officers/

PARTE UNO

Los orígenes y el significado de la protección de datos

Esta parte trata de explicar qué es la protección de datos y cómo se desarrolló en Europa, y cómo los instrumentos europeos de protección de datos nuevos y "modernizados" buscan abordar los últimos avances tecnológicos.

- La sección 1.1 presenta de los diferentes conceptos (si se superponen) de confidencialidad, privacidad, vida privada, protección de datos y el enfoque de este último desarrollado en Europa, incluidos los requisitos de derechos humanos y el estado de derecho que, en Europa, apuntalan protección de datos.

- La sección 1.2 cubre los orígenes de la protección de datos en Europa, la aparición de los principios y derechos básicos de protección de datos y su desarrollo en instrumentos jurídicos europeos y mundiales no vinculantes, y en uno vinculante, el Convenio de Protección de Datos de 1981 del Consejo de Europa (incluido su Protocolo Adicional de 2001).

- La sección 1.3 trata de la forma en que las normas y principios de protección de datos se desarrollaron en las directivas de protección de datos de 1990 y 2000 (para permitir el desarrollo del "mercado interior" de la UE, que requería tanto la libre circulación de datos como la protección del derecho fundamental a la protección de datos), con especial atención a la Directiva de Protección de Datos de 1995 (con la que el Protocolo Adicional de 2001 al Convenio de 1981 trató de armonizar dicho Convenio) (subsecciones 1.3.1 y 1.3.2); y se examinan las normas especiales para el sector de las telecomunicaciones (subsección 1.3.3).

  Las últimas subsecciones de esta sección se refieren brevemente a los instrumentos de protección de datos en lo que antes se denominaba Justicia y Asuntos de Interior (JAI) (subsección 1.3.4); en relación con la Política Exterior y de Seguridad Común (PESC) (subsección 1.3.5); y para las propias instituciones de la UE (subsección 1.3.6).

- La sección 1.4 introduce los últimos instrumentos jurídicos adoptados para hacer frente al futuro: el Reglamento General de Protección de Datos de la UE de 2016 (GDPR, en aplicación desde el 25 de mayo de 2018) (subsección 1.4.1) y la propuesta de sustitución de la Directiva comunitaria de 2002 sobre privacidad en las comunicaciones electrónicas por un Reglamento sobre privacidad en las comunicaciones electrónicas (subsección 1.4.2).

  Los siguientes apartados de esta sección se refieren brevemente al principal nuevo instrumento de protección de datos en lo que ahora se denomina el espacio de justicia, libertad y seguridad (ECI), la Directiva sobre protección de datos de las fuerzas de seguridad de 2016 (subapartado 1.4.3); la situación en relación con la PESC (subapartado 1.4.4); y la actualización del instrumento de protección de datos para las instituciones de la UE, el Reglamento 2018/1725 (subapartado 1.4.5). En la subsección 1.4.6 se analizan los flujos de datos entre los diferentes regímenes de protección de datos de la UE.
  El Convenio "Modernizado" del Consejo de Europa, abierto a la firma en octubre de 2018, se trata en la subsección final (subsección 1.4.7).

  NB: Esperamos presentar los instrumentos de protección de datos de la UE para las áreas mencionadas anteriormente (cooperación policial y judicial, PESC y las propias instituciones de la UE), adoptados para sustituir a los de los años noventa y principios de la década de 2000, y las últimas normas mundiales, con más detalle en una segunda edición.

El RGPD, que es el núcleo de este manual, se examina con más detalle en la Parte Dos.

1.1 Confidencialidad, privacidad/vida privada y protección de datos: conceptos diferentes pero complementarios en la era de la digitalización

1.1.1 Confidencialidad y privacidad/vida privada

Siempre ha habido áreas en las que la información personal fue tratada como sujeta a reglas especiales de **confidencialidad**. Los ejemplos clásicos son el Juramento hipocrático del siglo IV a. C. para **médicos**[4] y el **"secreto de confesión"**[5] de la Iglesia Católica.[5] Más recientemente, en particular del siglo XIX, banqueros, abogados, otros ministros de confesiones religiosas, los **empleados de correos y telecomunicaciones** y muchos otros han sido obligados a tratar la información que reciben de las personas en su capacidad oficial como confidencial, privilegiada[6] o incluso sacrosanta.

Tales obligaciones de confidencialidad generalmente se consideraban que servían tanto al individuo como a la sociedad: el individuo podía tener fe en que la persona a la que revelaba la información trataría dicha información con confidencialidad, y dicha confianza a su vez servía para el bien público, ya que su ausencia puede disuadir a las personas para buscar ayuda o revelar información a las autoridades, lo que socava la salud pública y otros beneficios sociales, por ejemplo, al tratar de contrarrestar la propagación de enfermedades de transmisión sexual o el extremismo político o religioso.

Sin embargo, tal y como explica Frits Hondius, subdirector de derechos humanos en el Consejo de Europa y responsable de la redacción del primer instrumento de protección de datos internacionalmente vinculante, el Convenio sobre protección de datos del Consejo de Europa de 1981, tratado en la sección 1.2.3, más adelante, aunque existiera este deber de confidencialidad:[7]

> no existía el correspondiente derecho conferido a pacientes, clientes o ciudadanos para verificar la exactitud y relevancia de los datos que los concernían. Y aunque existían sanciones legales para castigar los graves abusos del manejo de datos, no había leyes que proporcionaran indicaciones positivas sobre cómo los archivos de datos personales deberían ser configurados y administrados correctamente.

El derecho a la "**privacidad**" o al "**respeto a la vida privada**" se consagró en los tratados internacionales de derechos humanos posteriores a la Segunda Guerra Mundial, el Convenio Internacional de Derechos Civiles y Políticos de la ONU (ICCPR, art.17) y el Convenio Europeo de Derechos Humanos (CEDH, Art. 8).[8] Protege principalmente contra las interferencias innecesarias del Estado en la vida privada de una persona, como la interceptación de comunicaciones por parte de agencias estatales[9] o la criminalización de actos sexuales

---

[4] El Juramento Hipocrático es atribuido a Hipócrates (460-370 aC) en la antigüedad, aunque la información más reciente muestra que puede haber sido escrito después de su muerte. La versión más antigua existente data de alrededor de 275 dC y es la siguiente:
ἃ δ᾽ ἂν ἐνθεραπείῃ ἴδω ἢ ἀκούσω, ἢ καὶ ἄνευ θεραπείης κατὰ βίον ἀνθρώπων, ἃ μὴ χρή ποτε ἐκλαλεῖσθαι ἔξω, σιγήσομαι, ἄρρητα ἡγεύμενος εἶναι τὰ τοιαῦτα.
"Y lo que sea que vea o escuche en el curso de mi profesión, así como fuera de mi profesión en mi relación con hombres, si es lo que no debería publicarse en el extranjero, nunca lo divulgaré, manteniendo tales cosas como secretos sagrados". (Traducción de James Loeb, 1923). Véase
https://en.wikipedia.org/wiki/Hippocratic_Oah

[5] En la Iglesia Católica Romana, el "secreto del confesionario" o "secreto sacramental" es inviolable.
Véase: https://www.catholiceducation.org/en/religion-and-philosophy/catholic-faith/the-seal-of-the-confessional.html

[6] Como lo expresa la Autoridad de Regulación de Abogados (SRA, por sus siglas en inglés), que regula los abogados y las leyes en Inglaterra y País de Gales, existe (en la ley inglesa) una "diferencia entre la confidencialidad y el privilegio profesional legal. En pocas palabras, la información confidencial puede divulgarse cuando resulte apropiado, pero el privilegio es absoluto y, por lo tanto, la información privilegiada no puede divulgarse. Las comunicaciones confidenciales entre abogados y clientes con el fin de obtener y brindar asesoría legal son privilegiadas".
https://www.sra.org.uk/solicitors/code-of-conduct/guidance/guidance/Disclosure-of-client-confidential- information.page
En Francia, el secreto profesional de un abogado (avocat) es una cuestión de orden público, absoluto, ilimitado en el tiempo y que abarca todo tipo de asuntos legales y cualquier tipo de información (escrita, electrónica, de audio, etc.). Véase:
http://www.avocatparis.org/mon-metier-davocat/deontologie/secret-professionnel-et-confidentialite

[7] Frits Hondius, Una década de protección internacional de datos en: Netherlands International Law Review, Vol. XXX (1983), pp. 103 – 128 (no disponible online)

[8] El Artículo 12 de la Declaración Universal de Derechos Humanos de 1948, que fue el instrumento "madre" tanto para el PIDCP como para el CEDH (pero que no es un tratado vinculante), ya estipuló en el Artículo 12 que: "Nadie será sometido a interferencia arbitraria en su privacidad, familia, domicilio o correspondencia ... "El ICCPR y el CEDH se redactaron en paralelo en 1949-50 (pero el CEDH, que se abrió a la firma a fines de 1950 y entró en vigor en 1953, entró en vigor más de veinte años antes del ICCPR, que se abrió a la firma en 1966 y entró en vigor solo en 1976).

[9] p.e., ECtHR, Klass v. Alemania, sentencia del [AÑADIR FECHA]

privados.[10] Sin embargo, el Tribunal Europeo de Derechos Humanos también ha interpretado este derecho en el sentido de que exige que el estado proteja a los individuos contra la publicación de fotografías tomadas de ellos por entidades privadas, sin su consentimiento, en un entorno privado,[11] y en contra de la interceptación de sus comunicaciones por parte de sus empleadores sin una base legal adecuada.[12]

No obstante, aunque el artículo 8 del CEDH se ha interpretado y aplicado cada vez más para proteger a las personas con respecto a sus datos personales y en relación con la recopilación, uso y conservación de dichos datos, especialmente por parte de las agencias de seguridad estatales y nacionales,[13] en los años 70 y 80, la medida en que se podía confiar en el derecho a la vida privada en las relaciones entre individuos, y entre individuos y entidades privadas (la llamada cuestión del "efecto horizontal de los derechos humanos" o Drittwirkung) todavía no estaba muy claro[14] - y aún no se ha resuelto completamente en términos de la ley tradicional de derechos humanos. En cualquier caso, las personas no pueden derivar del CEDH (o el ICCPR) un derecho de acción contra otras personas: lo máximo que pueden hacer es tomar medidas contra el estado correspondiente por no protegerlas, en la legislación interna pertinente, contra las acciones de tales otras personas.

En resumen: Las leyes y normas sobre confidencialidad, privilegio profesional y secreto, y las garantías de los derechos humanos de privacidad y vida privada no protegían adecuadamente a las personas contra la recopilación abusiva y el uso de sus datos personales, y no lo hacen.
En consecuencia, más recientemente, se ha reconocido un derecho diferente e independiente a la "protección de datos personales" ("protección de datos"), como se analiza a continuación. Pero, por supuesto, este nuevo derecho *sui generis* siempre debe verse como estrechamente vinculado y complementario de los derechos tradicionales, como se consagra en el CEDH y el PIDCP en particular: la protección de datos busca garantizar la aplicación plena y efectiva de los derechos tradicionales en el (relativamente) nuevo contexto digital.

1.1.2 "Protección de datos"

Los ordenadores se construyeron por primera vez con fines militares en la Segunda Guerra Mundial. Los descifradores del Reino Unido, bajo la dirección del gran Alan Turing[15], construyeron versiones primitivas para el descifrado de los mensajes en alemán codificados por Enigma y Lorenz.[16] En EE. UU., la empresa IBM construyó, bajo la dirección de su primer consejero delegado, Thomas J Watson, grandes cantidades de equipos de tratamiento de datos para el ejército y comenzó a experimentar con computadoras analógicas[17] y los alemanes las usaron para calcular la trayectoria de misiles cohete V2.[18]

La necesidad de proteger los derechos humanos y las libertades en una democracia en relación con el

[10] p.e., ECtHR, Dudgeon v. el Reino Unido, sentencia del [AÑADIR FECHA]
[11] p.e., ECtHR, de Hannover v. Alemania, sentencia del [AÑADIR FECHA]
[12] p.e., ECtHR, Halford v. el Reino Unido, sentencia del 25 de junio de 1997
[13] Factsheet – Personal Data Protection, 2018, del Consejo de Europa, disponible en:
https://www.echr.coe.int/Documents/FS_Data_ENG.pdf
Una lista no exhaustiva de casos del Tribunal Europeo de Derechos Humanos relacionados con la protección de datos personales está disponible en:
https://www.coe.int/en/web/data-protection/echr-case-law
Para un debate más general, véase Lee A Bygrave, Protección de datos de conformidad con el derecho a la privacidad en los tratados de derechos humanos, International Journal of Law and Information Technology, 1998, volumen 6, páginas 247 a 284, disponible en:
https://www.uio.no/studier/emner/jus/jus/JUR5630/v11/undervisningsmateriale/Human_rights.pdf
[14] Véase Hondius, o.c. (nota 7, anterior) p. 107, con referencia al Informe de la Comisión de Expertos.
de Derechos Humanos, Consejo de Europa (DH / EXP (70)15).
[15] Véase http://www.maths.manchester.ac.uk/about-us/history/alan-turing/
[16] Véase: Chris Smith, Descifrando el código Enigma: Cómo la Bomba de Turing cambió el rumbo de la Segunda Guerra Mundial, 2 de noviembre de 2017, disponible en:
http://home.bt.com/tech-gadgets/cracking-the-enigma-code-how-turings-bombe-turned-the-tide-of-wwii-11363990654704
La máquina Colossus utilizada para decodificar los mensajes de Lorenz es considerada generalmente como "la primera computadora programable, electrónica, digital". Véase:
https://en.wikipedia.org/wiki/Colossus_computer
[17] Véase: https://en.wikipedia.org/wiki/Thomas_J._Watson
[18] Véase: La computadora analógica totalmente electrónica de Helmut Hoelzer utilizada en los cohetes V2 (A4) alemanes (mayoritariamente en alemán), disponible en:
http://www.cdvandt.org/Hoelzer%20V4.pdf

tratamiento automatizado de datos personales surgió más tarde cuando, en la década de 1960, los ordenadores comenzaron a utilizarse con fines de gestión en los sectores público y privado. Pero debido al alto coste de los ordenadores y el gran espacio que requerían en ese momento, esto solo se hizo en los países desarrollados, e incluso allí solo para las autoridades públicas y las grandes empresas. En un primer momento, los ordenadores se utilizaban para el pago de salarios y a los proveedores, para el registro de los pacientes en los hospitales, para el censo público y las estadísticas, así como para los archivos policiales.

A la luz de estos acontecimientos, a **finales de la década de 1960/principios de la década de 1970**, los mismos debates comenzaron a tener lugar en Alemania (en particular, en el Land of Hesse, sobre archivos policiales), Noruega, Suecia y Francia (particularmente debido a los recuerdos de los abusos a la población y otros registros públicos por parte de los ocupantes nazis durante la Segunda Guerra Mundial), el Reino Unido, los EE. UU., etc., y en la OCDE y el Consejo de Europa.[19] Al principio esos debates se llevaron a cabo entre profesionales sujetos a obligaciones éticas (en los EE. UU., en particular entre los médicos e ingenieros informáticos, que fueron los primeros en producir directrices sobre "Prácticas de información justas")[20] y entre los políticos que estaban preocupados por los riesgos por abuso o uso indebido o seguridad de los datos personales tratados de manera automática.

Luego, a **mediados y finales de los 70 y principios de los 80**, se extendió a poblaciones más amplias: en Francia, uno de los principales catalizadores fue la exposición de los denunciantes en 1974 de los planes gubernamentales de crear una base de datos nacional de todos los ciudadanos y residentes franceses con un número de identificación único para cada uno de ellos; y de la existencia de archivos policiales polémicos-.[21] En Alemania, hubo una oposición generalizada, en un clima político generalmente tenso, al censo nacional propuesto de 1983.[22] Esos debates no trataban solo sobre el riesgo de violación de la privacidad posibilitado por el uso de nuevas tecnologías, sino también sobre las consecuencias de los errores de datos y sobre el posible poder autoritario creado al centralizar los datos recopilados para diferentes propósitos y/o usar identificadores únicos para la interconexión de archivos. En Europa, generaron una demanda de "protección de datos" o “informática y libertades” específica y respaldada por la ley, reforzada por un mayor reconocimiento de esta necesidad por los tribunales constitucionales y otros tribunales superiores, y por la adopción de instrumentos internacionales (como se analiza en la sección 1.2 a continuación).

> El término "protección de datos" (en alemán: ***Datenschutz***) se acuñó originalmente en el título de la primera ley sobre el tema, la Ley de protección de datos de 1970 (Datenschutzgesetz) del Estado alemán de Hesse, redactada por "el padre de la protección de datos", Prof. Spiros Simitis.[23] Como señala Burkert, el título era en realidad "un nombre inapropiado, ya que [la Ley] no protegía los datos, sino los derechos de las personas cuyos datos [se estaban manejando]".[24]

---

[19] El Consejo de Europa adoptó sus primeras resoluciones sobre estos temas en 1973 y 1974: Resoluciones del Consejo de Ministros (73) 22 y (74) 29 (para enlaces, véanse las notas 39 y 40, más abajo). Véase el Memorándum Explicativo al Convenio Europeo de Protección de Datos, parra. 6, disponible en:
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434
Los principios Contenidos en dichas resoluciones están incluidos en el Anexo 1 de este Manual.

[20] Véase: Fair Information Practices: A basic history , disponible en
https://bobgellman.com/rg-docs/rg-FIPshistory.pdf
Gellman trabajó durante muchos años, desde la década de los 70 hasta los 90, sobre materias legislativas de privacidad de los Estados Unidos en la Cámara de Representantes

[21] Véase el artículo en el diario Le Monde del 21 de marzo de 1974, ”SAFARI ou la chasse aux Français” (“SAFARI o la caza de los franceses”), disponible en:
http://rewriting.net/2008/02/11/safari-ou-la-chasse-aux-francais/
El nombre de la vase da datos, SAFARI, era un acrónimo de “système automatisé pour les fichiers administratifs et le répertoire des individus”, pero también se eligió porque al ministro encargado del proyecto le encantaba ir de safari en África. La revelación encontró cobertura en todos los diarios al día siguiente, y el gobierno paró el proyecto unos días después, nombrando una comisión ad hoc para estudiar el problema y proponer soluciones legales.

[22] Véase: Marcel Berlinghoff, Zensus y Boykott. Die Volkszählung vor 30 Jahren, („El censo de lo9s años 30“) en: Zeitgeschichte-online, junio 2013, disponible en:
https://zeitgeschichte-online.de/kommentar/zensus-und-boykott-die-volkszaehlung-vor-30-jahren

[23] Hessisches Datenschutzgesetz (HDSG) (Ley de Protección de Datos del Land de Hesse) 1970, en vigor desde el 13 de octubre de 1970, B.O.E. del Land, Parte I, 1970, Nr. 41 (12 de octubre de 1970), p. 625ff, texto original (en alemán) disponible en:
http://starweb.Hesse.de/cache/GVBL/1970/00041.pdf

[24] Herbert Burkert, Privacy-Data Protection: A German/European Perspective (Protección de la Privacidad de los Datos) (sin fecha, aprox. del año 2000), p. 46, disponible en:
http://www.coll.mpg.de/sites/www/files/text/burkert.pdf

Pero se mantuvo: el término - ahora famoso y célebre en todo el mundo (los franceses ahora también se refieren a la ***protection des données***) - es la abreviatura de "la protección de los individuos con respecto al tratamiento de datos personales" (la larga frase utilizada en los títulos tanto de la Directiva de Protección de Datos de la CE 1995 como del Reglamento General de Protección de Datos de la UE de 2016).[25] Pero incluso esta frase más completa no aclara el significado del concepto a los ojos y para la mente europea.

La protección de datos tiene tanto aspectos de libertad individual como societaria.

Por lo tanto, en Francia, (donde la ley utiliza la expresión "informática, archivos y libertades*"/"informatique, fichiers et libertés")* la protección de datos se considera parte de los requisitos dobles individuales y sociales y constitucionales que:

> **La informática tiene que estar al servicio de cada ciudadano. ... No puede poner en peligro la identidad humana, los derechos humanos, la vida privada o las libertades individuales o públicas[26]**
>
> (Art. 1 de la Ley de Informática, Archivos y Libertades de 1978)

Esta ley francesa adquirió carácter constitucional, y los altos tribunales del país basan sus decisiones en la privacidad o la libertad, en función de los asuntos que se tratan.

En Alemania, la protección de datos se considera principalmente como derivada del (proto-) derecho fundamental al "[respeto por] la personalidad humana" (*das allgemeine Persönlichkeitsrecht*), garantizado por el art. 2 (1) de la Constitución, leído junto con el art. 1 (1). A partir de esto, el Tribunal Constitucional, en su famosa sentencia del Censo de 1983, derivó un derecho más específico a la "**autodeterminación informacional**" (*informationelle Selbstbestimmung*).[27] Sin embargo, el Bundesverfassungsgericht (Tribunal Constitucional Federal) todavía vincula clara y fuertemente este derecho individual a normas sociales más amplias y fundamentales:[28]

> Un orden social y legal en el que el ciudadano ya no puede saber quién sabe qué, y cuándo, sobre él y en qué situación es incompatible con el derecho a la autodeterminación informativa. Una persona que se pregunta si un comportamiento inusual se observa cada vez y luego siempre se mantiene registrado, usado o diseminado, tratará de no llamar la atención de esta manera.
>
> Una persona que asume, por ejemplo, que la participación en una reunión o iniciativa ciudadana se registra oficialmente, y puede crear riesgos para él, puede decidir no ejercer los derechos fundamentales pertinentes ([como se garantiza en] los Artículos 8 y de la Constitución). Esto no solo limitaría las posibilidades de desarrollo personal del individuo, sino también el bien común, porque la autodeterminación es un requisito previo esencial para una sociedad libre y democrática que se base en la capacidad y solidaridad de sus ciudadanos.

Otros estados europeos, si bien aceptan la necesidad de protección de datos y, de hecho, a menudo lo consagran en sus constituciones como un derecho sui generis,[29] no todos han adoptado el concepto alemán de autodeterminación informativa, a menudo precisamente porque sienten que pone demasiado énfasis en el aspecto de la libertad individual y no lo suficiente en los más amplios de la sociedad.[30]

---

[25] El RGPD emplea el término "personas naturales" en lugar de "individuos".

[26] L'informatique doit être au service de chaque citoyen. ... Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques." La frase omitida estipula que he "[La protección de datos] debe desarrollarse dentro del marco de la cooperación internacional".

[27] BVerfG, 15.12.1983, BVerfGE Bd. 65, S. 1 et seq... Sobre el concepto de la "autodeterminación informativa, véase § 151 et seq.

[28] Ídem, § 154 (traducción nuestra).

[29] Cons. la ley australiana de protección de datos de 1978, que contiene una clausula "constitucional" en su art. 1º declarando que la protección de datos es un derecho protegido por la constitución. La protección de datos también está prevista expresamente en las constituciones de países que se convirtieron en democracias en esta época, como España (Art. 18-4), Portugal (Art. 35), Grecia (Art. 9A), Hungría (Art. 59), Lituania (Art. 22), Eslovenia (Art. 38), Eslovaquia (Art. 19), o países que modificaron su constitución para reflejar la sociedad moderna, como Países Bajos (Art. 10).

[30] Véase, p.e., el blog Informationelle Selbstbestimmung - (noch) kein neues Grundrecht, 26 de octubre de 2017, sobre el rechazo de la cámara baja del Parlamento Federal Suizo (Nationalrat) para consagrar el principio de autodeterminación informativa en la Constitución

Aun así, básicamente, en Europa todos coinciden en que, como Hondius ya lo expuso en 1983:[31]

> La protección de datos tiene como objetivo salvaguardar un equilibrio justo y razonable entre los intereses de los individuos y los de la comunidad [en relación con el tratamiento de datos personales].

Los Estados europeos consideraron que, para alcanzar este equilibrio, se apliquen los siguientes **principios reguladores**:

- la recopilación y posterior uso y divulgación de datos personales deben estar sujetos a **la ley** (es decir, a las **normas jurídicas vinculantes**, en lugar de códigos voluntarios o directrices no vinculantes);[32]

- esas **leyes deben ser "generales"** (ómnibus) que, en principio, se aplican a todas las entidades públicas y privadas que procesan datos personales (con excepciones y modificaciones de las reglas y principios previstos en normas especiales cuando sea necesario, pero siempre respetando su "núcleo esencial");

- la ley en cuestión debe contener ciertas **normas sustantivas básicas** (que reflejen los principios "básicos" de protección de datos discutidos en el próximo título) y otorgar a los interesados **derechos humanos fundamentales**; y

- la aplicación de esas leyes debe ser supervisada por **órganos especiales de supervisión** (generalmente denominadas **agencias de protección de datos o APD**).

1.2 Las primeras leyes de protección de datos, principios e instrumentos internacionales [33]

1.2.1 Las primeras leyes de protección de datos

"Europa Occidental es la cuna de la protección"[34]

Como ya se mencionó, la primera ley de protección de datos en el mundo fue la ***Datenschutzgesetz*** (Ley de Protección de Datos) del Estado alemán de Hesse, adoptada en septiembre de 1970.[35] Esa ley también introdujo la primera autoridad independiente de protección de datos (aunque, debido a cuestiones de competencia estatal, solo para el sector público) y con poderes limitados de mediación en lugar de aplicación).

Federal Suiza:
https://www.humanrights.ch/de/menschenrechte-schweiz/inneres/person/datenschutz/informationelle-selbstbestimmung
En los Países Bajos, el principio no ha sido adoptado por las leyes o los tribunales – aunque el Tribunal Supremo, el Hoge Raad, se ha visto influido por la jurisprudencia del Tribunal Constitucional alemán. Véase: T. F. M. Hooghiemstra, Tekst en toelichting Wet bescherming persoonsgegevens (2001), Sección 4.3 (p. 18).

[31] Hondius, o.c. (nota 7, véase más arriba), p. 108.

[32] Cons. La interpretación del concepto "ley" en el Convenio Europeo de Derechos Humanos (en particular Artículo 8 – 11), por el Tribunal Europeo de Derechos Humanos.

[33] Para los Detalles históricos, con referencia especial al borrador en paralelo de las Guías de la OCDE de 1980 y el Convenio de Protección de Datos del Consejo de Europa de 1981 y a las diferencias de los puntos de que ya entonces aparecieron entre Europa y los Estados Unidos. Véase: Frits Hondius, o.c. (nota 7, véase más arriba), pp. 103 – 128, y el Memorándum Explicativo al Convenio de Protección de Datos del Consejo de Europa, o.c. (nota 19, véase más arriba), párrafo 14. Un resumen general muy útil del desarrollo histórico de la privacidad lo proporciona el Cap. 4 del Marco de Privacidad actualizado de la OCDE, titulado "The evolving privacy landscape: 30 years after the OECD Privacy Guidelines" (El cambiante terreno de la privacidad: 30 años después de las Guías de Privacidad de la OCDE, debatido con más detalle más abajo (véase la nota 40). Un fascinante recuento de los antecedentes del borrador de las Guías de la OCDE y la políticas (Europa vs. Estados Unidos), y las personalidades implicadas (incluidos Frits Hondius, Louis Joinet, Stefano Rodota y Spiros Simitis) lo proporciona Michael Kirby en Privacy Today: Something Old, Something New, Something Borrowed, Something Blue (La privacidad hoy: Algo viejo, algo nuevo, algo prestado, algo melancólico) Journal of Law, Information and Science, 2017 25(1), disponible en : http://www.austlii.edu.au/au/journals/JILawInfoSci/2017/1.html

[34] Hondius, o.c. (nota 7, véase más arriba), p. 104, con referencia a las primeras leyes apuntadas en el texto.

[35] Véase la nota 23 más arriba. Para más referencias sobre la historia de la protección de datos en Alemania, véase: Herbert Burkert, o.c. (nota 24, véase más arriba).

La ley de protección de datos de Hesse fue seguida en Europa en esa década, mediante la adopción de leyes nacionales (a nivel nacional) de protección de datos en **Suecia (1973),** la primera **ley alemana de protección de datos (finales de 1977)** (que cubría el tratamiento de datos personales) por las agencias federales y por el sector privado), la **Ley Francesa de Informática, archivos y Libertades** del 6 de enero de 1978, las leyes en **Austria, Dinamarca[36] y Noruega** (todas ellas de 1978) y Luxemburgo (1979). Aunque algunas de estas leyes, como la Ley Federal alemana, contenían conjuntos de reglas separadas para los sectores federal público - y privado, todavía eran leyes "generales" (ómnibus), porque las reglas para ambos sectores se basaban en los mismos principios básicos y derechos, a menudo derivados de la constitución.[37]

1.2.2 Los principios básicos

Las leyes de la década 1970 en Europa se unieron en torno a un **conjunto de principios y derechos "centrales"** cada vez más aceptados (en general). Eran similares a los principios básicos de *Fair Information Practices* redactados aproximadamente al mismo tiempo en los Estados Unidos (aunque estos eran menos detallados y no se establecían en una ley vinculante).[38]

Estos principios básicos de las leyes tempranas en Europa se reflejaron a su vez **en los instrumentos europeos más antiguos (no vinculantes)** sobre el tema, emitidos por el Consejo de Europa (y que a su vez se convirtieron en la base de los últimos datos vinculantes del Convenio de Protección del Consejo de Europa):

- Resolución del Consejo de Europa de 1973 (73)22 sobre Protección de la privacidad de las personas frente a los bancos de datos electrónicos en el sector privado, adoptada por el Comité de Ministros el 26 de septiembre de 1973;[39]

- Resolución del Consejo de Europa de 1974 (74)29 sobre Protección de la privacidad de las personas frente a los bancos de datos electrónicos en el sector público, adoptada por el Comité de Ministros el 20 de septiembre de 1974[40].

Los principios "centrales" se reconocieron a continuación en los **instrumentos mundiales, pero aún no vinculantes**, es decir:

- las Directrices de 1980 sobre la Protección de la privacidad y los flujos transfronterizos de datos personales de la OCDE;[41] y

- las Directrices para la regulación de los archivos informatizados de datos personales de 1989 de las Naciones Unidas, adoptadas por la Asamblea General de las Naciones Unidas (AGNU).[42]

El texto completo con los principios básicos de los cuatro instrumentos internacionales no vinculantes anteriores de los años 70 y 80, y los principios de las Prácticas justas de información de los Estados

[36] En Dinamarca hubo uncialmente dos leyes, una para el sector privado y otra para el sector público, adoptadas el mismo día (Leyes nº. 293 y 294, ambas del 8 de junio de 1978), pero ambas basadas en los mismos principios más amplios. Para los antecedentes, véase la introducción en Peter Blume, Personregistrering, Copenhague, 1991.Ambas estuvieron en vigor, con varias modificaciones, hasta el año 2000, cuando se introdujo una nueva legislación para implantar la Directiva de Protección de Datos de la CE de 1995.
[37] Las leyes estatales de protección de datos (Landesdatenschutzgesetze) cubren los sectores públicos estatales, pero se basan en los mismos principios, arraigados en la Constitución.
[38] Véase la sub-sección 1.3.4, más abajo.
[39] Disponible: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680502830
[40] Disponible en: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d1c51
[41] OCDE, Recomendaciones del Consejo acerca de las Guías que rigen la Protección de la Privacidad y el flujo transfronterizo de datos personales, de 23 de septiembre de 1989, disponible en: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonal data.htm. Para los antecedentes, véase Kirby, o.c. (nota 33, véase más arriba). Nótese que las Guías de la OCDE fueron revisadas en 2013 en el contexto de la creación de un Marco de la Privacidad de la OCDE más amplio que incluye nuevas reglas sobre cooperación para la aplicación de la privacidad, que se basaba en una recomendación del 2007 sobre este mismo asunto. Véase: https://www.oecd.org/sti/ieconomy/privacy.htm Pero esto no afecta a los principios básicos de 1980.
[42] Naciones Unidas, Guía para la regulación de los ficheros informatizados de datos personales, UNGA Res. 44/132, 44 UN GAOR Supp. (Nº. 49) en 211, UN Doc. A/44/49 (1989), disponible en: https://www1.umn.edu/humanrts/instree/q2grcpd.htm
Nótese que este es el primer instrumento en reconocer la necesidad de agencias de protección de datos independientes.

Unidos de 1973 se reproduce en los enlaces de las notas a pie de página.

Aquí bastará con señalar que su objetivo es abordar el problema inherente a los ordenadores: debido a su naturaleza facilitan nuevas y diversas formas de utilizar los datos, incluidos los datos personales, sin que las restricciones de seguridad y uso sean un aspecto propio de su especificidad. En otras palabras: los principios básicos buscan evitar el uso fraudulento de datos personales que facilitan las nuevas tecnologías si no se controlan. En este sentido, siguen siendo relevantes.

Tal como se expone de forma concisa en las Directrices de la OCDE.

Principios de 1980 de la OCDE

Principio de limitación de la recogida de datos

Deben existir límites para la recopilación de datos personales y dichos datos deben obtenerse por medios legales y justos y, cuando corresponda, con el conocimiento o consentimiento del interesado.

Principio de calidad de los datos

Los datos personales deben ser relevantes para los fines para los que se utilizarán y, en la medida necesaria para esos fines, deben ser precisos, completos y mantenerse actualizados.

Principio de finalidad

Los fines para los cuales se recopilan datos personales deben especificarse a más tardar en el momento de la recopilación de datos y el uso posterior se limita al cumplimiento de esos fines u otros que no son incompatibles con esos fines y que se especifican en cada ocasión de cambio de propósito.

Principio de la Limitación de Uso
Los datos personales no deben divulgarse, ponerse a disposición o usarse de otro modo para fines distintos a los especificados de acuerdo con [el principio anterior], excepto:

a. con el consentimiento del sujeto titular de los datos; o
b. por imperativo legal

Principio de salvaguarda de la seguridad
Los datos personales deben estar protegidos por medidas de seguridad razonables contra riesgos tales como la pérdida o el acceso no autorizado, destrucción, uso, modificación o divulgación de datos.

Principio de apertura
Debe haber una política general de apertura sobre desarrollos, prácticas y políticas con respecto a los datos personales. Deben estar disponibles medios para establecer la existencia y naturaleza de los datos personales, y los principales propósitos de su uso, así como la identidad y residencia habitual del controlador de datos.

Principio de Participación Individual
El individuo tiene que tener el derecho a:

a) obtener del responsable de los datos, o de otro modo, confirmación de si el responsable de datos tiene o no datos relacionados con él;
b) que se le comuniquen los datos relacionados con él dentro de un tiempo razonable; que la cantidad de datos recogidos no sea excesiva; en una manera razonable e inteligible para él;
c) que se le den razones si se rechaza una solicitud hecha bajo los subpárrafos (a) y (b), y para poder impugnar dicha denegación; y
d) poner en cuestión los datos relacionados con él y, si la impugnación tiene éxito, borrar, rectificar, completar o enmendar los datos.

Principio de Responsabilidad
Un controlador de datos debe ser responsable de cumplir con las medidas que dan efecto a los principios establecidos anteriormente.

Es importante subrayar que los principios (en todos los instrumentos) siempre deben leerse y aplicarse conjuntamente: solo así pueden brindar una protección seria contra abusos o usos indebidos de datos personales, como errores en datos digitalizados o almacenados, recogida de más datos de los necesarios o mantenerlos durante más tiempo de lo necesario, utilizando datos para fines diferentes a los declarados, el robo o la divulgación de datos a otros con fines ilegales, pérdidas de datos, piratería informática, etc., etc.

1.2.3 El Convenio del Consejo de Europa sobre Protección de Datos de 1981 y su Protocolo Adicional

El primer instrumento internacional vinculante en el campo de la protección de datos fue el Convenio del Consejo de Europa de 1981 para la Protección de las Personas con respecto al Tratamiento Automático de Datos Personales, más conocido como el Convenio de Protección de Datos (CPD) o "Convenio Nº 108" según su número dentro de la serie de tratados europeos.[43]

Como Convenio del Consejo de Europa (en lugar de un "Convenio Europeo"), el Convenio de Protección de Datos también puede ser ratificada por Estados que no son miembros del Consejo de Europa, por invitación (Artículo 23). Hasta la fecha (agosto de 2018), el Convenio ha sido ratificado por los 47 Estados miembros del Consejo de Europa y por seis países no europeos (Uruguay [2013], Mauricio [2016], Senegal [2016], Túnez [2017], Cabo Verde y México [2018])[44]. Se ha invitado a otros dos Estados no europeos a adherirse al Convenio: Argentina y Burkina Faso.[45] En 2001, el Convenio fue complementado por un Protocolo Adicional.[46]

El Convenio de 1981 y ese Protocolo adicional se describen brevemente a continuación en tiempo pasado porque, más recientemente, en 2018, se modificaron de manera más fundamental ("modernizaron") en un protocolo adicional, como se analiza en la sección 1.3 a continuación. Sin embargo, cabe destacar que el Convenio revisado ("modernizado") solo se aplicará a los Estados partes que se adhieran a él: para los demás, el texto de 1981 sigue siendo el aplicable (léase con el Protocolo adicional de 2001 según corresponda).

Como instrumento internacional vinculante, el Convenio de 1981 (a diferencia de los anteriores instrumentos no vinculantes) tenía que incluir **definiciones** jurídicas más precisas de los principales conceptos en la ley de protección de datos: "**datos personales**", "**controlador**", "**instrumento**" y "**tratamiento**" (aunque en los últimos instrumentos vinculantes fue necesaria una ampliación y se agregaron) (Art. 2).

Los principales principios de protección de datos expuestos anteriormente - **Principio de Limitación de Recogida, Principio de Calidad de Datos, Principio de Especificación de Propósitos y Principio de Limitación de Uso** - se establecieron en el Artículo 5 del Convenio de 1981 (sin utilizar esos términos: el Convenio enumera estos principios juntos bajo encabezado "Calidad de los datos"). El **Principio de seguridad de los datos** (al que se hace referencia en el Convenio como el Principio de salvaguardia de la seguridad) se detalla en el Artículo 7; y los **principios de apertura y participación individual** se establecieron en el artículo 8 (bajo el título "*Salvaguardias adicionales para el interesado*")[47].

El Convenio añadió a estos un artículo especial sobre el tratamiento de "**categorías especiales de datos**", es decir, "*datos personales que revelan origen racial, opiniones políticas o creencias religiosas o de otro tipo, así como datos personales relativos a la salud o la vida sexual*" y "*datos personales relacionados con condenas penales*" (Art. 6). Se estipuló que dichos datos, comúnmente denominados "*datos confidenciales*", "no se tratarán automáticamente a menos que la legislación nacional establezca garantías adecuadas".

NB: La necesidad de reglas especiales sobre ciertos tipos de datos se debatió acaloradamente en su momento. Algunos, incluido Simitis, consideraron que cualquier dato podría ser sensible, dependiendo del contexto, mientras que algunos de los datos enumerados podrían ser inocuos en otros contextos. Otros consideraron que solo se debían regular los datos confidenciales, ya que eran intrínsecamente peligrosos y podían conducir a la discriminación. Al final, prevaleció la propuesta hecha por Louis Joinet, representante francés y presidente del

[43] Título completo: Consejo de Europa, Convenio para la Protección de las Personas en Relación al Procesado Automático de Datos, abierto para su firma en Estrasburgo el 28 de enero de 1981, CETS Nº 108, disponible en: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37

[44] Véase: https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/108/signatures?p_auth=qsJbzlEi

[45] Ídem

[46] Título completo: Consejo de Europa, Protocolo Adicional al Convenio para la protección de las personas con respecto al procesado automático de datos personales en relación con las autoridades de supervisión y los flujos de datos transfronterizos, abierto para su firma en Estrasburgo el 8 de noviembre de 2001, CETS No. 181, disponible en: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680080626
El Protocolo Adicional ha sido ratificado por 36 de los 47 estados miembro del Consejo, y por seis estados que no son miembros (Cabo Verde, Mauricio, México, Senegal, Túnez y Uruguay). Burkina Faso ha sido invitada a unirse. Véase: https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/181/signatures?p_auth=yDDCP83k

[47] Debido a que la aplicación de los principios básicos constituye la salvaguarda principal de los individuos: los derechos de los interesados son complementarios a esos, porque permiten un mayor control por parte del individuo, en casos individuales.

comité del Consejo de Europa encargado de la redacción[48], y todos los datos personales fueron regulados, con un mayor nivel de protección para esos datos confidenciales.

Al mismo tiempo, el Convenio permitió a los Estados-Partes adoptar **excepciones y restricciones** a la mayoría de los requisitos del Convenio (pero no a los requisitos de seguridad de datos) para proteger "*la seguridad del estado, la seguridad pública, los intereses monetarios del estado o la supresión de los delitos*" o "*" "afectado" o los derechos y libertades de los demás*", siempre que la excepción esté "prevista por la legislación de la Parte "y" constituya una medida **necesaria** [y proporcionada] en una sociedad democrática" para proteger esos intereses (Art. 9 (2)).[49]

Además de dar efecto legal a los principios básicos de protección de datos (con la adición de reglas especiales sobre datos confidenciales) y derechos de los interesados, el Convenio de 1981 también confirmó dos de los otros **requisitos reglamentarios** europeos mencionados anteriormente:

- Exigía que los Estados-partes aplicaran sus disposiciones en las normas jurídicas vinculantes. Estos podrían adoptar la forma de leyes, reglamentos o disposiciones administrativas, y podrían complementarse con directrices o códigos no vinculantes, pero las principales normas debían adoptar la forma de "medidas vinculantes".[50]
- Exigía que los estados parte aplicaran sus leyes ampliamente, **a (todos) los "archivos automáticos de datos personales y el tratamiento automático de datos personales en los sectores público y privado**" (artículo 3(1)). En otras palabras, al menos en principio, requería la adopción de **leyes generales ("ómnibus").[51]**

Sin embargo, el Convenio de 1981 aún no exigía que los Estados-partes establecieran una **agencia independiente de protección de datos**. Tampoco abordaba aún un problema que pronto se convirtió en importante a la luz de los flujos de datos transfronterizos cada vez más frecuentes: la **necesidad de restringir la búsqueda de flujos transfronterizos** para evitar las reglas sustantivas y las negaciones de los derechos cruciales de los interesados, al imponer el territorio de un estado con leyes de protección de datos adecuadas.

Por el contrario, el Convenio de 1981 estipulaba que los Estados-partes deberían:

> no deberá, con el único propósito de proteger la privacidad, prohibir o estar sujeto a autorización especial los flujos transfronterizos de datos personales que vayan al territorio de cualquier otra Parte (artículo 12(2)) - a menos que el Estado-parte en cuestión haya adoptado las reglas estrictas para la categoría de datos relevante, o que la transferencia al otro Estado-parte se hubiera hecho con la intención de eludir la ley en el primer Estado-parte (Art. 12(3)).

En otras palabras, el Convenio de 1981 aún no se ocupó de la cuestión de los datos personales que llegan a los Estados que no son partes en el Convenio.

Finalmente, cabe señalar que el Convenio solo se aplicaba a "archivos de datos personales automatizados y tratamiento automático de datos personales" (artículo 3(1), véase también el artículo 1). En otras palabras, los **archivos manuales**, incluidos los "archivos manuales estructurados", aún no estaban sujetos a sus disposiciones (aunque los Estados-Partes podrían optar por extender la aplicación del Convenio a dichos archivos: artículo 3 (2) (c)).

Dos de los defectos fueron corregidos en el Protocolo Adicional sobre autoridades de supervisión y

[48] Louis Joinet fue, hasta su jubilación, un juez francés que fue miembro de una comisión ad hoc para redactor el anteproyecto de la ley francesa de protección de datos de 1978 antes de convertirse en el primer redactor de la agencia francesa de protección de datos (CNIL). Se convirtió en un reputado representante francés en el Comité de Derechos Humanos de las Naciones Unidas, y como tal se encargó de redactar las Guías de las Naciones Unidas (nota 42, véase más arriba). Véase: https://fr.wikipedia.org/wiki/Louis_Joinet http://www.liberation.fr/societe/2013/12/18/louis-joinet-le-hessel-de-la-justice_967496

[49] En la legislación del TEDH, el requisito de proporcionalidad se entiende dentro del requisito de necesidad estipulado expresamente (en una sociedad democrática), mientras que en la legislación de la UE, en concreto en Carta de los Derechos Fundamentlaes de la Unión Europea, los dos conceptos se tratan como principios independientes (aunque muy estrechamente relacionados):*cf*. Art. 52 CFR.

[50] Memorandum Explicativo del Convenio del Consejo de Europa, o.c. (nota 19, véase más arriba), párrafo. 39.

[51] Esto está sujeto a la estipulación de que cualquier Estado parte puede declarar "que no aplicará esta convención a ciertas categorías de archivos de datos personales automatizados" (Art. 3(2) (a)).

flujos de datos transfronterizos, adoptado en 2001 (ya mencionado),[52] el cual, como el título indica, requiere el establecimiento de APD **independientes con poderes de investigación e intervención, y llevar procedimientos legales** (artículo 1) y la imposición de una **prohibición en principio de la transferencia de datos personales a un país que no garantiza un "nivel adecuado de protección"** (artículo 2). El Protocolo Adicional se adoptó principalmente para acercar el régimen del Convenio al régimen de la vigente Directiva de Protección de Datos de la CE de 1995, que se trata en el punto en 1.3 a continuación.

Muy recientemente, en mayo de 2018, el Convenio de 1981 fue "**modernizado**" aún más, para alinearlo con la legislación más reciente de protección de datos de la UE y la evolución general (global) de la protección de datos, como se expone en el punto 1.4.3 a continuación.

Dentro del Consejo de Europa, los asuntos de protección de datos son abordados por una serie de órganos, incluida la Asamblea Parlamentaria del Consejo de Europa (APCE), un Comité Consultivo, conocido como "T-PD", establecido por el Convenio núm. 108, que tiene una gran responsabilidad en la supervisión diaria de la evolución de la protección de datos y en la elaboración de proyectos de directrices y recomendaciones sectoriales y de otro tipo en este ámbito, y del Comité de Ministros del Consejo de Europa (COM o CM), que adopta en particular esas propuestas. Entre ellos, emitieron muchas opiniones, recomendaciones y estudios en el área, siempre con referencia al Convenio.[53]

Además, existe una interacción entre el Convenio de Protección de Datos y el Convenio Europeo de Derechos Humanos, y el Tribunal Europeo de Derechos Humanos toma nota cada vez más del Convenio sobre Protección de Datos y los tipos de documentos mencionados anteriormente en su propia interpretación del Artículo 8 del Convenio de Derechos Humanos (que garantiza el derecho a la vida privada); mientras que APCE, el Comité Consultivo y el Comité de Ministros a su vez recurren a la jurisprudencia de la Corte en su trabajo en esta área.[54]

1.3 La legislación de la Unión Europea en materia de protección de datos en los 90 y los primeros años del 2000

1.3.1 Protección de datos en la Unión Europea

Antecedentes

Durante algún tiempo, la Comunidad Europea (como se llamó entonces la UE)[55] pensó que el Convenio de Protección de Datos del Consejo de Europa de 1981 otorgaba suficiente protección en este campo. Sin embargo, a finales de ese decenio quedó claro que el Convenio no había dado lugar a una protección amplia o armonizada, en general, de los datos personales en la Comunidad: para septiembre de 1990, solo había sido ratificada por siete Estados miembros de la CE (aún no había adoptado la legislación pertinente), y las leyes en esos Estados miembros diferían considerablemente en aspectos importantes.[56] En ese momento, Italia solo

[52] Véase nota 46, véase más arriba.
[53] Véase:
http://website-APCE.net/en_GB/web/apce/documents (documentos APCE) Nótese que estos cubren muchos más asuntos que solamente la protección de datos – pero pueden buscarse bajo el término "protección de datos"
https://www.coe.int/t/dghl/standardsetting/dataprotection/Documents_TPD_en.asp (documentos T-PD);
https://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp (documentos COM relativos a protección de datos).
[54] Véase la Factsheet del Consejo de Europa – personal data protection (nota 13, véase más arriba) y Anexo 1 – Jurisprudencia sobre un documento de trabajo del "Working Party sobre el Art. 29" de la UE, Documento de Trabajo 01/2016 sobre la justificación de las interferencias con los derechos fundamentales a la privacidad y la protección de datos mediante medidas de vigilancia a la hora de transferir datos personales (Garantías Básicas Europeas) (WP237), adoptado el 13 de abril de 2016, que relaciona 15 sentencias importantes del ECtHR relevantes para la protección de datos (y otras cinco del CJEU), disponibles en http://ec.europa.eu/justice/Artículo-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf
[55] En el momento de la introducción del juego de propuestas de la Comisión expuesto en esta sección (septiembre de 1990), la Comisión aún era formalmente la "Comisión de las Comunidades Europeas" (en plural). El término "Comunidad Europea" (en singular) solamente se aplicó desde 1992 bajo el Tratado De Maastricht hasta que entró en vigor el Tratado de Lisboa en 2009. No obstante, y en aras a la simplicidad, nos referiremos de manera general a la Comunidad Europea en esta Sección, y a la Unión Europea en el siguiente, Sección 1.4, así como en las Partes Segunda y Tercera.
[56] Comisión de las Comunidades Europeas, Comunicación sobre la protección de las personas en relación con el procesado de datos personales en la Comunidad y la seguridad de la información. COM(90) 314 final – SYN 287 y 288, Bruselas, 13 de septiembre 1990, Introducción. El documento completo está disponible online en el excelente archivo del Centre for Intellectual Property and Information

tenía una ley de protección de datos en relación con los trabajadores, España no tenía una ley general a pesar de que estaba prevista la protección de datos como un derecho fundamental en su Constitución, etc.

Esta diversidad se contrapone al objetivo de la Comunidad Europea en ese momento de armonizar todo tipo de normas y leyes para facilitar la apertura del mercado interno, con la propuesta de libre circulación de bienes, servicios, capital y personas. Más concretamente, durante la conferencia internacional de autoridades de protección de datos de 1989, celebrada en Berlín, la Comisión Europea informó a los representantes reunidos de las agencias de protección de datos de la CE que las normas para el sector de las telecomunicaciones debían armonizarse. Esto demostró que era crucial contar con leyes de protección de datos sólidas y bien aplicadas en todos los Estados miembros.[57]

Como resultado directo de esta iniciativa, al año siguiente, en septiembre de 1990, la Comisión Europea presentó un conjunto de propuestas ambiciosa destinadas a proteger los datos personales del "Primer Pilar" de la CE[58]. El paquete incluía propuestas para dos directivas del P"Primer Pilar", es decir: [59]

- **una directiva general de la CE** "*referida a la protección de las personas en relación con el tratamiento de datos personales*", que después de un prolongado proceso legislativo se convirtió en la principal Directiva de Protección de Datos de la CE, Directiva 95/46/CE, expuesta a continuación, en el punto 1.3.2; y

---

Law de la Universidad de Cambridge, en:
https://resources.law.cam.ac.uk/cipil/travaux/data_protection/3%2013%20September%201990%20Communication.pdf. Véase en particular los párrafos. 6 – 8.

[57] En la conferencia internacional de agencias de protección de datos celebrada en Berlín, Spiros Simitis, Comisario de Protección de Datos para el Estado federado de Hesse (e iniciador de la primera ley de protección de datos en el mundo en ese estado), hizo un llamamiento público a Jacques Fauvet, el entonces presidente de la agencia francesa de protección de datos, la CNIL (y anteriormente el jefe del periódico "Le Monde"), para que escribiese a su gran amigo Jacques Delors, entonces presidente de la Comisión Europea, para tomar una iniciativa que armonizase las leyes de protección de datos dentro de la CE.

[58] El Tratado de la Unión Europea, firmado en Maastricht el 7 de febrero de 1992 (el "Tratado de Maastricht"), preveía una estructura de tres pilares bajo una misma estructura. El primer pilar estaba formado por la Comunidad Económica Europea (CEE), la Comunidad Europea del Carbón y del Acero (CECA) y la Comunidad Europea de la Energía Atómica (CEEA) (aunque cada una de ellas conservaba su propia personalidad jurídica) y posteriormente abarcaba el mercado único creado en 1993. Los pilares segundo y tercero abarcaban, respectivamente, la Política Exterior y de Seguridad Común (PESC) y la cooperación en los ámbitos de la Justicia y los Asuntos de Interior (JAI). Los pilares fueron formalmente abolidos por el Tratado de Lisboa, pero se siguen elaborando instrumentos separados para las distintas áreas (véase el análisis del alcance del GDPR en la segunda parte, sección 2.3, más adelante). Véase el sitio web del centro de investigación CVCE de la Universidad de Luxemburgo sobre los acontecimientos históricos en el proceso de integración europea (1945-2014), en particular la página sobre "El primer pilar de la Unión Europea":
https://www.cvce.eu/en/education/unit-content/-/unit/02bb76df-d066-4c08-a58a-d4686a3e68ff/4ee15c10-5bdf-43b1-9b5f-2553d5a41274
La Directiva de protección de datos de 1995 (y las demás directivas expuestas en la presente sección) se realizan (y se emitieron) todas ellas en el momento en que el Primer Pilar aún estaba en vigor, y se emitieron únicamente para ese pilar. Las medidas de protección de datos en los otros dos pilares se describen brevemente en las subsecciones 1.3.4 y 1.3.5, más adelante, y las normas de protección de datos para las propias instituciones de la UE se examinan brevemente en la subsección 1.3.6.

[59] Comisión de las Comunidades Europeas, Comunicación sobre la protección de personas en relación al procesado de datos personales en la Comunidad y seguridad de la información (nota 56). El paquete contenía otras cuatro propuestas, es decir:
- el borrador de una resolución de los representantes de los Estados Miembros que habría ampliado la aplicación de los principios contenidos en la directiva general a archivos mantenidos por autoridades públicas a los que se aplicaría la Directiva principal sobre Protección de Datos como tal – que nunca se adoptó como tal, pero que puede ser vista como el origen de las reglas de protección de datos relacionados con la aplicación de la ley y asuntos judiciales, que culminaron recientemente con la Directiva de protección de datos para la aplicación de la ley (Directiva (UE) 2016/680) de la que no se habla en este Manual: Véase la nota del recuadro "Acerca de este Manual" en la p. 1, véase más arriba);
- el borrador de una declaración sobre la aplicación de los estándares de protección de datos fijados por la principal Directiva de Protección de Datos a ficheros mantenidos por las instituciones comunitarias mismas – que a la postre conllevó el Reglamento (EC) 45/2001 (ídem);
- una recomendación para una decisión del Consejo sobre la adhesión de la Comunidad Europea al Convenio del Consejo de Europa sobre protección de datos, que hasta la fecha no se ha producido porque la UE, al no ser un Estado miembro, no puede adherirse al Convenio, pero esto se está remediando en el Consejo "Modernizado" de la Convención de Protección de Datos de Europa, discutido a continuación, en 1.4.3; y
- una propuesta de decisión del Consejo sobre la adopción de un plan de acción sobre seguridad de la información, que dio lugar a una amplia acción en este campo por parte de la UE, incluido el establecimiento, en 2004, de la Agencia de la Unión Europea para la Seguridad de las Redes y de la Información, ENISA, y la adopción de una estrategia elaborada de información y seguridad cibernética, que no se analiza más a fondo en este manual, pero se puede encontrar aquí:
https://www.enisa.europa.eu/about-enisa
https://ec.europa.eu/digital-single-market/en/cyber-security
Para las propuestas separadas enumeradas en la Comunicación de la Comisión (y otros documentos relacionados con el proceso legislativo), siga los enlaces en esta página:
https://www.cipil.law.cam.ac.uk/projectseuropean-travaux/data-protection-directive

- una propuesta de **directiva EC adicional** "*sobre la protección de los datos personales en el contexto de las redes públicas de telecomunicaciones digitales, en particular la red digital de servicios integrados (RDSI) y las redes móviles digitales públicas*" que se convirtió en la Directiva de protección de datos de telecomunicaciones, Directiva 97/66/CE, adoptada en diciembre de 1997, reemplazada por la Directiva 2002/58 / CE, la denominada "Directiva sobre privacidad electrónica", que se analiza a continuación, en el punto1.3.3;

Antes de debatir estas dos directivas, es importante tener en cuenta la naturaleza y las limitaciones inherentes de dichos instrumentos.

Naturaleza y limitaciones de las directivas EC

Al debatir sobre los principales instrumentos de protección de datos de la UE, y en particular las dos directivas de protección de datos antes mencionadas deben tenerse en cuenta tres cuestiones. En primer lugar, cualquier instrumento legal de la UE (o previamente: EC) está, por su propia naturaleza, limitado a asuntos dentro del alcance de la legislación de la UE (o anteriormente: EC). Algunas cuestiones, especialmente las actividades de los Estados miembros en relación con la **seguridad nacional** están (casi) totalmente fuera del alcance de la legislación de la UE (o anteriormente: CE)[60] y no de los instrumentos jurídicos de la UE (o de la CE) (incluidas esas directivas o, de hecho, el RGPD mismo, o cualquier futura norma de protección de datos de la UE, en cualquier forma) son por lo tanto aplicables a tales actividades. Esto se reafirma expresamente en las directivas (y el RGPD): véase el artículo 3 (2) de la Directiva de protección de datos de 1995 y el artículo 1 (3) de la Directiva sobre privacidad electrónica (y el artículo 2 (2) (a) del RGPD).[61]

En segundo lugar, las directivas de la CE expuestas a continuación, como directivas de la CE, se limitaron a cuestiones del denominado **Primer Pilar**[62] y, por su propia naturaleza, no se aplican a las actividades del segundo o tercer pilar, para las que se han redactado instrumentos separados de protección de datos que se mencionan brevemente en las secciones 1.3.4 y 1.3.5, pero que no se examinan con mayor detenimiento en esta primera edición del Manual. Baste señalar que cualquier transmisión o puesta a disposición de datos personales por entidades sujetas a las directivas (incluidas tanto entidades del sector privado como organismos públicos que realizan actividades sujetas a la ley del primer pilar (CE)), a cualquier entidad encargada de hacer cumplir la ley o la agencia de seguridad nacional estaba (y en el caso de la Directiva e-Privacy todavía está) sujeta a esos instrumentos (porque tales revelaciones constituían "tratamiento" en términos de esas directivas, por esas entidades), incluso si la obtención (recepción) y más el tratamiento de los datos divulgados estaba sujeto a otros instrumentos (incluida, en relación con la aplicación de la ley en particular, hasta hace poco, la Decisión marco 2008/977 / JAI del Consejo y, ahora, la Directiva de protección de datos de aplicación de la ley de 2016), o no sujetos a La legislación de la UE (o la CE) en absoluto (es decir, si fue realizada por agencias de seguridad nacional).[63]

En tercer lugar, una directiva, por definición, no se aplica directamente en los ordenamientos jurídicos de los Estados miembros: no tiene "efecto directo". Por el contrario, sus disposiciones deben ser "**transpuestas**" a la legislación nacional por los Estados miembros, y para esto, a los Estados miembros se les otorgó (y aún se les concede) discreción considerable. Este fue sin duda el caso en relación con las dos directivas discutidas a continuación, y como se observará en la segunda parte, esto condujo a considerables divergencias entre las legislaciones nacionales de los Estados miembros que aplicaban ("transponían") esas directivas; esa fue, de hecho, una de las principales razones para elegir la forma de un reglamento (directamente aplicable) para el sucesor de la Directiva de Protección de Datos de 1995, el RGPD (aunque, como veremos en esa parte, el

[60] Decimos "(casi) totalmente" por dos razones. En primer lugar, cada vez es más difícil, especialmente en relación con el terrorismo (un concepto bastante mal definido) distinguir las acciones de los Estados en relación con su seguridad nacional de las acciones adoptadas en virtud del derecho penal o el derecho relativo a la protección de la "seguridad internacional", "seguridad pública" u "orden público", todos los cuales son asuntos que, en mayor o menor grado, están ahora al menos parcialmente sujetos a la legislación de la UE. En segundo lugar, incluso si las acciones de los organismos de los Estados miembros responsables de la seguridad nacional están fuera del alcance de la legislación de la UE, las actividades de los organismos encargados de hacer cumplir la ley y las entidades privadas (por ejemplo, la recopilación y divulgación de datos por parte de los bancos en virtud de la legislación sobre lavado de dinero, o y la divulgación de los registros de nombres de los pasajeros por parte de las compañías aéreas a las agencias de los Estados miembros) a menudo están sujetos a la legislación de la UE (en particular, la legislación de protección de datos de la UE). Contras. el segundo punto en el texto.

[61] Sobre las limitaciones en el alcance del RGPD de la UE, véase la segunda parte, Sección2.3, Elementos clave del RGPD, en particular la subsección 2.3.1, Disposiciones Generales.

[62] Véase más abajo la nota a pie de página 67

[63] Sobre las limitaciones en el ámbito del RGPD de la UE, véase la Parte Dos, en particular la Sección 2.2, Situación y enfoque del Reglamento GDPR: armonización con especificaciones de flexibilidad a nivel nacional.

Reglamento todavía permite también una implantación diferente en muchos aspectos.[64]

1.3.2 La principal Directiva de Protección de Datos de la CE de 1995

General

Como se señaló anteriormente, a principios de la década de 1990, la Comisión de las Comunidades Europeas (como entonces se la conocía)[65] se enfrentó a un dilema. Por un lado, la protección de datos se reconoce cada vez más como un derecho protegido por la Constitución de la UE y exige restricciones en el uso y los flujos de datos personales.[66] Por otro lado, el desarrollo del mercado interno, en el llamado " Primer Pilar "de la Comunidad, [67] requirió la libre circulación de datos, incluidos datos personales, relacionados con transacciones comerciales. Para cuadrar este círculo, la Comisión propuso que para este primer pilar se adopten dos directivas. En esta sección, discutiremos la directiva principal, la Directiva 95/46 / EC.[68]

Propósito y finalidad de la Directiva de protección de datos de 1995:

En reconocimiento del dilema anterior, la Comunidad Europea dio a la directiva dos objetivos vinculados, es decir: proporcionar un alto nivel de protección de datos a lo largo del "primer pilar" de la Comunidad ("alto nivel" porque el objetivo de la directiva era proteger los derechos humanos), como condición sine qua non para el libre flujo de datos personales dentro del elemento principal de ese pilar, el mercado interior emergente (véase el artículo 1 de la Directiva y los considerandos 10 y, especialmente, 11).

Características principales de la Directiva de Protección de Datos de 1995:

A continuación se exponen las **características principales** de la Directiva de Protección de Datos de 1995, en comparación con el Convenio de 1981 (Nota: las nuevas características o características que contienen importantes elementos nuevos están marcadas *NUEVO – no obstante, cabe destacar que normalmente se amplían a sugerencias planteadas o propuestas en los considerandos del Convenio). La finalidad de describir estas características principales de la Directiva de 1995 es proporcionar un resumen de algunos componentes fundamentales del enfoque de protección de datos de la UE, que se ha reafirmado totalmente en el Reglamento general de protección de datos y se explican aquí en consecuencia, mientras que las nuevas características introducidas mediante el Reglamento se detallarán en la Parte Dos. Las innovaciones más importantes fueron la exigencia de autoridades independientes de protección de datos y las medidas

[64] Véase Parte Dos, en particular la Sección 2.2, Estado y Enfoque de la armonización del RGPD con flexibilidad.
[65] Véase la nota 54.
[66] La protección de datos ahora se reconoce expresamente como un derecho sui generis en el Artículo 8 de la Carta de los Derechos Fundamentales de la UE (CDF), distinto del derecho a la vida privada y familiar y la privacidad (aunque, por supuesto, está estrechamente relacionado con él), protección por Artículo 7. La CDF solo se proclamó en 2000, pero no obtuvo pleno efecto legal hasta la entrada en vigor del Tratado de Lisboa el 1 de diciembre de 2009. Véase:
https://en.wikipedia.org/wiki/Charter_of_Fundamental_Rights_of_the_European_Union
En otras palabras, la Carta aún no tenía pleno efecto legal en el momento en que se propusieron las directivas. Sin embargo, incluso antes de que se redactara o se diera efecto legal a la Carta, a los derechos fundamentales ya se les otorgó un estatus casi constitucional en las Comunidades Europeas, Véase: Francesca Ferraro y Jesús Carmona, Derechos fundamentales en la Unión Europea - El papel de la Carta después del Tratado de Lisboa. Servicio de Investigación del Parlamento Europeo, Bruselas, marzo de 2015, Sección 2: Derechos fundamentales de la UE antes del Tratado de Lisboa, disponible en:
http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/554168/EPRS_IDA(2015)554168_EN.pdf
Los redactores de la Directiva de Protección de Datos de 1995, por lo tanto, todavía colocaron correctamente la protección de datos personales como un derecho fundamental en la base del instrumento propuesto.
[67] El Tratado de la Unión Europea, firmado en Maastricht el 7 de febrero de 1992 (el "Tratado de Maastricht"), provisto de una estructura de tres pilares bajo un único frontis. El primer pilar estaba formado por la Comunidad Económica Europea (CEE), la Comunidad Europea del Carbón y el Acero (CECA) y la Comunidad Europea de la Energía Atómica (CEEA) originales (aunque cada una conservaba su propia personalidad jurídica). Los Pilares Segundo y Tercero cubrieron, respectivamente, la Política Exterior y de Seguridad Común (PESC) y la cooperación en los campos de Justicia y Asuntos de Interior (JAI). Los pilares fueron formalmente abolidos por el Tratado de Lisboa, pero aún se emiten instrumentos separados para las distintas áreas (Cons. la discusión del alcance del RGPD en la Parte Dos, Sección 2.3, a continuación). Véase el sitio web del centro de investigación CVCE de la Universidad de Luxemburgo sobre los acontecimientos históricos en el proceso de integración europea (1945 - 2014), en particular la página "El primer pilar de la Unión Europea":
https://www.cvce.eu/en/education/unit-content/-/unit/02bb76df-d066-4c08-a58a-d4686a3e68ff/4ee15c10- 5bdf-43b1-9b5f-2553d5a41274
La Directiva de Protección de Datos (y las demás directivas tratadas en esta sección) fue (y fueron) todas ellas publicadas cuando el Primer Pilar aún estaba en vigor, y se publicaron solamente para dicho pilar.
[68] Título completo: Directiva 95/46 / CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, sobre la protección de las personas en relación con el tratamiento de datos personales y sobre la libre circulación de dichos datos, DO L281, 23.11.1995, págs. 31 a 50, disponible en:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN

para garantizar la protección continua de los datos transferidos a terceros países (no UE/EEE).

*NUEVO Definiciones

La Directiva amplió las definiciones básicas del Convenio de 1981 y añadió otras nuevas. Específicamente, aclaró (dentro de la definición de "datos personales") cuándo las personas deberían considerarse "identificables" (por "cualquier persona"), y (en una definición separada) cuando un conjunto de datos manuales debe considerarse suficientemente "estructurado" para estar sujeto a la Directiva. Los "archivos manuales [estructurados]" se incluyeron en el alcance de la Directiva para evitar la elusión de sus reglas mediante el uso de dichos archivos.

La Directiva ***estableció una definición algo modificada de "responsable",*** y añadió una ***definición global de "procesado de datos personales***" y definiciones de los conceptos de "tratamiento", "tercero" y "destinatario". También añadió una definición de "consentimiento del interesado" que en efecto establecía las condiciones que debían cumplirse antes de que cualquier consentimiento reclamado pudiera considerarse válido: el consentimiento, para ser válido, tenía que ser "***otorgado libremente, específico e informado***" y ***expresado*** de alguna manera (Art. 2(h)).[69]

Mientras que el Convenio de 1981 tenía cuatro definiciones, la Directiva proporcionaba ocho (o nueve, si se tiene en cuenta la definición de "persona identificable" dentro de la definición de "datos personales" por separado).

Principios de la protección de datos:

La Directiva repitió en gran medida los **principios de protección de datos** del Convenio de 1981, pero con algunas aclaraciones, incluyendo que el propósito para el que se tratarán los datos personales no solo debe ser "especificado" y "legítimo" (como ya se estipuló en el Artículo 5 (b)) del Convenio), pero también "explícito" (Art. 6 (1) (b)), y en lo que respecta al "tratamiento ulterior de los datos con fines históricos, estadísticos o científicos" (Véase el Art. 6 (1) (c) y (e)).

*NUEVO Bases legales para el tratamiento

Una importante característica nueva de la Directiva de 1995 fue que, para conseguir una mayor armonización entre las leyes de los Estados miembros, establecía en el artículo 7 **una lista exhaustiva de "criterios para legitimar el tratamiento de datos**", lo que más tarde se denominaría "**bases jurídicas**" **para el tratamiento de datos personales**. Conforme a la Directiva, el tratamiento de datos personales (no sensibles) solo se permite si (en resumen):

(a) el titular de los datos había dado ***inequívocamente*** su ***consentimiento*** (que, por supuesto, también tenía que ser "***libre, específico e informado***" y ***expreso:*** Art. 2(h), mencionado anteriormente); o

(b) el tratamiento era ***necesario*** para la ejecución de un contrato del que el interesado es parte o para tomar medidas a petición del interesado antes de celebrar un contrato (por ejemplo, para una verificación de crédito); o

(c) el tratamiento era ***necesario*** para el cumplimiento de una ***obligación legal*** a la cual el controlador está sujeto; o

(d) el tratamiento era ***necesario*** para proteger los ***intereses vitales del interesado***; o

(e) el tratamiento era ***necesario*** para la realización de una ***tarea llevada a cabo en interés público o en el ejercicio de la autoridad oficial*** conferida al responsable del

[69] El consentimiento tenía que tomar la forma de una "**indicación** específica e informada **de sus deseos**, libremente dada **por la cual el sujeto de los datos indica que está de acuerdo** con que los datos personales relacionados con él estén siendo tratados", para citar el texto completo.

tratamiento o a un tercero a quien se divulgan los datos; o

(f) el tratamiento era ***necesario*** para los fines de los ***intereses legítimos*** perseguidos por el responsable o por el tercero o las partes a quienes se divulgan los datos, excepto cuando dichos intereses fueron anulados por los intereses de los derechos o libertades fundamentales de los interesados que requieren protección bajo el Artículo1(1). [el llamado criterio de "intereses legítimos" o "equilibrio" / base jurídica].

En resumen: en la mayoría de los casos se permitía el tratamiento de datos personales no sensibles, en función de la legislación, de un contrato o con el consentimiento del titular de los datos, o basándose en que era un interés legítimo del responsable que no está sobrepasado por los intereses o los derechos y libertades fundamentales de los interesados.

En el Convenio sobre protección de datos de 1981 no figuraba ninguna lista de ese tipo.

*NUEVO <u>Reglas específicas para el tratamiento de datos sensibles</u>

La Directiva de 1995 enumeró en gran parte las mismas **principales "categorías especiales de datos"** generalmente denominadas "datos confidenciales", como se establecieron en el Convenio de 1981, con cambios menores, es decir, [70]

> datos personales que revelan origen racial o étnico, opiniones políticas, religiosas o creencias filosóficas, afiliación sindical, y… datos relacionados con la salud o la vida sexual

Sin embargo, en lugar de simplemente estipular que tales datos "no deberían tratarse automáticamente a menos que la legislación nacional establezca garantías apropiadas" (Convenio Consejo de Europa, Art. 6), la Directiva, en el Artículo 8 (1), estableció una **prohibición en principio** para el tratamiento de tales datos sensibles, sujeto a un número limitado de excepciones. Las principales **excepciones,** en efecto, **constituían bases jurídicas especialmente restrictivas** para el tratamiento de datos confidenciales. Eran (de nuevo, en resumen):

- tratamiento sobre la base del consentimiento no solo libre, específico e informado, sino también **explícito** del interesado, excepto cuando una ley nacional prohíba el tratamiento de tales datos incluso con el consentimiento del interesado en circunstancias particulares (artículo 8) (2)(a));

- tratamiento que es ***necesario*** para cumplir con las obligaciones y los derechos del responsable según la ***legislación laboral*** (siempre que la legislación nacional establezca una "salvaguardia adecuada") (artículo 8 (2)(b));

- tratamiento que es ***necesario*** para proteger los **intereses vitales** del interesado u otra persona en la que el interesado sea física o legalmente incapaz de dar su consentimiento (artículo 8 (2) (c));

- tratamiento "llevado a cabo en el curso de sus actividades legítimas con las garantías apropiadas por una fundación, asociación o cualquier otro **organismo sin ánimo de lucro con un objetivo político, filosófico, religioso o sindical** y con la condición de que el tratamiento se refiera únicamente a los ***miembros*** del organismo o las personas que tienen contacto regular con él en relación con sus finalidades? y que "los datos no se revelan a un tercero sin el consentimiento de los interesados" (artículo 8 (2) (d)) ;

- tratamiento "de datos personales (confidenciales) "**que el interesado manifiesta públicamente**" (Art. 8 (2) (e), primera sub-oración); y

[70] El Convenio de 1981 no incluía la referencia a datos "étnicos", referidos a "creencias religiosas u otras" (en lugar de "creencias religiosas o filosóficas"), y no incluía la afiliación sindical.

- tratamiento " de datos personales (sensibles) que es necesario para el establecimiento, ejercicio o defensa de **reclamaciones legales**" (Art. 8 (2)(e), segunda sub-oración);

Cabe destacar que la lista no incluía un criterio de "**interés legítimo**" o "**equilibrio**": el tratamiento de datos confidenciales podría, en principio, en virtud de la Directiva, no tratarse sobre la base de que es en interés legítimo del responsable del tratamiento o tercero, que no fueron superados por los intereses de los derechos fundamentales del interesado.

Sin embargo, la Directiva también estipulaba que la prohibición en principio del tratamiento de datos sensibles (nota: de cualquier tipo de datos confidenciales) no se aplicaba "cuando el tratamiento de los datos se ***requiere*** para los fines de ***medicina preventiva, diagnóstico médico, provisión de atención o tratamiento*** o la ***gestión de los servicios de atención de la salud***", siempre que esto se haga bajo una obligación relevante de secreto (Art. 8(3)). Nótese que esto se aplica a cualquier tipo de datos confidenciales, pero, por supuesto, dichos datos solo pueden usarse para tales fines cuando sea relevante (por ejemplo, la información sobre la procedencia étnica puede ser relevante en relación con ciertas enfermedades, como la anemia drepanocítica; las creencias religiosas de una persona pueden ser relevantes para ciertos tratamientos, como la transfusión de sangre para los testigos de Jehová).

Además, aunque las normas anteriores eran, como tales, estrictas, la Directiva también contenía una cláusula mucho más amplia (apartado 4 del artículo 8) que permitía a los Estados miembros conceder **excepciones adicionales**, es decir, permitir el tratamiento de (cualquier tipo de) datos sensibles que no se basen en los motivos enumerados en el artículo 8, apartado 2, ya sea por ley o por decisión de su autoridad nacional de supervisión (autoridad de protección de datos), "***por razones de interés público sustancial***", siempre que sea sujeto a "***salvaguardas adecuadas***", que definirá el Estado Miembro.

La Directiva también establecía un enfoque algo más restrictivo para el tratamiento de **datos personales relacionados con condenas penales** (artículo 8(5)) y de los **números de identificación nacional** u otros "**identificadores de aplicación general**" (artículo 8(7)), Pero dejó los detalles de la regulación de dicho tratamiento a los Estados miembros.

Del mismo modo, si bien fue más enfático que el Convenio de 1981 sobre la necesidad de **equilibrar la protección de datos y la libertad de expresión e información**, dejó la consecución específica de este equilibrio también a los Estados miembros (artículo 9).

*NUEVO **Información a los titulares de datos**

El Convenio de Protección de Datos de 1981 solo requería cierta transparencia general sobre "la existencia de un archivo automatizado de datos personales, sus propósitos principales, así como la identidad y residencia habitual o el lugar principal de negocios del controlador del archivo" (Art. 8 (a)).

Por el contrario, los artículos 10 y 11 de la Directiva de protección de datos de 1995 establecen con cierto detalle la **información que debe proporcionar cualquier responsable a los interesados**, o el movimiento del controlador, cuando, respectivamente, los datos personales fueron recabados de ellos o de un tercero. Los detalles que deben proporcionarse incluyen, en ambos casos, la ***identidad del controlador*** y la ***finalidad del tratamiento***. Se debe proporcionar ***más información*** (incluida información sobre los datos que deben recopilarse como obligatorios o no, información sobre cualquier divulgación de los datos) en la medida necesaria para garantizar un tratamiento justo (véanse los artículos 10(c) y 11(1) (c)).

*NUEVO Derechos de los interesados

El Convenio de Protección de Datos de 1981 ya exigía que los interesados tuvieran derecho a obtener **acceso** a sus datos cuando lo solicitasen, a intervalos razonables; el derecho a **rectificación o borrado** de datos que fueran incorrectos o tratados en violación de los principios de protección de datos; y un derecho a la **subsanación** si no se cumplía con el ejercicio de estos derechos (Art. 8(b) - (d)).

La Directiva confirmó los dos primeros derechos, pero añadió **importantes detalles adicionales**. Confirmó que el **derecho de acceso** incluía el derecho a que los datos fueran "comunicados" al

interesado (lo que ya estaba estipulado en el Convenio), pero añadió que esto tenía que ser "*de forma inteligible*" y que "*cualquier información disponible como [la **fuente** de los datos]*" también debe proporcionarse (Art. 12(a), segundo punto). Añadió el "**bloqueo**" como una opción aparte de la rectificación y el borrado (aunque sin definir el concepto) [71] (Art. 12(b)); y estipuló que cualquier rectificación, bloqueo o borrado debe señalarse a la atención de ***terceros*** a quienes se les han divulgado los datos (Art. 12(c)).

También introdujo nuevos derechos: un **derecho general a oponerse** al tratamiento por "razones legítimas imperiosas", "al menos" en relación con el procesado de una tarea llevada a cabo en interés público o en el ejercicio de la autoridad oficial, o sobre la base de criterio de "interés legítimo" / "equilibrio" - con tal objeción que debe cumplirse si fue "justificada" (Art. 14(a)); un **derecho más específico y más fuerte para oponerse al tratamiento de los datos con fines de marketing directo** (en esos días, principalmente por medio de correo directo, esto es antes del nacimiento de Internet y el correo electrónico "spam") que siempre deben respetarse, sin que el interesado tenga que proporcionar ninguna justificación (Art. 14(b)); y el **derecho a no estar sujeto a una decisión totalmente automatizada basada en la elaboración de perfiles**[72] que tuviera efectos legales u otros efectos significativos (sujeto a ***excepciones*** importantes pero estrictamente calificadas) (artículo 15). En este último sentido, es importante señalar que el artículo 12(a), tercer punto, estipulaba que los interesados también tenían el **nuevo** derecho a obtener (en el contexto de una solicitud de acceso) **información sobre la "lógica"** involucrada en cualquier tratamiento automatizado de datos relativos a ellos, "al menos" en el caso de tales decisiones totalmente automáticas basadas en el perfil. Con respecto a la inteligencia artificial, es tanto más importante.
Estos derechos de la Directiva de 1995, que se prorrogan y se refuerzan en el RGPD, adquieren cada vez más importancia en relación con la toma de decisiones basadas en la "inteligencia artificial".

* NUEVO Confidencialidad y seguridad de los datos

El Convenio de 1981 simplemente estipuló que debían adoptarse "medidas de seguridad apropiadas" para proteger los datos personales contra "la destrucción accidental o no autorizada o la pérdida accidental, así como contra el acceso, la alteración o la divulgación no autorizados" (artículo 7).

La Directiva amplió considerablemente este aspecto al imponer, ante todo, un **deber de confidencialidad** a cualquier persona implicada en el tratamiento de datos personales (artículo 16), y luego estipuló que se exigía al responsable que implementara "medidas técnicas y organizativas apropiadas para proteger datos personales contra la destrucción accidental o ilegal o pérdida accidental, alteración, divulgación no autorizada o acceso, en particular cuando el tratamiento implica la transmisión de datos a través de una red, y contra todas las demás formas ilegales de tratamiento "(Artículo 17 (1), con más detalles). Esta última disposición fue tomada de la Ley Federal Alemana de Protección de Datos de 1977.

También estableció importantes requisitos nuevos para cuando un responsable contrate a un procesador para tratar datos en su nombre (del controlador), incluido un requisito de "garantías suficientes" con respecto a la seguridad y confidencialidad, y un requisito de un contrato por escrito detallado entre el controlador y procesador (Art. 17 (2) - (4)).

* NUEVO Restricciones sobre transferencias transfronterizas de datos

Como se señala en 1.2.3, supra, el Convenio de 1981, tal como se adoptó originalmente, no exigía que los Estados-partes adoptaran una **prohibición de exportar datos personales desde su territorio a un estado que no brindaba una protección similar**. Se trató solo de flujos de datos personales entre las partes del Convenio. La introducción de tal prohibición (sujeta a excepciones limitadas), deriva de la legislación y la experiencia en Francia y Dinamarca, y fue, por lo tanto, otra nueva característica importante de la Directiva de 1995.

Específicamente, estipuló que los datos personales sujetos a la Directiva podrían, en principio, solo transferirse a terceros países que garantizaran un nivel de protección que pudiera considerarse "**adecuado**"

[71] El correspondiente concepto de "restricción de procedo" se define en el RGPD como "el marcado de datos personales almacenados con el objetivo de limitar su tratamiento en el futuro" (Art. 4 (3) RGPD).
[72] Texto completo: "Una decisión que produce efectos legales sobre [el interesado] o lo afecta significativamente"
y que se basa únicamente en el procesado automatizado de datos destinados a evaluar ciertos aspectos personales relacionados con él, como su desempeño en el trabajo, solvencia, confiabilidad, conducta, etc. "La disposición se tomó directamente de la Ley de Protección de Datos de Francia de 1978. Artículos 2 y 3.

en términos de la Directiva (artículo 25 (1)); y que correspondería a la Comisión Europea determinar (por medio de lo que se llamó una "**decisión de adecuación**") si ese fue el caso con respecto a un tercer país específico (artículo 25 (2))[73]. La Comisión pasó a determinar la "idoneidad" no solo en relación con los terceros países en su conjunto, sino también en los **sectores** de determinados países (por ejemplo, inicialmente, el régimen de los organismos del sector público en Canadá) y en los **regímenes** especiales establecidos en determinados países (es decir, el régimen de "puerto seguro" establecido por los EE. UU., ya que fue reemplazado por el régimen de "Escudo de privacidad").

La prohibición en principio de la transferencia a países (o sectores en países) sin protección adecuada estaba sujeta a un número limitado de excepciones establecidas en el Artículo 26 (1) de la Directiva, la mayoría de las cuales eran similares a los motivos legales para el tratamiento en general, es decir (en resumen):

(a) el interesado había dado su ***consentimiento inequívocamente*** a la transferencia (que, por supuesto, también tenía que ser "***libre, específico e informado***" y ***expresado***: Art. 2(h), señalado anteriormente); o
(b) la transferencia era ***necesaria*** para la ejecución de un contrato entre el responsable y el interesado, o para tomar medidas a petición del interesado antes de celebrar un contrato (por ejemplo, para una verificación de crédito);
(c) la transferencia fue ***necesaria*** para la celebración o cumplimiento de un contrato entre el responsable y un tercero, celebrado en interés del afectado (por ejemplo, una reserva de hotel);
(d) la transferencia era ***necesaria*** o ***legalmente requerida*** para un interés público, motivos importantes, o para el establecimiento, ejercicio o defensa de ***reclamaciones legales***;
(e) la transferencia es ***necesaria*** para proteger los ***intereses vitales del interesado***; o
(f) la transferencia se realiza desde un ***registro abierto al público*** (sujeto a las condiciones que se aplican para acceder al registro en general)

Adicionalmente, se autorizó a los Estados miembro a autorizar transferencias cuando el responsable del tratamiento presenta "salvaguardas adecuadas" para la protección de los intereses y derechos de protección de datos de los interesados (artículo 26 (2)), por ejemplo, en forma de cláusulas de transferencia datos ad hoc o (para transferencias de datos intra-corporativas) por medio de las llamadas Normas Corporativas Vinculantes" (BCR); y se autorizó a la Comisión a aprobar ciertas "cláusulas contractuales estándar" para las transferencias de datos, que garantizarían dicha protección (artículo 26 (4)).

Algunas agencias de protección de datos, y en sus inicios el GT29, también consideraron garantías contenidas en las denominadas ***Normas empresariales vinculantes*** (BCR), es decir, normas elaboradas por empresas internacionales o grupos de empresas que regularon los usos internos y los flujos de datos personales dentro de esas empresas o grupos.[74] A pesar de las dudas por parte de otras APD, la idea se

[73] El término "protección adecuada" se eligió porque el término "equivalente" estaba reservado en la legislación de la CE (entonces la UE) a las relaciones entre las normas entre los Estados miembros, mientras que, en base al derecho internacional, habría sido "equivalente en efecto". Pero en su sentencia en Maximillian Schrems v. el Comisionado de Protección de Datos, sentencia CJEU en el Caso C-362/14, 6 de diciembre de 2015, el Tribunal sostuvo que el término "protección adecuada" debería interpretarse como en efecto que requiere una protección "esencialmente equivalente" en el tercer estado: Véase párr. 96 de la sentencia, pero eso fue, por supuesto, muchos años después de que la Directiva de 1995 (o incluso el Protocolo adicional de 2001 del Convenio de 1981, que se menciona más adelante en el texto) fueron adoptados.

[74] El WP29 abordó las NEV en una serie de documentos de trabajo y recomendaciones, entre los que se incluyen:

- *Working Document*: *Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*, adoptado por el Grupo de Trabajo del artículo 29 el 3 de junio de 2003; (WP74);
- *Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules*, adoptado por el Grupo de Trabajo del artículo 29 el 3 de junio de 2003 (WP108);
- *Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data*, adoptado por el Grupo de Trabajo del artículo 29 el 10 de enero de 2007 (WP133);
- *Working document setting up a table with the elements and principles to be found in Binding Corporate Rules*, adoptado por el Grupo de Trabajo del artículo 29 el 24 de junio de 2008 (WP153);
- *Working document setting up a framework for the structure of Binding Corporate Rules,* adoptado por el Grupo de Trabajo del artículo 29 el 24 de junio de 2008 (WP154);
- *Working document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules*, adoptado por el Grupo de Trabajo del artículo 29 el 24 de junio de 2008, en su versión final revisada y adoptada el 8 de abril de 2009 (WP155);
- *Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules*, adoptado el 6 de junio de 2012 (WP195).

Véase también:

incluyó formalmente en el RGPD (tal como se indica en la Parte Dos).

Las limitaciones a las transferencias de datos personales a terceros países sin la protección adecuada estimuló la acción fuera de Europa. En particular, las APD francesas y españolas lo utilizaron para promover la adopción de leyes adecuadas en sus respectivas áreas lingüísticas globales (respectivamente, Latinoamérica y países francófonos, de forma particular en África).

NB: Como se señala en el punto 1.2.3, supra, se introdujo un requisito de "idoneidad" para las transferencias de datos para el Convenio de 1981 en el Protocolo Adicional de 2001 de dicho Convenio, con el objetivo de armonizar el régimen del Convenio a este respecto con el régimen previsto en la Directiva de la CE de 1995 (véase el artículo 2 (1) PA), aunque, por supuesto, solo se aplica a los Estados Parte el Convenio original que también se adhirieron al Protocolo[75].

*NUEVO Códigos de conducta (y certificaciones)

Otra característica nueva introducida por la Directiva fue su referencia a los **códigos de conducta** como un medio para "contribuir a la correcta implantación de las disposiciones nacionales adoptadas por los Estados miembros de conformidad con esta Directiva, teniendo en cuenta las características específicas de los diversos sectores" (art. 27(1)) - aunque solo fue tan lejos como para "alentar" tales códigos (ídem); exigir a los Estados miembros que prevean la evaluación de ***proyectos de códigos nacionales*** (Art. 27(2)); y en sí misma previendo que el Grupo de Trabajo del Artículo 29 (GT29, que se discute más adelante bajo ese encabezado), evalúe de manera similar los ***proyectos de códigos a nivel comunitario*** (Art. 27(3)).

En la práctica, solo unos pocos de estos códigos han sido aprobados o incluso sometidos a aprobación. El primer borrador del Código de prácticas europeo para el uso de datos personales en el marketing directo de la Asociación Europea de Marketing Directo (FEDMA) se presentó al GT29 en 1998, pero la versión final solo se aprobó en 2003.[76] Un proyecto de Código de conducta para los proveedores de servicios en la nube, elaborado por un grupo de trabajo de la industria establecido en 2013 y en realidad presidido conjuntamente por dos Direcciones Generales de la UE (DG Connect y DG Justicia) se presentaron al GT29 en enero de 2015, pero no fueron aprobados por el GT29 en su opinión sobre el borrador, y sigue siendo un "trabajo en proceso de desarrollo".[77]

Aunque no se menciona expresamente en la Directiva, la Comisión Europea también alentó el establecimiento de esquemas de certificación.[78] Proporcionó financiación inicial a un grupo de APD y expertos liderados por el APD de Schleswig-Holstein para el establecimiento de un ***esquema de certificación paneuropeo, el Sello de Privacidad Europeo (EuroPriSe)***, bajo el cual los productos y servicios que involucran el uso de datos personales pueden ser evaluados y, si se considera que cumplen con la Directiva (y, en su caso, otros instrumentos de protección de datos de la UE, como la Directiva de privacidad

---

- *Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents*, adoptado el 27 de febrero de 2014 (WP212).

[75] Véase nota 46. Cabe señalar que no queda claro si el término "adecuado" en este artículo del Protocolo puede o debe interpretarse de acuerdo con la sentencia Schrems (nota 73), y por lo tanto, si el PA realmente logró este objetivo.

[76] Texto del Código:
https://ec.europa.eu/digital-single-market/en/NUEVOs/data-protection-code-conduct-cloud-service-providers
El Grupo de Trabajo Art. 29 Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing (WP232, adoptado el 13 de junio de 2003) disponible en:
http://ec.europa.eu/justice/Artículo-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf

[77] Véase
https://ec.europa.eu/digital-single-market/en/news/data-protection-code-conduct-cloud-service-providers
(19 de julio, 2013 – antecedentes general y documentos sobre los antecedentes)
https://ec.europa.eu/digital-single-market/en/news/data-protection-code-conduct-cloud-service-providers
(12 de octubre, 2015 – última información disponible en este sitio web)
Grupo de Trabajo Art.29, Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing (WP232, adoptada el 22 de septiembre, 2015), disponible en:
http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf
Para más información y opiniones sobre el RGPD, consulte la carta del WP29 dirigida a los proveedores de servicios de insfraestructura en la nube de 6 de febrero de 2018, disponible en: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=615033

[78] Cuando Internet comenzó a surgir en el mundo en general a principios de la década de 1990, la APD francesa sugirió a las demás APD de la UE ya la Comisión Europea que los esquemas de certificación podrían ser un medio muy eficaz para tratar con los servicios en línea establecidos fuera de Europa, pero no se hizo nada en ese momento.

electrónica, debatida en el siguiente encabezado), otorga un certificado que confirma dicha conformidad (aunque, dado que no existe una base formal para el esquema en la Directiva de 1995, estas certificaciones, por supuesto, no tienen fuerza legal).[79]

*NUEVO Reglas sobre la "ley aplicable"

Como debe quedar claro a partir de las diversas entradas bajo los diferentes encabezamientos, arriba, bajo la Directiva, los Estados miembros tuvieron considerable discreción para determinar la manera precisa en que querían "transponer" las disposiciones de la Directiva; muchas de esas disposiciones dejaron a los Estados miembros adoptar las normas que consideren apropiadas para contextos particulares. Esto dio lugar a una grave falta de armonización[80], y fue uno de los motivos principales por los que se eligió la forma de un reglamento para que los instrumentos sucedieran a la Directiva. [81]
Las dificultades causadas por estas discrepacias fueron, en cierta medida, aliviadas por una disposición crucial en la Directiva de protección de datos de 1995, sobre la "ley aplicable". Esta disposición (Art. 4) estableció efectivamente tres reglas diferentes para el sector privado:

(1) los responsables que se establecieron en un solo Estado Miembro tenían que cumplir con la ley de protección de datos de ese Estado Miembro en relación con cualquier tratamiento que controlaran y que se "llevó a cabo en el contexto de las actividades de un establecimiento de [qué] controlador "(Art. 4 (1) (a), primera sub-oración);

(2) los responsables establecidos en más de un Estado Miembro [léase: los establecimientos en más de un Estado Miembro] tenían que garantizar "que cada uno de estos establecimientos cumpliese con las obligaciones establecidas por la legislación nacional aplicable" (que no es necesario ser el país del establecimiento en cuestión) (Art. 4 (1) (a), segunda sub-oración);

(3) los responsables que no estaban establecidos en la Comunidad (UE) tenían que cumplir con las leyes de cualquier Estado Miembro en el territorio en el que "hicieron uso de equipos, automatizados o no" (Art. 4 (12) (c))y dichos controladores tenían que "designar a un representante" en ese territorio (Art. 4 (2)).[82]

Cabe señalar que estas reglas no solo permitieron a los Estados miembros proteger los derechos sobre protección de datos de sus **ciudadanos** de vulneraciones de actores fuera de su territorio o de la UE. Si no que, bajo las tres reglas, los **datos de todas las personas** ("personas físicas") procesadas por los responsables relevantes tenían que ser protegidos, ***independientemente de si los interesados estaban en la UE o no, y si eran ciudadanos de la UE, residentes o no***, en línea con el principio de *universalidad de los derechos humanos.*[83]

Estas normas fueron difíciles de aplicar en la práctica (en particular en relación con los controladores no pertenecientes a la UE/EEE), [84] pero proporcionaron al menos alguna orientación sobre cómo tratar diferentes leyes en diferentes Estados miembros que en teoría podrían ser aplicables a cualquier operación particular transnacional de tratamiento de datos personales. Ninguna disposición de este

[79] Véase: https://www.european-privacy-seal.eu/EPS-en/about-europrise
[80] Véase el estudio de Douwe Korff, Report on an EU study on the implementation of the [1995] data protection directive, 2002, encargado por la UE en 202, disponible en: http://papers.ssrn.com/sol3/papers.Cons.m?abstract_id=1287667
[81] Véase Parte Dos, Sección 2.1 y el texto del primer encabezado "A regulation…" en la Sección 2.2, más abajo.
[82] La aplicación de esta tercera regla se complicó por el uso de diferentes palabras en los diferentes idiomas (todas ellas iguales y válidas jurídicamente: la diretiva original se redactó en francés, y el término utilizado fue *moyens, means* en inglés. La palabra que se eligió en el resto de idiomas oficiales con raíz latina fue su equivalente lingüístico, con el mismo significado que *means*. La versión oficial en alemán también utilizó la misma palabra: *mittel.* Sin embargo, el texto en inglés hacía referencia al uso de "equipos" (*equipment*), al igual que la holandesa *(middelen).* Esto llevó al Reino Unido y a Países Bajos a limitar la aplicación de la regla a situaciones en las que el controlador no perteneciente a la UE / EEE poseía algún equipo local en la UE / EEE (en el caso, el Reino Unido), mientras que otros países sostuvieron que incluso la presencia de un teléfono inteligente en la UE / EEE era suficiente para hacer que cualquier controlador "use" un dispositivo de este tipo para transitar datos sujetos a la Directiva. *Cf.* El debate sobre "legislación aplicable" en relación con la Directiva de privacidad electrónica en se detalla en el siguiente apartado 1.3.3.
[83] Véase Douwe Korff, Maintaining Trust in a Digital Connected Society, informe redactado para la International Telecommunications Union (ITU), mayo 2016, Sección 2.3, Universalidad de los Derechos Humanos disponible en: http://www.itu.int/en/ITU-D/Conferences/GSR/Documents/ITU_MaintainingTrust_GSR16.pdf
[84] Véase: Douwe Korff, Der EG-Richtlinienentwurf über Datenschutz und "anwendbares Recht", en: Recht der Datenverarbeitung, Año 10 (1994), Vol. No. 5- 6, p. 209 et seq.; La cuestión de la „ley aplicable"en: Compliance Guide 3 – Interim report (parte de la nueva ley británica de protección de datos de 1998, Programa de Información & Cumplimiento), Privacy Laws & Business, Noviembre1999.

tipo dirigida a evitar "conflictos de ley" estaba contenida en el Convenio de protección de datos de 1981.

Por lo que se refiere al sector público, la determinación de la legislación aplicable era en la práctica más sencilla: todas las autoridades y organismos públicos, incluidas las instituciones diplomáticas, estaban sujetos únicamente a la legislación sobre protección de datos (o a las leyes) de su propio Estado miembro.

*NUEVO Autoridades de supervisión

Otra novedad importante de la Directiva de 1995, en comparación con el Convenio de 1981[85], fue el requisito de que todos los Estados miembros debían designar:

> una o más autoridades públicas son responsables de supervisar la aplicación en su territorio de las disposiciones adoptadas por los Estados miembros de conformidad con la presente Directiva.
> (Art. 28(1), primera frase)

Con el objetivo de ser efectivas, estas "**autoridades de supervisión**", en la práctica más comúnmente conocidas como ***agencias de protección de datos o APD,*** (de las cuales había varios en los Estados miembros federales), debían otorgar amplias facultades de ***investigación, intervención y dirección*** (incluidas las facultades para ordenar el bloqueo), borrado o destrucción de datos, o para prohibir el tratamiento) (Art. 28(3), primer y segundo punto), y tenía que poder "actuar con total independencia en el ejercicio de las funciones que se les confían" (Art. 28(1), segunda oración). El requisito de independencia lo es también de democracia y de imperio de la ley. Dado que los requisitos de independencia no se mencionaban en la directiva, la Comisión tuvo que recurrir a acciones judiciales contra diferentes Estados miembros para aclarar el asunto. Los resultados de estas acciones judiciales se han reflejado en disposiciones más elaboradas de la RGPD sobre esta materia.

Debían ser ***consultados*** por las autoridades cuando elaboraban medidas o reglamentos relacionados con la protección de datos (Art. 28 (2)) y tenían que poder "***iniciar procedimientos legales***" en relación con presuntas violaciones de su ley nacional de protección de datos. (Art. 28 (3), punto).

También se les encargó la notificación y el "control previo", como se explica en el siguiente subtítulo.

También era crucial, aparte de los recursos más formales que se mencionan en el siguiente subtítulo después de eso, a las APD se les debía otorgar el derecho a "**escuchar las reclamaciones** [léase: tramitar las quejas] presentadas por cualquier persona, o por una asociación que represente a esa persona" relacionados con la protección de datos (art. 28 (4)).

Las APDs, que a nivel de la UE trabajan juntas en el "**Grupo de trabajo del Artículo 29**" expuesto en el último subtítulo de la presente sección, se han convertido en las principales defensoras de los derechos de protección de datos en la UE (incluso si sus poderes y efectividad se encuentran bajo la legislación nacional adoptada para aplicar la Directiva siguen siendo diferentes).

*NUEVO Notificación y "comprobación previa"

*NUEVO *Notificación:*

Con el fin de lograr una **transparencia general** sobre el tratamiento de datos personales y ayudar a garantizar el pleno cumplimiento de la ley de protección de datos, la Directiva de protección de datos de 1995 también contempla un amplio sistema de notificación de operaciones de tratamiento de datos personales (art. 18, ver art. 19 para los detalles del contenido de la notificación); y estipuló que los

[85] Ya estaba previsto por las Directrices de la ONU no vinculantes adoptadas en 1990 (véase nota 41 más arriba).
Además, como se señala en 1.2.3, se incluyó un requisito para que los estados establezcan autoridades de supervisión independientes, siguiendo el modelo de la Directiva de protección de datos de 1995, para el Convenio de 1981 en el Protocolo adicional de 2001 de esta. Directiva de la CE (Véase art. 1 AP) - que solo es aplicable a aquellos Estados-Partes en el Convenio que también se adhirieron al Protocolo (tal como figura en la nota 45, véase más arriba).

datos notificados deberían incorporarse en un registro que debería ser accesible al público (Art. 21 (2)). Se basó en el sistema que se adoptó por primera vez en Suecia en 1973, y luego fue adoptado por muchos otros Estados miembros de la UE.

Sin embargo, la Directiva también permitió a los Estados miembros, como alternativas equivalentes a la notificación, prever ***simplificaciones*** o ***excepciones*** de la obligación de notificación general en (principalmente) dos situaciones "equivalentes", es decir:[86]

- cuando, para el tratamiento "no riesgoso",[87] la APD del Estado Miembro había emitido "***normas simplificadas***" que establecían los parámetros básicos para el tratamiento (es decir, los fines del tratamiento, los datos o categorías de datos que se están procesando, la categoría o categorías del titular de los datos, los destinatarios o las categorías de destinatarios a quienes se divulgarán los datos y el tiempo durante el cual se almacenarán los datos) (Art. 18 (2), primer punto), con los responsable que declararon formalmente que acataron esas normas simplificadas que están **exentas** de notificación; o
- cuando la ley del Estado Miembro requiera el nombramiento de un oficial de protección de datos independiente dentro de la organización del responsable de "garantizar de manera independiente la aplicación interna de [la ley nacional de protección de datos adoptada para implementar la Directiva] y de mantener una Registro de operaciones de tratamientos realizadas por el responsable", que contiene la misma información que, de lo contrario, tendría que ser notificada a la APD (Art. 18(2), segundo punto).

La primera excepción se basó en el sistema francés de "*normes simplifiées*" (normas simplificadas); la segunda en el sistema alemán de requerir el nombramiento de Delegados de Protección de Datos dentro de las organizaciones de todos los responsables públicos y los responsables de los mayores entes del sector privado.[88] En relación con ambos sistemas alternativos, la Directiva estipulaba que los responsables (o algún otro organismo designado por el Estado Miembro) deberían hacer pública la misma información a la que se podría acceder a través del registro de operaciones notificadas (Art. 21(3)).

*NUEVO *"Comprobación previa":*

En línea con el enfoque francés, la Directiva de 1995 requería que el tratamiento que planteaba "**riesgos específicos para los derechos y libertades de los interesados**" ("tratamiento de riesgo") estuviera sujeto al requisito de "***verificación previa***" (Art. 20). Se dejó a los Estados miembros determinar **qué tipos de operaciones de tratamiento** se someterían a este requisito de mayor alcance (teniendo en cuenta el propósito del tratamiento, los tipos de datos y la escala del tratamiento en cuestión). Los Estados miembros también podían elegir cómo y quién llevaría a cabo dicho control, en particular:

- si se requiere una comprobación previa al ***enviar una notificación*** que indique que la operación notificada fue de un tipo que requirió tal verificación por parte de la APD (el enfoque francés, que siguió la mayoría de Estados miembros); o
- si el tratamiento iba a ser regulado por una ley o un instrumento legislativo subsidiario por parte de la APD, en el curso de la preparación del instrumento, o por el Parlamento, en el curso de la adopción de tal instrumento.
  (Art. 20(2) y (3)).

Debido a estas diversas opciones en la Directiva, los diferentes Estados miembros adoptaron (o más bien,

[86] Las otras operaciones que podían quedar exentas de la obligación de notificación eran los **registros públicos**, en los que se tramitaban los **registros de los miembros y asociados de los organismos políticos, religiosos, filosóficos o sindicales sin ánimo de lucro (sujetos a ciertas garantías) y los archivos manuales** (apartados 3 a 5 del artículo 18).

[87] Texto completo: "Operaciones de procesado que es improbable que se verán afectadas o que afecten de manera adversa a los derechos y libertades de los titulares de los datos".

[88] Mencionados respectivamente como *behördliche-* y *betriebliche Datenschutzbeauftragten*, que no deben confundirse con las autoridades de protección de atos federales y estatales, *Landes-* and *Bundesdatenschutzbeauftragten*. Cabe señalar que, aunque algunos Estados miembros han introducido el concepto de DPD en las leyes que aplican la directiva, lo han hecho de diferente modo, con diferente ámbito y tareas para los DPD, y con diferentes condiciones para sus nombramientos. Tal como se detalla en la Parte Dos, el RGPD, sin embargo, proporciona orientaciones detalladas y armonizadas sobre el nombramiento, y lo vincula con el principio de "responsabilidad".

retuvieron) diferentes regímenes a este respecto, lo que significaba que algunas operaciones estaban sujetas a notificación o controles previos en algunos Estados miembros, pero no en otros.

*NUEVO Subsanaciones y sanciones específicas

El Convenio de 1981 estipuló que los Estados-partes en ese convenio deberían "establecer ***sanciones y recursos apropiados***" por violaciones de sus leyes nacionales de protección de datos, pero no aclararon qué sería "apropiado".

En contraste con esta estipulación en el Convenio de 1981, la Directiva de 1995 estipuló que los interesados deberían tener acceso a un **recurso judicial** por cualquier (presunta) violación de sus derechos (aparte del derecho a presentar denuncias ante la agencia nacional de protección de datos pertinente) señalada en el subtítulo anterior (Art. 22). Además, cualquier persona que hubiera sufrido daños como resultado de cualquier tratamiento ilegal u otro acto incompatible con la Directiva debía tener derecho a obtener una **-indemnización** del controlador (a menos que este último pueda probar que no fue responsable) (Art. 23).[89] Y más allá de estos recursos, los Estados miembros también debían prever nuevas "medidas adecuadas" y "sanciones", independientemente de cualquier reclamación o queja individual (Art. 24).

Sin embargo, en muchos Estados miembros, las sanciones reales que podrían imponerse en virtud de la legislación nacional pertinente, o que se impusieron en la práctica, fueron relativamente menores.[90]

*NUEVO El Grupo de Trabajo del Artículo 29 y el Comité del Artículo 31

Finalmente, la Directiva de protección de datos de 1995 estableció dos organismos a nivel de la UE, que llevan el nombre de los artículos bajo los cuales fueron creados:

- El denominado "**Grupo de trabajo del artículo 29**", un grupo de organismos independientes compuesto por representantes de las autoridades de protección de datos de los Estados miembros, así como del SEPD, y un representante de la Comisión Europea (responsable de la secretaría del grupo, sin derecho a voto), al que se encomendó la tarea de contribuir a una aplicación más armonizada de la Directiva, en particular mediante la adopción de recomendaciones y dictámenes (por iniciativa propia) y la emisión de un dictamen sobre cualquier proyecto de código de conducta elaborado a nivel de la UE; y que debía ser consultado por la Comisión Europea sobre cualquier propuesta en relación con *"los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales"* (es decir, protección de datos) y sobre todo ello, proyecto de borrador sobre la protección de la adecuación en un tercer país[91] y

- El llamado "**Comité del artículo 31**", compuesto por representantes de los gobiernos de los Estados miembros, pero presidido por un representante de la Comisión, al que todos los proyectos de medidas que deben adoptarse en virtud de la Directiva deben someterse a dictamen; si el Comité emitía un dictamen negativo, la medida debía remitirse al Consejo, donde podría ser revocada por mayoría cualificada.[92]

El **Grupo de Trabajo del Artículo 29** (GT29) ha emitido **numerosos documentos de trabajo y opiniones** sobre una amplia gama de temas relacionados con la aplicación de la Directiva de Protección de Datos de 1995 y la Directiva de Privacidad Electrónica de 2002 (que se analiza en 1.3.3, a continuación).[93] Estos

[89] El Reino Unido trató inicialmente limitar esto solo al daño material, pero al final se sostuvo que la Directiva requiriera que las personas también deber de ser capaces de obtener una compensación por los daños no materiales.
[90] La necesidad de sanciones más fuerte se ha vuelto más frecuente con la aparición de Internet, en gran parte controlado por entidades no pertenecientes a la UE/EEE que tienen menos probabilidades de cumplir con las regulaciones de la UE. Esto se refleja en la mucho más estricta estipulación en el RGPD de que las APD pueden imponer multas administrativas de hasta € 10,000,000 o el 2% de la facturación anual del actor responsable, o incluso en casos extraordinarios hasta 20,000,000 ó el 4% de la facturación anual (Art 83 RGPD).

[91] Para detalles, véase el Artículo 30.
[92] Para detalles, véase el Artículo 31.
[93] Todos los documentos de trabajo del Grupo de Trabajo del Art. 29 adoptados entre 1997 y noviembre de 2016 se pueden consultar en esta página-archivo:
http://ec.europa.eu/justice/Artículo-29/documentation/opinion-recommendation/index_en.htm

documentos, y especialmente las opiniones formales, aunque no son legalmente vinculantes, siguen teniendo una gran autoridad en términos de las directivas. Han ayudado a garantizar que las directivas se apliquen plena y estrictamente, a un "alto nivel", y hasta cierto punto han mitigado los problemas derivados de las discrepancias en las leyes de los Estados miembros.

NB: El sucesor del GT29, el European Data Protection Board (EDPB) Comité Europeo de Protección de Datos, se basa en el trabajo del GT29: en su primer día de existencia, el 25 de mayo de 2018, confirmó una serie de opiniones del GT29 que se habían redactado en previsión del RGPD[94]. Su secretaría corre a cargo de los PDE.

1.3.3 La Directiva de Protección de datos de telecomunicaciones, la Directiva EC sobre privacidad electrónica de 2002 y las modificaciones a la Directica sobre privacidad electrónica de 2009.

General

La **Directiva de protección de datos de telecomunicaciones**, propuesta al mismo tiempo que la Directiva de protección de datos de 1995, se adoptó el 15 de diciembre de 1997.[95] Su relación con la Directiva de protección de datos de 1995 se aclaró en el art. 1 (2), que establecía que las disposiciones de la directiva eran "particularizar y complementar" la directiva principal. Específicamente, las definiciones precisas de protección de datos en la Directiva de 1995, y todos los demás principios y reglas de esa directiva, se aplicaron también a los responsables y a las operaciones de tratamiento sujetas a la Directiva de Protección de Datos de Telecomunicaciones, excepto cuando esta última establece normas más específicas o diferentes. En otras palabras, la Directiva de protección de datos de telecomunicaciones fue una *lex specialis* en relación con la Directiva de protección de datos de 1995, la *lex generalis*.

La implantación de esta directiva se retrasó, en parte porque, en 1999, la Comisión llevó a cabo una revisión general del marco regulatorio para las comunicaciones electrónicas, con vistas a desarrollar nuevas tecnologías y prácticas comerciales. Uno de los resultados de esta revisión fue una propuesta, en 2000, para reemplazar la Directiva de Protección de Datos de Telecomunicaciones con una Directiva nueva sobre protección de datos en el sector de las comunicaciones electrónicas.[96] Esto llevó a la adopción, en julio de 2002, de la Directiva de Privacidad y Electrónica. Comunicaciones, Directiva 2002/58/CE, generalmente conocida como la "**Directiva de privacidad electrónica**".[97] También enfatizó su carácter subsidiario y complementario en relación con la principal Directiva de protección de datos de 1995, en los mismos términos que su predecesor (ver Art. 1(2)).

En 2009, la Directiva de 2002 se modificó mediante una directiva independiente, la Directiva 2009/136/CE[98], a

---

Las actualizaciones y los documentos adoptados después de noviembre de 2016 hasta la abolición del WP29 el 25 de mayo de 2018 se pueden encontrar aquí:
http://ec.europa.eu/NUEVOsroom/Artículo29/NUEVOs-overview.Cons.m

[94] Véase nota 248

[95] Título completo: Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ L24, 30.01.1998, pp. 1 – 8, disponible en:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31997L0066&from=EN
La Directiva de Protección de Datos de Telecomunicaciones se ha redactado extensamente sobre el trabajo realizado en el Consejo de Europa, sobre la recomendación del Consejo de Europa para la adopción de la Recomendación No. R (95) 4 del Comité de Ministros del Consejo de Europa. Estados miembros sobre la protección de datos personales en el área de servicios de telecomunicación, con referencia a los servicios telefónicos, adoptada el 7 de febrero de 1995, disponible en
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805010 8e –
y en el trabajo de las APD en el Grupo de Trabajo sobre la Protección de Datos en Telecomunicaciones (el "Grupo de Berlín"), creado en 1993. Véase: https://www.dataprotectionauthority.be/berlin-group

[96] Propuesta de Directiva del Parlamento Europeo y del Consejo sobre el tratamiento de datos personales y la protección de la privacidad en el sector de las comunicaciones electrónicas, Bruselas, 12.07.2000, COM (2000) 385 final.

[97] Título completo: 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 (Directiva sobre la privacidad y las comunicaciones electrónicas)), OJ L201, 31.07.2002, pp. 37 – 47, disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN

[98] Título completo: Directiva 2009/136/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009 por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) no 2006/2004 sobre la cooperación en materia de protección de los consumidores, OJ L337, 18.12.2009, pp. 11-36, disponible en: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:ES:PDF

la denominada habitualmente la "Ley de las *cookies*" porque regulaba las *cookies* (aunque también regulaba otros asuntos adicionales y actividades de tratamiento de datos). En el siguiente texto describiremos las normas tal como aparecían en la Directiva de 2002, modificada por la Directiva de 2009. En aras de la brevedad, de vez en cuando nos referiremos a la Directiva de protección de datos de 1995 como la "directiva principal", ya la Directiva de privacidad electrónica como su directiva "subsidiaria".

En la fecha en que se redacta este documento (diciembre de 2018), la Directiva de privacidad electrónica sigue vigente, a pesar de su instrumento "madre", la Directiva principal de protección de datos de 1995 ha sido reemplazada por el Reglamento general de protección de datos. Un sucesor de la Directiva electrónica de privacidad, que también debe ser un reglamento (en lugar de una directiva), está en proceso de ser adoptado (ver la sección 1.4.2, a continuación). No obstante, dado que la Directiva sobre privacidad en las comunicaciones electrónicas sigue vigente actualmente, en esta primera edición del manual se le sigue prestando toda la atención que merece y por qué, a la espera de la adopción de la nueva propuesta de Reglamento de privacidad en las comunicaciones electrónicas, describiremos a continuación la Directiva sobre la privacidad en las comunicaciones electrónicas que aún es aplicable actualmente.

Objetivo, finalidad y ámbito de aplicación de la Directiva sobre privacidad electrónica de 2002, modificada en 2009.

Considerando que la principal Directiva de protección de datos de 1995 se aplicó ampliamente a todo el tratamiento de datos personales por parte de cualquier entidad relevante del sector público o privado activo en el "Primer pilar" de la Comunidad Europea, la Directiva de privacidad electrónica, como un instrumento subsidiario, tiene un ámbito mucho más limitado (definido de forma más específica). En sus propias palabras, se aplica:

> Al tratamiento de datos personales en relación con la **prestación de servicios de comunicaciones electrónicas accesibles para el público en redes de comunicación públicas** en la Comunidad, *incluidas las redes de comunicación públicas de apoyo a dispositivos de identificación y recopilación de datos.*
>
> (Artículo 3, énfasis añadido; las palabras en cursiva se añadieron en la enmienda de 2009)[99]

El término "servicio de comunicaciones electrónicas"está definido precisa y estrictamente en el Artículo 2(C) de la Directiva Marco revisada[100], del siguiente modo:

> "servicio de comunicaciones electrónicas" hacer eferencia a un servicio prestado por lo general a cambio de una remuneración que consiste, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión, pero no de los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o ejerzan control editorial sobre ellos; **quedan excluidos asimismo los servicios de la sociedad de la información definidos en el artículo 1 de la Directiva 98/34/CE[101], que no consistan, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas** (énfasis añadido).

EL GT29 indicó la conclusión que se deduce de esta estipulación del Artículo 3 y de las definiciones en estos

---

[99] En las modificaciones de 2009 se eliminó la excepción para los intercambios analógicos, incluida en la versión original (2002) de la Directiva de privacidad electrónica.

[100] Título completo: Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco*)*, OJ L 108, 24.04.2002, pp. 33 – 50, disponible en: https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX%3A32002L0021

[101]Título completo: Directiva 98/34/CE del Parlamento Europeo y del Consejo de 22 de junio de 1998 por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas, OJ L 204, 21.07.1998, pp.37-48, disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A31998L0034

instrumentos en su *Opinion on Geolocation servies on Smart mobile devices* de 2011:[102] la Directiva sobre privacidad en las comunicaciones electrónicas se aplica a los proveedores de servicios de comunicaciones electrónicas, a los operadores de telecomunicaciones y los proveedores de acceso a Internet, pero no a proveedores de servicios de sociedad de la información.[103]

(Tal como se detalla más exhaustivamente en el siguiente apartado 1.4.2, la Comisión propone eliminar este límite en virtud del Reglamento de privacidad electrónica propuesto, pero hasta que este se lleve a cabo, se mantiene como está).

Dentro de este marco limitado, la Directiva de privacidad electrónica tiene los mismos objetivos que la Directiva principal: garantizar un ***alto nivel de protección*** de los datos personales (pero en este caso específicamente para ese sector) y permitir la ***libre circulación de datos personales*** dentro de la Comunidad (en dicho sector) (*cf.* Art. 1(1)). Ha tenido un importante impacto en el área de las comunicaciones electrónicas, de rápido crecimiento y que va ganando peso, lo que garantiza un nivel de protección de los datos más alto en ese ámbito dentro de la UE que en cualquier otra aprte del mundo.

Ahora bien, a pesar de la aparentemente clara redacción del Artículo 3, la cuestión del ámbito exacto de la Directiva de privacidad electrónica no está completamente clara, puesto que algunas de sus disposiciones se aplican, o se interpreta que se aplican, de una forma más amplia, y porque la Directiva de privacidad electrónica no incluye una disposición específica sobre la legislación aplicable. Sin negar el éxito de la Directiva de privacidad electrónica, estas ambigüedades deben señalarse brevemente.

Ambigüedad y falta de coherencia respecto al ámbito

En primer lugar, existe ambigüedad respecto al ámbito de aplicación:

> La Directiva de privacidad electrónica tal como señaló la Comisión en su propuesta de Reglamento de privacidad electrónica:[104]
>
> Los consumidores y las empresas confían cada vez más en servicios nuevos basados en internet que les permiten realizar comunicaciones interpresonales, como la tecnología de Voz sobre protocolo de internet, mensajería instantánea y servicios web de correo electrónico, que sustituyen a los servicios de comunicación tradicionales. **Estos servicios de comunicación OTT *normalmente* no están sujetos al marco de comunicaciones electrónicas vigente en la Unión, incluida la Directiva de privacidad electrónica.**

Un estudio de 2013 encargado por la Comisión (The SMART Study) concluyó lo siguiente:[105]

> **Las disposiciones nacionales relativas a cuestiones como las *cookies*, los datos de tráfico y ubicación o las comunicaciones no deseadas, adoptadas en virtud de la Directiva de privacidad electrónica, tienen normalmente un ámbito de aplicación diferente al definido por el Artículo 3 de la Directiva de privacidad electrónica**, que se limita únicamente a proveedores de servicios de comunicación electrónica públicos (es decir, empresas de telecomunicaciones tradicionales). [El estudio concluyó que] el límite del ámbito de la Directiva a los proveedores de servicios de comunicación electrónica es ambiguo y puede resultar en un trato desigual si los proveedores de servicios de la sociedad de la infrmación que utilizan internet para prestar servicios de comunicación se excluyen de forma general de este ámbito.

También hay una falta de claridad en cuanto a la legislación nacional aplicable:

---

[102] Grupo de Trabajo Art. 29, *Opinion 13/2011 on Geolocation services on smart mobile devices* (WP185, adoptada el 16 de mayo de 2011), disponible en: http://ec.europa.eu/justice/Artículo-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf

[103] WP29 *Opinion 13/2011 on Geolocation services on smart mobile devices* (nota anterior), apartado 4.2.1., *Aplicabilidad de la directiva de privacidad electrónica revisada* (págs. 8-9).
Tal como se detalla más exhaustivamente en el siguiente apartado 1.4.2, la Comisión propone eliminar este límite en virtud del Reglamento de privacidad electrónica propuesto, pero hasta que este se lleve a cabo, se mantiene como está.

[104] Propuesta de Reglamento de privacidad electrónica (nota 175 siguiente), apartado 1.1, pág. 1, énfasis añadido.

[105] "Directiva sobre intimidad en las comunicaciones electrónicas: evaluación de la transposición, la eficacia y la compatibilidad con la propuesta de Reglamento sobre protección de datos" (SMART 2013/0071) (en lo sucesivo denominado "el estudio SMART"), que puede consultarse en la dirección siguiente:
https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data (para ver el informe completo, siga los enlaces al final de la página).

Hasta que la Directiva sobre privacidad en las comunicaciones electrónicas no sea sustituida por la propuesta de Reglamento sobre privacidad en las comunicaciones electrónicas (que puede que no lo sea durante algún tiempo), las ambigüedades y desproporciones antes mencionadas seguirán existiendo y la eficacia de la Directiva sobre intimidad en las comunicaciones electrónicas se verá obstaculizada por ello.

Relación entre la Directiva de privacidad electrónica y el RGPD

La Directiva sobre privacidad en las comunicaciones electrónicas era una *lex specialis* en relación con la *lex generalis* de la Directiva de 1995 y, por lo tanto, también es una *lex specialis* en relación con su sucesor, el RGPD. Por lo tanto, en lo que respecta a las cuestiones que se rigen específicamente por la Directiva sobre privacidad en las comunicaciones electrónicas, se aplica la Directiva sobre intimidad en lugar de las disposiciones de la RGPD.

Así pues, los fundamentos jurídicos de la RGPD no son aplicables cuando la Directiva sobre privacidad en las comunicaciones electrónicas establece normas más específicas para el tratamiento de datos personales. Por ejemplo, se aplica el artículo 6 de la Directiva sobre privacidad en las comunicaciones electrónicas, que establece una lista especí fica de fundamentos jurídicos relativos al tratamiento de datos de tráfico, incluidos los datos de tráfico que constituyen datos personales, y, por consiguiente, no se aplica el artículo 6 de la RGPD. Sin embargo, en todos los demás casos relativos al tratamiento de datos personales, se aplica la RGPD.

Lo mismo se aplica a **entidades que están, o no, "reguladas específicamente por la Directiva de privacidad electrónica**. A tenor de la opinión del GT29, que considera que la Directiva de privacidad electrónica se aplica únicamente a proveedores de servicios de comunicación electrónica, esto significa que, del mismo modo (salvo en relación con las normas especiales establecidas en los Artículos 5(3) y 13, que pueden aplicarse más ampliamente), el tratamiento de datos, incluidos los datos reguladso más específicamente por la Directiva de privacidad electrónica (como los datos de tráfico) por *entidades diferentes a los proveedores de servicios de comunicación electrónica*, está sujeto al RGPD y no a la Directiva de privacidad electrónica, a pesar de las disposiciones especiales estipuladas en la Directiva de privacidad electrónica relativas a dichos datos.

En otras palabras:

- Los proveedores de servicios de comunicación electrónica deben atenerse la Directiva de privacidad electrónica en relación con cualquier cuestión que esté específicamente regulada en dicha directiva, y al RGPD en lo que respecta al resto de cuestiones; y

- Las entidades que no son proveedores de servicios de comunicación electrónica deben atenerse a las estipulaciones recogidas en el Artículo 5(3) de la Directiva de privacidad electrónica en relación con el acceso a la información en dispositivos y en el Artículo 13 de dicha directiva en lo que respecta a las comunicaciones no deseadas, y al RGPD en lo relativo a cualquier otra cuestión (es decir, no están sujetos a ninguna de las disposiciones recogidas en la Directiva de privacidad electrónica salvo las dos mencionadas).

Las situaciones específicas en las que surgen las cuestiones mencionadas se señalan cuando resulta pertinente en el resto de subapartados de este apartado.

Características clave de la Directiva de privacidad electrónica[106]

Definiciones

Dado que la Directiva sobre la privacidad electrónica fue concebida expresamente como una ley especial a la *lex generalis* de la Directiva de 1995 sobre protección de datos, las **definiciones relacionadas con la protección de datos** de la Directiva de Protección de Datos de 1995 también se aplicaron en relación con

[106] Muchos de los requisitos de la Directiva de privacidad electrónica anotados aquí ya estaban contenidos en la Directiva de protección de datos de telecomunicación de 1997 y simplemente se traspusieron a la Directiva de privacidad electrónica, pero esto no se destaca en mayor medida cada vez. Cuando se marca como "NUEVA" una cuestión o disposición, significa que es o introduce algo que no se había habordado (todavía) en la Directiva de protección de datos de 1995.

la Directiva sobre la privacidad electrónica, tal como se establece expresamente en el Artículo 2, primera oración de la Directiva de privacidad electrónica. No obstante, dado que la Directiva de protección de datos de 1995 se ha reemplazado por el RGPD, todas las referencias a las definiciones en dicha directiva deberán interpretarse como referencias a las correspondientes (aunque en ciertos aspectos actualizadas y reforzadas) definiciones del reglamento. Esto se indica a continuación, bajo el título independiente de "Consentimiento". [107]

Además, mientras que las **definiciones de los términos más técnicos** relacionados con la comunicación electrónica en la Directiva Marco para Redes y Servicios de Comunicaciones Electrónicas[108] que fue el resultado de la revisión mencionada[97] - ***servicio de comunicaciones electrónicas[109]; servicio de comunicaciones electrónicas disponible al público; red de comunicaciones públicas***; etc. - también se aplican a los términos técnicos relevantes utilizados en la Directiva de privacidad electrónica. Esto incluye el término "**suscriptor**" (a un servicio de comunicación electrónica).

Además, en el Artículo 2, la Directiva de privacidad electrónica agrega una serie de **definiciones adicionales** *NUEVAS, como **"usuario", "datos de tráfico", "datos de ubicación", "servicio de valor añadido"** y **"violación de seguridad de los datos personales"** (ver el artículo para consultar información detallada).

*MODIFICADO Consentimiento

El cambio más importante en las definiciones de conceptos clave en el RGPD en comparación a los de la Directiva de protección de datos de 1995 está relacionado con el "**consentimiento**" como base legal para el tratamiento de datos personales.

Concretamente, el artículo 2, letra f), de la Directiva sobre intimidad en las comunicaciones electrónicas establece que el "consentimiento" de un usuario o abonado, tal como se utiliza en dicha Directiva, corresponde al consentimiento del interesado en la Directiva sobre protección de datos. Dado que todas las referencias a la Directiva de protección de datos deben interpretarse ahora como referencias a la RGPD, el consentimiento en virtud de la Directiva sobre intimidad en las comunicaciones electrónicas debe entenderse de la misma manera que el consentimiento en virtud de la RGPD, donde se define como:

> cualquier indicación libre, específica, informada e inequívoca de los deseos del interesado mediante la cual éste, mediante una declaración o una acción afirmativa clara, manifieste su acuerdo con el tratamiento de los datos personales que le conciernen (art. 4(11) de la RGPD).

La RGPD también aclara con más detalle qué condiciones deben cumplirse antes de que cualquier consentimiento pueda considerarse válido y especifica, entre otras cosas, lo que significa para que el consentimiento se otorgue libremente, y lo que podría constituir una acción afirmativa clara[110]. Además, el Comité Europeo de Protección de Datos (EDPB) ha publicado directrices sobre el consentimiento.[111]

Estas aclaraciones de la RGPD y de las presentes directrices son especialmente pertinentes en relación con varias disposiciones clave de la Directiva sobre intimidad en las comunicaciones electrónicas que requieren el consentimiento del usuario o abonado. Entre ellas se incluyen:

- Artículo 5.3 para el almacenamiento o recopilación de información desde equipos terminales;
- Artículos 6 y 9 para la reutilización de datos de tráfico y ubicación para servicios de valor añadido para fines de servicios de comunicaciones electrónicas de

[107] El RGPD también aclara en cierto modo el concepto de "datos personales", manifestando que una persona también puede ser "identificable" mediante el uso de un "identificador en línea" (Art. 4(1) RGPD; Art. 2(a) de la Directiva de protección de datos de 1995). Esto también debería tenerse en cuenta en la aplicación de la Directiva de privacidad electrónica.
[108] Nota al pie 100, arriba.
[109] Este término se ha comentado anteriormente, en el apartado "Objetivo, propósito y alcance de la Directiva de privacidad electrónica".
[110] Véanse los artículos 7 y 8 de la RGPD y los considerandos relacionados 32 a 33 y 42 a 43.
[111] EDPB Guidelines on Consent under Regulation 2016/679 (wp259rev.01). Estas Directrices fueron adoptadas por el Grupo de Trabajo del Artículo 29 (WP29) el 28 de noviembre de 2017 y revisadas el 10 de abril de 2018. Posteriormente han sido aprobados por su sucesor, el Comité Europeo de Protección de Datos (EDPB). Complementan un dictamen anterior del Grupo de Trabajo del artículo 29 sobre la definición de consentimiento (WP187, dictamen, 15/2011).

marketing;

- Artículo 12 para directorios de suscriptores; y
- Artículo 13 para comunicaciones no deseadas.

En relación con estas cuestiones, el consentimiento, para que sea válido, debe ser ahora el "consentimiento de la RGPD", y los Estados miembros deben revisar las leyes nacionales que transponen la Directiva sobre intimidad en las comunicaciones electrónicas y las prácticas nacionales de aplicación para asegurarse de que cumplen con el RGPD.

Las cuestiones antes mencionadas se examinan más adelante en los epígrafes correspondientes.

Seguridad

El Artículo 4 (1) repite efectivamente el requisito de seguridad de datos de la Directiva de Protección de Datos de 1995, al estipular que los proveedores de servicios de comunicaciones electrónicas deben tomar "***medidas técnicas y organizativas adecuadas para salvaguardar la seguridad de sus servicios***", y agregar que "si es necesario", esto debe hacerse "junto con el proveedor de la red de comunicaciones públicas [relevante]". También agrega, al igual que la Directiva principal, que el nivel de seguridad debe ser "***apropiado para el riesgo presentado***", teniendo en cuenta el estado de la técnica y el costo de las medidas. El Artículo 4(1a), introducido por la Directiva de 2009, añade lo siguiente:

> Sin perjuicio de la Directiva 95/46/CE, las medidas a las que se hace referencia en el párrafo 1 deben, al menos:
>
> - Garantizar que solo el personal autorizado puede acceder a los datos personales para fines legales autorizados;
> - Proteger los datos personales almacenados o transferidos de la destrucción accidental o ilegal, la alteración o la pérdida accidentales, y el almacenamiento, el tratamiento, el acceso o la divulgación no autorizados o ilegales; y
> - Garantizar la aplicación de una política de seguridad respecto al tratamiento de datos personales.

Tanto la Directiva de privacidad electrónica (en el Artículo 4) como el RGPD (en los Artículos 32-34) establecen la obligación de garantizar la seguridad, así como la obligación de notificar las violaciones de datos personales[112] a la autoridad nacional competenten y a la autoridad de supervisión [es decir, la autoridad de protección de datos], respectivamente.[113] Estas obligaciones coexistirán en paralelo bajo las dos leyes, de acuerdo con sus respectivos ámbitos de aplicación. De conformidad con el Artículo 95 del RGPD, este no impodrá obligaciones adicionales a personas físicas o jurídicas en relación con cuestiones sujetas a obligaciones específicas establecidas en la Directiva de privacidad electrónica. No obstante, como *lex specialis* del RGPD, la Privacidad electrónica no debería [tampoco] resultar en un nivel más bajo de protección que el establecido por el RGPD.

El Artículo 4(1) también estipula lo siguiente:

> Las autoridades nacionales competentes podrán examinar las medidas adoptadas por los proveedores de servicios de comunicaciones electrónicas disponibles al público y podrán formular recomendaciones sobre las mejores prácticas con respecto al nivel de seguridad que debería conseguirse con estas medidas.

Cabe destacar que estas “autoridades relevantes” no tienen por qué ser las autoridades nacionales de protección de datos. Veáse siguiente apartado “Supervisión y aplicación”.

*NUEVO Notificación de riesgos

[112] Los requisitos de notificación de violaciones de datos se detallan en el correspondiente apartado, a continuación del presente.
[113] Para obtener más información de las diferentes autoridades implicadas en la aplicación de la Directiva de privacidad electrónica, véase la siguiente cita del presente subapartado y el comentario correspondiente, así como el análisis del último título de este apartado.

El Artículo 4(2) de la Directiva de privacidad electrónica estipula lo siguiente:

> En el supuesto de que exista un **resgo particular de violación de la seguridad de la red**, el proveedor de un servicio público de comunicaciones electrónicas debe **informar** a los suscriptores de dicho riesgo y, si el riesgo no se incluye en el ámbito de las medidas que debe adoptar el proveedor de servicios, de los posibles recursos, así como de los posibles **costes** implicados. (énfasis añadido)

El requisito de "notificación de riesgos" (que ya se establecía en el texto original de 2002) debe distinguirse de los requisitos más exhaustivos de "notificación de violación de la seguridad de los datos", que se especifican en en siguiente apartado – que se añadieron en las modificaciones de 2009 y que solo se aplican cuando ha tenido lugar una violación, mientras que el Artículo 4(2) estipula la notificación de cualquier riesgo relativo a una violación que *podría ocurrir*.

*NUEVO Notificación de violación de seguridad de datos

La Directiva de privacidad electrónica (en su versión enmendada en 2009) estipula que, además de la "notificación de riesgos" detallada anteriormente, los proveedores de servicios de comunicación electrónica deben ***notificar a la "autoridad nacional competente"*** cualquier violación de la seguridad de los datos personales –léase violación real– "sin demora" (Art. 4(3), primera subcláusula – cabe señalar que esta autoridad no tiene por qué ser la APD.

Únicamente si "**es probable que la violación de la seguridad de los datos personales afecte negativamente a los datos personales o la privacidad de un suscriptor o un particular**", el proveedor deberá asimismo "**notificar al suscriptor o particular"** cualquier violación "sin demora" (Art. 4(3), segunda subcláusula). No obstante, dicha notificación al correspondiente suscriptor o particular no es necesaria:

> si el proveedor ha probado a satisfacción de la autoridad nacional competente que ha aplicado las medidas tecnológicas de protección convenientes y que estas se han aplicado a los datos afectados por la violación de seguridad. Las medidas de protección de estas características convertirán los datos en incomprensibles para toda persona que no esté autorizada a acceder a ellos. (Art.4(3), tercera subcláusula)

En otras palabras, no hay necesidad de informar a los suscriptores y otras personas físicas afectadas (en particular los interesados, pero también personas jurídicas que sean suscriptores) de una violación de la seguridad de los datos que implique sus datos personales si el proveedor puede demostrar a la "autoridad competente" que los datos que han sufrido la violación (en particular, cualquier dato que haya podido divulgarse de forma inadecuada o se haya puesto a disposición de terceros) se han hecho "incomprensibles" para cualquier pesona o personas que hayan podido obtener acceso como resultado de la violación mediante la aplicación de medidas de protección tecnológica adecuadas (como se detalla en el Artículo 4 del Reglamento 611/2013 de la Comisión).[114]

Por otro lado, la "autoridad competente" puede "solicitar" a un proveedor que notifique una violación de la seguridad de los datos a los suscriptores relevantes y otras personas físicas afectadas si el proveedor no lo ha hecho; es decir, porque la autoridad no aprueba la evaluación del proveedor por la que manifiesta que no es probable que la violación "afecte negativamente" a los datos personales o a la privacidad de dichos suscriptores o personas físicas, o porque la autoridad no considera que los datos filtrados sean completamente "incomprensibles" para receptores no autorizados (por ejemplo, porque la clave para descifrarlos se ha filtrado o ha podido filtrarse, o porque el método de encriptado no es lo suficientemente

[114] Título completo: Reglamento (UE) nº 611/2013 de la Comisión de 24 de junio de 2013 relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas, OJ L 173 de 26.06.2013, págs. 2-8, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32013R0611&from=EN
El Reglamento de la Comisión se adoptó en base al Artículo 4(5) de la Directiva de privacida electrónica, que le permitió adoptar "medidas de aplicación técnicas relativas a las circunstancias, el formato y los procedimientos aplicables a los requisitos de notificación e información a los que se hace referencia en este Artículo" (Art. 4(5)), tras consultar a la Agencia Europea de Seguridad de las Redes y de la Información, al WP29 y al SEPD, e implicar al resto de partes relevantes.

fuerte)[115] (Art. 4(3), subcláusula 4).

La quinta y última subcláusula del Artículo 4(3) estipula lo siguiente:

> La notificación al suscriptor o particular debe describir al menos la naturaleza de la violación de la seguridad de los datos personales y los puntos de contacto en los que pueden obtener más información, y debe recomendar medidas para mitigar los posibles efectos negativos de dicha violación. La notificación a la autoridad nacional competente deberá describir, asimismo, las consecuencias de la violación de la seguridad y las medidas propuestas o adoptadas por el proveedor para gestionarla.

La Directiva de privacidad electrónica, en su versión modificada por la Directiva de 2009, también establece **requisitos formales** importantes para fundamentar las nuevas estipulaciones mencionadas. De este modo:

> [Las autoridades nacionales competentes] también podrán **controlar** si los proveedores han cumplido sus obligaciones de notificación en virtud de este párrafo, y deberán imponerles las **sanciones** pertinentes en el caso de que no lo hagan.
>
> (Artículo 4(4), primera subcláusula, segunda oración, énfasis añadido)

La eficacia de estas facultades de revisión (inspecciones) y sanción se apoya en un requisito adicional, establecido en la segunda subcláusula del Artículo 4(4):

> Los proveedores deberán mantener un **inventario de violaciones de datos personales** que incluya los hechos relacionados con la violación, sus efectos y las medidas correctoras adoptadas que bastarán para permitir a las autoridades nacionales competentes verificar el cumplimiento de lo dispuesto en el párrafo 3. El inventario solo incluirá la información necesaria a estos efectos. (énfasis añadido)

La Directiva de privacidad electrónica modificada establece la publicación de "**directrices**" e "**instrucciones**" por parte de las "autoridades nacionales competentes" acerca de las "circunstancias en las que los proveedores deben notificar violaciones de datos personales, el formato de dicha notificación y la forma en que debe realizarse" (Art. 4(4), primera subcláusula, primera oración).

Los requisitos de notificación de violaciones de datos de la Directiva de privacidad electrónica mencionados, limitados por el ámbito de dicha directiva, anuncian los requisitos de notificación de la violación de seguridad más generales incluidos actualmente en el Reglamento general de protección de datos, aplicables a cualquier operación de tratamiento de datos personales, que se detallan en el apartado 2.1. de la Parte Dos. Pueden considerarse redundantes.[116]

Requisitos específicos para el tratamiento para fines concretos:

En lugar de repetir los principios generales de protección de datos y la lista de bases para el tratamiento legal que se establecen en la Directiva principal de protección de datos de 1995, la Directiva de privacidad electrónica establece un requisito general de confidencialidad de las comunicaciones y una serie de requisitos específicos y Condiciones para ciertos datos específicos u operaciones de tratamiento. A través de ellos, la Directiva de privacidad electrónica pretende aplicar los principios y derechos de la Directiva de protección de datos de 1995 a estas cuestiones específicas, con el objetivo de armonizar la aplicación de dichos principios y derechos en los Estados miembros, tal como se detalla a continuación en diferentes apartados.

No obstante, en primer lugar es importante recordar que, en la medida en que la Directiva de privacidad electrónica establece motivos legales específicos para el tratamiento con fines concretos (tal como se

[115] Por ejemplo, los algoritmos débiles como el MD5 o el SHA1 se consideran obsoletos y los datos encriptados mediante su uso ya no pueden considerarse realmente "incomprensibles" (léase "indescifrables"). Ver: https://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet.
También pueden existir casos en los que se violen los datos de comunicaciones electrónicas cuyo contenido se había encriptado totalmente mediante algoritmos sólidos como el SHA-256, pero no los metadatos. Cabe señalar que, tal como se indica en la página web mencionada, "la clasificación de algoritmo criptográfico fuerte" puede variar con el tiempo".

[116] Documento de trabajo de la Comisión (nota 99), Annex V: REFIT analysis of coherence of the e-Privacy Directive with the GDPR (Tabla – comentario de los Artículos 4.3, 4.4 y 4.5 – Notificación de violación de seguridad de datos personales).

estipula en dicha directiva), los motivos legales más generales para el tratamiento con fines diversos recogidos en los Artículos 5 y 6 del RGPD no se aplican.[117]

Por consiguiente, en aquellos casos en que la Directiva de privacidad electrónica requiere consentimiento −como en relación con el acceso a información en dispositivos (Art. 5(3)), o el envío de mensajes de *marketing* no deseados (Art. 13)− o establece una serie de bases legales específicas y fines de tratamiento −como en relación con el tratamiento de datos de tráfico (Art. 6)−, cualquier entidad sujeta a dichas normas −que en virtud de los Artículos 5(3) y 13 es cualquier entidad, y en virtud del Artículo 6 son los proveedores de servicios de comunicación electrónica− no podrá ampararse en cualquier otro motivo o principio estipulado en el RGPD. En particular, no podrán ampararse en el motivo de "fines compatibles" para efectuar el tratamiento establecido en el Artículo 5(1)(b) del RGPD.

*NUEVO ***Confidencialidad de las comunicaciones:***

El Artículo 5(1) de la Directiva de privacidad electrónica subraya la importancia fundamental de la confidencialidad de las comunicaciones, consagrada en muchas constituciones, al menos con respecto al correo y a las llamadas telefónicas (aunque a menudo ahora se extiende expresamente o mediante la interpretación de todas las formas de comunicación)[118] al estipular que los Estados miembros deben:

> garantizar la **confidencialidad de las comunicaciones y los datos de tráfico** relacionados mediante una red de comunicaciones pública y servicios de comunicaciones electrónicas disponibles al público, a través de la legislación nacional. En particular, ***deberán prohibir la escucha, grabación, almacenamiento u otros tipos de interceptación o vigilancia de las comunicaciones y los datos de tráfico relacionados por parte de personas distintas de los usuarios, sin el consentimiento de los usuarios interesados***, excepto cuando estén legalmente autorizados... (énfasis añadido)

Tal como aclaran las palabras "*escucha, pulsación [etc.]* … por parte de personas que no sean usuarios", esta disposición no solo se aplica a proveedores de servicios de comunicación electrónica. Más bien (de acuerdo con las excepciones indicadas a continuación), los Estados miembros deben prohibir, en virtud de sus legislaciones nacionales, dichas interferencias con el derecho de confidencialidad de las comunicaciones **de cualquier persona**, incluidas las agencias estatales y entidades privadas, como empresas.

El Art. 5(1) permite, como excepción, el *"almacenamiento técnico necesario para la transmisión de una comunicación sin perjuicio del principio de confidencialidad".* Hay una excepción adicional en el Artículo 5(2) en relación con el registro de comunicaciones y datos de tráfico para proporcionar evidencia de una transacción comercial o comunicación comercial.). La llamada Directiva de Retención de Datos, que se trata brevemente en el punto 1.3.4, a continuación, contempla una excepción más general y obligatoria a esta prohibición de interceptación y recopilación de datos de comunicaciones, pero fue declarada nula por el Tribunal de Justicia, tal como se analiza en ese punto.

*NUEVO ***El empleo de "cookies" y otras tecnologías intrusivas:***

La Directiva de privacidad electrónica modificada estipula en su Artículo 5(3), en unos términos bastante técnicos, que los Estados miembros deben garantizar que:

> El almacenamiento de **información o la obtención de acceso a la información almacenada en el equipo terminal de un suscriptor o usuario** solo se permite a condición de que el suscriptor o usuario en cuestión haya dado su **consentimiento** y haya recibido información **clara y completa** de acuerdo con la Directiva 95/46/CE, *inter alia*, sobre los propósitos del tratamiento.

La Directiva aclara lo siguiente en la oración posterior de este párrafo:

[117] Véase cita del Documento técnico oficioso de la Comisión en el apartado "Relación entre la Directiva de privacidad electrónia y el RGPD" anterior.
[118] *Cf.* la interpretación extensa del concepto de "correspondencia" en el Artículo 8 del CEDH por el Tribunal Europeo de Derechos Humanos en el famoso caso Klass v. la República Federal de Alemania (sentencia de 6 de septiembre de 1978), párr. 41, donde el Tribunal sostuvo que las "conversaciones telefónicas... están cubiertas por las nociones de "vida privada" y "correspondencia" [en ese Artículo]

> Esto no impedirá ningún almacenamiento o acceso técnico con el único propósito de llevar a cabo la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o según sea estrictamente necesario para proporcionar un servicio de la sociedad de la información solicitado explícitamente por el suscriptor o usuario.

Cabe destacar que las expresiones "con el único propósito" y "según sea estrictamente necesario" subrayan que esta excepción debe aplicarse de forma muy precisa.

La frase *"el almacenamiento de información, o la obtención de acceso a información ya almacenada, en el equipo terminal de un abonado o usuario"* es un lenguaje técnico para las tecnologías que permiten que un visitante de un sitio web sea reconocido por el sitio web y rastreado mientras utiliza el sitio web o incluso a través de sitios web. Los principales medios utilizados para ello son las llamadas **"cookies",** razón por la cual la Directiva de 2009 que reforzó las normas a este respecto (como se discute más adelante) se denominó inicialmente la **"Ley de cookies"** de la UE, y a veces se la sigue denominando como tal (por ejemplo, lo mismo ocurre con el sitio web de una entidad privada sobre este tema[119])

De hecho, hay una serie de cookies que surgen de herramientas técnicas estandarizadas a nivel internacional llamadas "RFC", adoptadas por el Internet Engineering Task Force (IETF), que pueden considerarse en el lenguaje cotidiano y que van desde "cookies de seguimiento de terceros" altamente intrusivas hasta las no intrusivas que mejoran el funcionamiento de los sitios web sin necesidad de rastrear al visitante,;[120] y existen otras tecnologías intrusivas como las "cookies flash", los métodos de almacenamiento HTML5 y las llamadas "evercookies. [121]

Todas se incluyen en la definición de *"información almacenada en el equipo terminal"* y, por tanto, (aunque resulta algo problemático) se tratan del mismo modo en virtud de la Directiva de privacidad electrónica.[122]

El propósito y el significado del Artículo 5(3) se explican en un lenguaje más simple en los considerandos (24) y (25) de la Directiva de privacidad electrónica, que aclara que la disposición anterior se extiende mucho más allá de las "cookies". Vale la pena citarlos en su totalidad:

> Los equipos terminales de los usuarios de las redes de comunicaciones electrónicas y cualquier información almacenada en dichos equipos forman parte de la esfera privada de los usuarios que requieren protección en virtud del Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales. Los llamados ***spyware, errores web, identificadores ocultos y otros dispositivos similares pueden ser introducidos en el terminal del usuario sin su conocimiento para obtener acceso a la información, almacenar información oculta o rastrear las actividades del usuario y pueden invadir seriamente la privacidad de estos usuarios El uso de tales dispositivos debe permitirse únicamente con fines legítimos, con el conocimiento de los usuarios interesados***. (énfasis añadidos)
>
> Sin embargo, tales dispositivos, por ejemplo, las llamadas "cookies", pueden ser una herramienta legítima y útil, por ejemplo, para analizar la efectividad del diseño de sitios web y la publicidad, y para verificar la identidad de los usuarios que participan en línea. actas. Cuando tales dispositivos, por ejemplo, las cookies, estén destinados a un propósito legítimo, como facilitar la prestación de servicios de la sociedad de la información, su uso debe permitirse a condición de que los usuarios

---

[119] Véase, por ejemplo: http://www.cookielaw.org/the-cookie-law/

[120] Véase:
Estas recomendaciones de la IETF sobre *cookies* (empezando por el RFC 2109 de 1997), que incluye un concepto no exhaustivo de privacidad y algunos datos obligatorios útiles en *cookies*
https://tools.ietf.org/html/rfc2109 (el RFC 2109 original);
https://tools.ietf.org/html/rfc2965 (RFC 2965, que sustituye al RFC 2109 pero conserva la misma lista de datos); y
https://tools.ietf.org/html/rfc6265 (RFC 6265 de 2011, qiue también mantiene la lista original, pero introduce el acceso de terceros a la *cookie* – la recomendación vigente en la actualidad).
See also this Wikipedia page:
https://en.wikipedia.org/wiki/HTTP_cookie
Esto proporciona información detallada sobre todos los tipos de cookies: cookies de sesión, cookies persistentes, cookies seguras, cookies sólo HTTP, cookies del mismo sitio, cookies de terceros, supercookies y cookies de zombies, proporcionando información técnica detallada.

[121] Véase: https://webcookies.org/doc/eu-web-cookies-directive

[122] Esto puede cambiar en el Reglamento de privacidad electrónica propuesto, que podría tratar estas tecnologías de forma diferente de acuerdo con su intrusismo relativo.

> reciban información clara y precisa de conformidad con la Directiva 95/46 / EC sobre los propósitos de las cookies o dispositivos similares para garantizar que los usuarios conozcan la información que se está colocando en el equipo terminal que están utilizando. Los usuarios deben tener la oportunidad de negarse a tener una cookie o dispositivo similar almacenado en su equipo. Esto es particularmente importante cuando los usuarios que no son el usuario original tienen acceso al equipo terminal y, por lo tanto, a cualquier dato que contenga información sensible a la privacidad almacenada en dicho equipo. La información y el derecho a rechazar pueden ofrecerse una vez para el uso de varios dispositivos que se instalarán en el equipo terminal del usuario durante la misma conexión y también cubrirá cualquier uso adicional que se pueda hacer de esos dispositivos durante las conexiones posteriores. Los métodos para proporcionar información, [ofrecer el derecho de rechazar][123] o solicitar el consentimiento deben ser tan fáciles de usar como sea posible. El acceso a contenido específico del sitio web aún puede estar condicionado a la aceptación bien informada de una cookie o dispositivo similar, si se usa con un propósito legítimo. (énfasis añadido).

La principal diferencia respecto a la Directiva de 2002 fue que cambió el régimen que regulaba el uso de dichas tecnologías, que pasó de ser uno en el que el suscriptor o usuario tenía que ser notificado y tenía que disponer del "derecho de rechazar" la configuración de *cookies*, etc.,[124] al establecido en el el Artículo 5(3), en virtud del cual el uso de *cookies* solo está permitido cuando el suscriptor o usuario no solo han sido notificados, sino uqe han dado su consentimiento **positivo y explícito** de conformidad con las condiciones de consentimiento (válido) establecidas en la Directiva de protección de datos de 1995[125], que lo definía del siguiente modo:

> toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan. (Art. 2(h))

No obstante, habida cuenta de la sustitución de la Directiva de 1995 por el RGPD, surge la cuestión de si esto debería interpretarse como una necesidad de **aplicar la forma más estricta de consentimiento estipulada en el Reglamento**. Si es así, el consentimiento para la instalación de *cookies* y herramientas similares estará basado en:

> toda manifestación de voluntad libre, específica, informada e **inequívoca** por la que el interesado acepta, ya sea **mediante una declaración o una clara acción afirmativa**, [la instalación de la *cookie* o el uso de otras herramientas][126]

Esto significaría que el uso de casillas ya marcadas en relación con el uso de *cookies*, etc. ya no cuplen los requisitos de consentimiento establecidos en la Directiva de privacidad electrónica.

No obstante, sigue siendo pertinente la cuestión de que la Directiva de privacidad electrónica básicamente trata igual todas las *cookies* y herramientas de rastreo, sin hacer distinciones, por ejemplo, entre *cookies* de sesión y *cookies* persistentes.

En la práctica, la disposición ha llevado a una cultura de "lo tomas o lo dejas" en Internet, en el que los visitantes del sitio web se ven obligados a hacer clic en "Estoy de acuerdo" (para colocar tipos de "cookies" generalmente no especificados) con el fin de obtener acceso a un sitio (incluso sitios de organismos públicos). El Estudio SMART concluyó lo siguiente[127]:

> puede que las normas relativas a *cookies* y tecnologías similares no hayan satisfecho completamente su objetivo, pueso que los usuarios reciben demasiados mensajes de aviso que no tienen en consideración de forma adecuada.

Todavía está por ver si esto cambiará en el marco de un nuevo Reglamento sobre la privacidad

---

[123] Para obtener más información relativa al derecho de rechazar, véase las siguientes dos notas a pie de página.

[124] En la versión original de 2002, la primera oración del Artículo 5(3) estipulaba lo siguiente:
Los Estados miembros velarán por que únicamente se permita el uso de las redes de comunicaciones electrónicas con fines de almacenamiento de información o de obtención de acceso a la información almacenada en el equipo terminal de un abonado o usuario a condición de que se facilite a dicho abonado o usuario información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46/CE y de que el responsable del tratamiento de los datos le ofrezca el derecho de negarse a dicho tratamiento.

[125] Este cambio no se refleja en los considerandos citados en el texto, que no se modificaron respecto a la Directiva 2002 original y sigue haciendo referencia al "derecho a rechazar", aunque este se eliminó en la Directiva de 2009. De hecho, estas palabras carecen de sentido en la actualidad.

[126] *Cf.* Artículo 4(11) RGPD. Énfasis añadido.

[127] Véase la anterior nota de pie de página 105.

electrónica, pero, por supuesto, estas cuestiones están directamente relacionadas con la aplicación de todos los principios y derechos básicos de protección de datos, incluida la limitación de la finalidad, la minimización de los datos, la limitación de la retención, etc., por ejemplo, en relación con cuestiones como los períodos de retención adecuados para las distintas cookies (en función de su finalidad),[128] cómo debe obtenerse el consentimiento válido ("consentimiento RGPD") para el uso de diferentes cookies, y cómo debe permitirse que los interesados ejerzan sus derechos, etc. - y cómo estas cuestiones pueden y deben aplicarse sobre la base de la protección de datos por diseño y por defecto - el principio ahora expresamente consagrado en el RGPD.

NUEVO** ***Limitaciones en el uso de datos de tráfico y ubicación:

El Artículo 6 de la Directiva de privacidad electrónica impone restricciones estrictas de limitación y retención de datos en el tratamiento de datos de tráfico y ubicación por parte de proveedores de servicios de comunicación electrónica. En principio, los datos de tráfico (es decir, los datos tratados con el fin de - y necesarios para - el transporte de una comunicación o para la facturación) solo pueden ser tratados y almacenados por el proveedor del servicio de comunicaciones electrónicas pertinente para los fines de la ***transmisión*** de una comunicación electrónica, la ***facturación*** del abonado por la comunicación, o para permitir ***pagos de interconexión*** (es decir, pagos entre proveedores por el uso de las redes de cada uno) (Art. 6(1) y (2)). Este tratamiento no precisa el consentimiento del suscriptor o usuario del servicio, puesto que es necesario para la prestación del servicio. Cuando ya no son necesarios para esos servicios, deben ser "borrados o anonimizados" (Art. 6(1)).[129]

Los datos de tráfico solo se pueden utilizar para la ***comercialización de servicios de comunicaciones electrónicas o para la prestación de servicios de valor añadido***, pero en estos casos solo con el ***consentimiento*** del suscriptor o del usuario. Una vez más, esto significa que ahora que el RGPD es plenamente aplicable, debe cumplir los requisitos del mismo respecto al consentimiento válido; es decir, que ahora el consentimiento válido debe ser:

> toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, [el uso de sus datos de tráfico para actividades de *marketing* por parte de proveedores de servicios de comunicación electrónica o para la prestación de un servicio de valor añadido específico].

La Directiva de privacidad electrónica también estipula que el proveedor de servicios debe informar al suscriptor o usuario de sus servicios sobre los tipos de datos de tráfico que se procesan y sobre la duración de dicho tratamiento; para el tratamiento basado en el consentimiento (es decir, para servicios de marketing y valor añadido: ver más arriba), esta información debe realizarse ***antes de obtener dicho consentimiento*** (Art. 6(4)).

Finalmente, la Directiva de privacidad electrónica estipula que el tratamiento de datos de tráfico para un proveedor de servicios de comunicaciones electrónicas para ***diferentes propósitos subsidiarios*** relacionados con la prestación de los servicios (***facturación, gestión del tráfico, consultas de clientes, detección de fraudes, mercadeo*** y provisión de ***servicios de valor añadido***), por parte de los miembros del personal del proveedor, o de cualquier procesador contratado por el proveedor, **debe estar restringido por "necesidad de tener acceso"**: cada uno de ellos solo debe tener acceso a los datos de tráfico que necesiten para su tarea (art. 6(5)). Sin embargo, los "organismos [externos] competentes", como los que resuelven las disputas de pagos de facturación o de interconexión, deben, por supuesto, tener acceso a los datos de tráfico cuando sea necesario (Art. 6 (6)).

La Directiva de privacidad electrónica es aún más estricta en lo que respecta al tratamiento de "**datos de ubicación distintos a los datos de tráfico**"; es decir, los datos tratados en una red de comunicaciones

[128] Algunos sitios web estipulan períodos de retención de 25 años, lo que es manifiestamente excesivo, cualquiera que sea su finalidad.
129 Sobre los problemas con la anonimización de dichos datos, véase la discusión del tema en el contexto del RGPD, en la Parte Dos, Sección 2.1, a continuación.

electrónicas que indican la ***posición geográfica del equipo terminal de un usuario*** (tal como, por lo general, un teléfono móvil) pero que ***no se procesa con el fin de transmitir una comunicación electrónica o una facturación por dicha comunicación***. Dichos datos solo pueden ser tratados cuando se convierten en anónimos,[130] o, en la medida en que puedan utilizarse para la prestación de un servicio de valor añadido, con el consentimiento de los usuarios o suscriptores de dicho servicio (Art. 9(1), primera frase). El proveedor del servicio de comunicaciones electrónicas debe **informar** nuevamente a los usuarios y suscriptores de los detalles del tratamiento, antes de obtener dicho consentimiento (ídem, segunda oración). Esos usuarios y suscriptores deben, además, poder retirar dicho consentimiento en cualquier momento (ídem, tercera oración) y/o desactivar temporalmente dicho seguimiento de ubicación, "utilizando un medio simple y gratuito" (Art. 9(2))). Y nuevamente, el tratamiento de dichos datos debe estar restringido al personal del proveedor de servicios de comunicaciones electrónicas, o del proveedor del servicio de valor agregado relevante (o de un procesador contratado por cualquiera de ellos) (Art. 9 (3)).

*NUEVO *Facturación detallada*

Los suscriptores deben tener derecho a elegir si desean recibir facturas no desglosadas (Art. 8(1), y los Estados miembros también deben proporcionar otras soluciones para mejorar la privacidad en relación con las facturas desglosadas (Art. 8(2), por ejemplo, facturas desglosadas que sólo muestra los códigos de país o regionales para las llamadas salientes, o que omiten u ocultan los tres últimos dígitos del número al que se ha llamado, tanto para explicar el importe de la factura como para proteger la privacidad del usuario (que puede no ser el suscriptor o un miembro de la familia).

*NUEVO *Identificación de llamadas y líneas conectadas y desvío automático de llamadas*

Los proveedores de servicios de comunicación electrónica deben ofrecer a las personas que llaman a las personas llamadas (incluidas las personas que llaman desde la UE [entonces EC] que realizan llamadas a terceros países) la **opción de evitar la identificación de la línea de llamada por parte de la persona que recibe la llamada**, pero las personas que reciben una llamada de un número no identificado dentro o fuera de la EU/EC) debe poder **bloquear** la llamada; y las personas deben poder desconectar su propia identificación de línea de llamada a llamada (Art. 8(1)-(4)).

Los proveedores de servicios de comunicaciones electrónicas también deben **informar al público** (y, por supuesto, en particular a sus suscriptores y usuarios) de estas opciones (Art. 8(6)).[131]

Sujeto a las normas nacionales pertinentes (y, por supuesto, a los principios generales de necesidad y proporcionalidad), los proveedores de servicios de comunicación electrónica pueden anular los bloqueos en la identificación de la línea de llamada, ya sea mediante la aplicación de un suscriptor, para ***rastrear llamadas maliciosas*** o molestas (para facilitar las investigaciones de reclamaciones por parte de proveedores y autoridades policiales, y para proporcionar pruebas en causas judiciales), o para asistir a los servicios de ambulancia y bomberos para ***responder a llamadas de emergencia*** (Art. 10(1) y (2)).

El suscriptor también debe tener "la posibilidad", utilizando un medio simple y gratuito, de ***detener el desvío automático de llamadas*** por parte de un tercero a la terminal del suscriptor" (Art. 11).

Todas estas opciones obligatorias han sido incorporadas a las normas técnicas internacionales, de modo que ahora pueden aplicarse fácilmente en la práctica en relación con los teléfonos inteligentes, etc.

*NUEVO *Directorios de suscriptores*

[130] Véase nota anterior.

[131] Estas opciones fueron desarrolladas inicialmente por APD nacionales. Curiosamente, estas opciones, en contraste con las normas de *cookies* técnicas, tan pronto como se empezaron a ofrecer comercialmente los servicios de "identificación de llamadas", etc. en la década de 1980, se integraron a las normas internacionales técnicas de transmisión de telecomunicaciones (líneas antiguas), y cuando aparecieron los móviles, se integraron a los móviles para activar las opciones. Esto se consiguió gracias a los reguladores de Francia y Alemania, que plantearon estas cuestiones con los negociadores de telecomunicaciones europeos que luego aplicaron estas soluciones completas y fáciles de usar a nivel mundial, a través de normas GSM.

Como resultado de la presión ejercida por las APD nacionales, la Directiva de privacidad electrónica incluye disposiciones en virtud de las cuales los suscriptores deben ser informados de cualquier intención de incluir sus datos (es decir, su número de teléfono fijo o móvil) en un ***directorio de suscriptores*** que esté disponible ***públicamente o sea accesible a través de los servicios de consulta de directorios***; y deben ser capaces de no ser incluidos en dichos directorios (es decir, para "ir ex-directorio"), sin cargo y sin tener que proporcionar razones (Art. 12(1) y (2)).[132]

Estos derechos se aplican a las personas físicas, pero los Estados miembros también deben hacer arreglos para garantizar que "los intereses legítimos de los suscriptores distintos de las personas físicas [es decir, de las 'personas jurídicas' como las empresas]" también estén "suficientemente protegidos" a este respecto (Art. 12 (4)).

Si se va a usar un directorio para "***cualquier otro propósito que no sea la búsqueda de datos de contacto de personas en base a su nombre y, cuando sea necesario, un mínimo de otros identificadores***", por ejemplo, si esos datos se van a usar para fines de mercadeo, evaluación del crédito[133] o campaña política: se debe solicitar a los suscriptores un consentimiento adicional, específicamente para el uso de sus datos para otros fines (Art. 12 (3)).[134]

**NUEVO* *Comunicaciones no solicitadas*

Como se señala en el punto 1.3.2, la Directiva de protección de datos de 1995 ya otorga a los interesados un **derecho** incondicional **a oponerse** al uso de cualquiera de sus datos personales con fines de marketing directo (Art. 14 (b) de la Directiva de 1995); es decir, marketing de cualquier tipo: comercial, político, etc. Actualmente, hace referencia por lo general al marketing por correo postal. La Directiva de privacidad electrónica agrega a esto un requisito de **consentimiento previo** para el uso de ***máquinas de llamadas automáticas y faxes***[135] para tales fines (Art. 13(1)). La razón es que el envío de mensajes a través de estos medios es mucho más barato que el uso del correo tradicional y, por tanto, es más probable que aumente su uso. Este requisito se aplica tanto a las personas físicas como a las personas jurídicas (personas y empresas, etc.). Además, tal como se indicó anteriormente en el apartado "Objetivo, propósito y alcance de la Directiva de privacidad electrónica", esta disposición se aplica a **cualquier entidad** que desee utilizar esos medios para enviar mensajes de marketing directos.

Sin embargo, si un cliente proporciona detalles de contacto electrónico (número de teléfono o dirección de correo electrónico, etc.) a una empresa en el contexto de una venta de un producto o servicio, el vendedor puede usar esos detalles para la **comercialización de sus propios productos o servicios** similares a un cliente de este tipo (denominado "**marketing de proximidad**"), siempre que se le proporcione un medio fácil de oponerse a tales acciones en cada comunicación (es decir, a menos que se ofrezca una "**exclusión**" de marketing adicional en cada comunicación) (Art. 13(2)).

Con respecto a otras formas de marketing directo (es decir, marketing directo no "próximo" por otros medios que no sean las máquinas de fax o llamadas automáticas o el correo electrónico), los Estados miembros pueden elegir entre un consentimiento previo (es decir, la opción de "*opt-in*" que se ofrece en el momento de recopilar los datos personales) y un ("fue informado pero no objetó ") modelo de "opt out - exclusión

---

[132] La batalla de las APD por estas protecciones tuvo lugar antes de que se adoptase la Directiva de telecomunicaciones de 1997. En Alemania se centraron en no tener que proporcionar razones para la exclusión de los directorios telefónicos. En Francia, la cuestión principal era que esto debería ser gratuito. Durante las negociaciones sobre la Directiva de telecomunicaciones, Francia estuvo a punto de abandonarla por ese motivo. De hecho, no estar incluido en un directorio telefónico se traducía en ese momento en un menor número de comunicaciones (por lo que se obtenían menos beneficios en una época en la que las llamadas telefónicas se pagaban de una en una), mientras que alrededor del 20% de los suscriptores pedían no estar incluidos en directorios telefónicos. Con el uso actual de internet, es aún más importante que no se moleste a los usuarios con llamadas telefónicas si se publican sus números.

[133] Cons. **"red-lining":** la práctica de otorgar un tratamiento diferencial en los préstamos, la vivienda, los seguros y otros servicios basados en la dirección de una persona y en el historial predeterminado de esas áreas, una práctica declarada ilegal en los Estados Unidos hace muchos años. Véase, p.e._
https://www.investopedia.com/terEstado Miembro/r/redlining.asp
También: Sobre cómo los efectos racistas del Redlining duraron décadas, NY Times, 24de agosto 2017, disponible en https://www.nytimes.com/2017/08/24/upshot/how-redlinings-racist-effects-lasted-for-decades.html (con mapas ilustrativos de esta práctica)

[134] La cuestión es si esto también se aplica a las "personas jurídicas", ya que este párrafo no se menciona en el cuarto párrafo del Artículo 12.

[135] Una "máquina de facsímiles" o "fax" es una máquina que permite que una imagen (a menudo una imagen de un documento) se envíe a través de una red telefónica. En estos días su uso es raro. Véase:
https://faxauthority.com/fax-history/

voluntaria"(art. 13(3)).[136] Sin embargo, el envío de mensajes de marketing directo por correo electrónico" disfraza u oculta la identidad del remitente en cuyo nombre se realiza la comunicación, o si dicha identidad se oculta y no se indica una dirección válida a la cual el destinatario puede enviar una solicitud para que dichas comunicaciones cesen, siempre debe estar prohibida (Art. 13(4)).

Derogaciones:

El artículo 15 de la Directiva sobre privacidad electrónica aclara que los Estados miembros pueden restringir los diversos derechos otorgados y las obligaciones impuestas por la directiva sobre la misma base que en la cláusula general de derogación de "**interés público importante**" en la Directiva principal de protección de datos de 1995 (art. 13), es decir, "cuando dicha restricción constituye una medida necesaria, apropiada y proporcionada dentro de una sociedad democrática para salvaguardar **la seguridad nacional** (es decir, la seguridad del Estado), la **defensa, seguridad pública y la prevención, investigación, detección y enjuiciamiento de delitos**" - a lo que la Directiva de privacidad electrónica simplemente añade: "O ***del uso no autorizado del sistema electrónico de comunicación***". Las palabras subrayadas están reforzadas en la Directiva de privacidad electrónica mediante la estipulación expresa adicional de que:

> Todas las medidas a las que se hace referencia en este párrafo se ajustarán a los principios generales del derecho comunitario, incluidos los mencionados en el artículo 6, apartados 1 y 2, del Tratado de la Unión Europea. (Art. 15(1), última frase)

Los artículos en el TUE a los que se refieren, respectivamente, a la Carta de los Derechos Fundamentales de la UE (anunciada en 2000, es decir, después de la entrada en vigor de la Directiva de Protección de Datos de 1995) y al Convenio Europeo de Derechos Humanos.

Si bien este es un reconocimiento expreso bienvenido del requisito fundamental, constitucional de la UE, de respetar los derechos y libertades fundamentales, por supuesto no es nuevo: los principios pertinentes del estado de derecho en la práctica (y en la ley) ya se aplicaron también en el momento de la adopción de la Directiva "madre", como "principios generales del derecho comunitario"[137]

> Los Estados miembros podrán, entre otras cosas, adoptar medidas legislativas que prevean la **retención de datos durante un período limitado** justificado por los motivos establecidos en el presente apartado. (Artículo 15(1), segunda frase)

Este texto original, con sus **limitaciones explícitas** del estado de derecho, que prohíbe efectivamente la **retención indiscriminada de datos,** es importante en vista de los intentos subsiguientes del legislador europeo para imponer precisamente dichas obligaciones indiscriminadas de retención de datos en virtud de la llamada Directiva de Retención de Datos, finalmente declarada nula por el Tribunal de Justicia, según lo discutido en 1.3.4, a continuación.

*DIFERENCIA ***Supervisión y aplicación***

Mientras que la aplicación de la Directiva de protección de datos de 1995 corrió a cargo de autoridades de protección de datos independientes y especializadas, que se han encargado también de la aplicación del RGPD, los Estados miembros de la UE podrían delegar la supervisión y la aplicación de la Directiva de privacidad electrónica en un organismo diferente, o incluso a varios organismos. Esto se ha traducido en la delgación de la supervisión en diferentes autoridades respecto a distintas cuestiones abordadas por la Directiva de privacidad electrónica en los Estados miembros.

La Comisión concluyó que la "delegación de competencias de aplicación a una amplia gama de autoridades que a veces se solapan" también parecía haber "[obstaculizado] la eficacia de las normas en casos tranfronterizos".[138]

---

[136] El modelo de "exclusión voluntaria" de la UE requiere que se informe al sujeto de los datos sobre: (i) la intención de utilizar sus datos para marketing directo; (ii) su derecho a optar por dicha comercialización; y (iii) detalles de cómo (simple y sin cargo) ejercer este derecho. Tenga en cuenta que el modelo europeo de "exclusión voluntaria" difiere fundamentalmente del de EE. UU., Que no requiere la información de los interesados en ninguno de estos detalles.

[137] Véase más arriga la nota a pie de página 66.

[138] *Ídem.*

Aplicación de otros elementos principales de la Directiva de protección de datos de 1995:

Finalmente, en esta descripción general de las normas de la Directiva sobre privacidad electrónica, se debe tener en cuenta que ésta estipula expresamente que los requisitos de la Directiva de 1995 con respecto a los recursos judiciales, la responsabilidad y las sanciones (que se detallan más arriba en la sección 1.3.2) también se aplicará en relación con la Directiva de privacidad electrónica (Art. 15(2)); que el Grupo de trabajo del Artículo 29 (también discutido en esa sección) llevará a cabo sus tareas según lo establecido en la Directiva de 1995 también en relación con la Directiva de privacidad electrónica (Art. 15(3)); y que los Estados miembros deben aplicar sanciones "eficaces, proporcionadas y disuasorias" por incumplimiento de la Directiva (Art. 15(a).

1.3.4. Instrumentos de protección de datos del tercer pilar.[139]

Entre mediados de los años noventa y 2009, la UE creó un número considerable de organismos destinados a facilitar la cooperación entre los Estados miembros en el ámbito de la policía y el Derecho penal ("Justicia y Asuntos de Interior" o JAI) -el denominado "tercer pilar" de la UE[140]-, todos ellos centrados en la creación de bases de datos personales paneuropeas y de normas y procedimientos para el acceso a dichas bases de datos por parte de los Estados miembros, así como para el intercambio de datos personales entre ellos.

Entre ellos figuraban Europol (1998), el Sistema de Información de Schengen, SIS-I (2001, actualizado a SIS II en 2013), Eurojust (2002), Eurodac (2003), el Sistema de Información de Visados, VIS (2004) y el Sistema de Información Aduanero, CIS (2009).

Durante este período, el Consejo adoptó unos 123 actos en el ámbito de la justicia y los asuntos de interior[141]. En 2005, siete Estados miembros firmaron el Convenio de Prüm y, mediante su Decisión de 23 de junio de 2008, el Consejo Europeo acordó integrar las principales disposiciones del Convenio de Prüm en el marco jurídico de la UE para permitir un intercambio más amplio (entre todos los Estados miembros de la UE) de datos biométricos (ADN y huellas dactilares) en la lucha contra el terrorismo y la delincuencia transfronteriza.

En 2008, el Consejo adoptó una Decisión marco global para establecer principios comunes de protección de datos personales en el ámbito JAI[142]. Sin embargo, aunque muchas de las normas de la Directiva Marco de 2008 se inspiraron en la Directiva 95/46/CE y en el Convenio del Consejo de Europa, como observó el entonces Supervisor Europeo de Protección de Datos, Peter Hustinx, "el nivel de protección era mucho más bajo en términos de alcance y sustancia"[143]. En cuanto al ámbito de aplicación, señaló que[144]:

> la Decisión sólo se aplica cuando los datos personales se transmiten o se ponen a disposición de otros Estados miembros y, por lo tanto, no se aplica al tratamiento "nacional"[es decir, el tratamiento efectuado por un Estado miembro y dentro de un Estado miembro], a diferencia de la Directiva 95/46/CE.

En 2009, tras la entrada en vigor del Tratado de Lisboa, que puso fin a la estructura de tres pilares[145], se inició

---

[139] For details of the law in this area, see the historical sections in the relevant chapters in: Steve Peers, (2016). EU Justice and Home Affairs Law: Volume I: EU Immigration and Asylum Law (Fourth Edition) and Volume II: EU Criminal Law, Policing, and Civil Law (Fourth Edition), both Oxford University Press, 2016.

[140] See footnote 58, above.

[141] See Emilio De Capitani, Metamorphosis of the third pillar: The end of the transition period for EU criminal and policing law, EU Law Analysis blogspot, 10 July 2014, available at: https://eulawanalysis.blogspot.com/2014/07/metamorphosis-of-third-pillar-end-of.html

[142] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30 December 2008, p. 60, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008F0977

[143] Peter Hustinx, EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, p. 15, available at: https://www.statewatch.org/news/2014/sep/eu-2014-09-edps-data-protection-article.pdf

[144] Idem, with reference to Recital 7 and Article 1 of the Framework Decision.

[145] See again footnote 58, above

un período transitorio de cinco años durante el cual el Derecho comunitario en materia de Justicia y Asuntos de Interior debía integrarse en el marco jurídico y constitucional supranacional adecuado de la UE (véase la sección 1.4.2)[146]. En 2018, la Decisión marco de 2008 fue sustituida por una nueva Decisión (ídem).

1.3.5 La protección de datos en el Segundo Pilar

Entre 1970 y 1993 se estableció un sistema informal para la "Cooperación de Política Europea" (CPE) en asuntos exteriores. El Tratado de Maastricht, que entró en vigor el pasado año, se formalizó en la "Política Exterior y de Seguridad Común" (PESC), el "segundo pilar" de la UE. Sin embargo, hasta el desarrollo ulterior de la PESC con arreglo al Tratado de Lisboa de 2009 (que abolió la estructura de "pilares")[147], como se expone en la sección 1.4.4, no existían normas específicas de protección de datos que se aplicaran al tratamiento de datos personales en este ámbito (aparte de las propias leyes de protección de datos de los Estados miembros y el Convenio del Consejo de Europa).

1.3.6 La protección de datos en las instituciones de la UE

No existían normas de protección de datos completas o coherentes aplicables a las propias instituciones de la UE hasta 2001, cuando un Reglamento (CE) nº 45/2001 introdujo por primera vez dichas normas, sobre la base del artículo 286 del TUE, de acuerdo a sus requerimientos[148].

Las normas de protección de datos del Reglamento de 2001 se basaban en las normas comunitarias sobre protección de datos que existían entonces y que se aplicaban a los Estados miembros, en particular la Directiva de protección de datos de 1995 y la Directiva sobre intimidad en las comunicaciones electrónicas de 2002.

El Reglamento 45/2001 también estableció la figura del Supervisor Europeo de Protección de Datos como una autoridad de supervisión independiente con la responsabilidad de supervisar el tratamiento de datos personales por parte de las instituciones y organismos comunitarios, y exigió la designación de un responsable de la protección de datos (RPD) por parte de cada una de dichas instituciones u organismos.
El Reglamento (CE) nº 45/2001 fue derogado por el Reglamento (UE) nº 2018/1725, que entró en vigor el 11 de diciembre de 2018, como se indica en la sección 1.4.5.

1.4 La Ley de protección de datos para el futuro

A finales de la primera década del siglo XXI, quedó claro que los instrumentos de protección de datos esencialmente del siglo XX, discutidos en la sección 1.3, arriba, ya no eran suficientes: habían sido concebidos y redactados antes del acceso masivo al Internet (o al menos la red mundial), computación ubicua (y móvil), "Big Data", "Internet de las cosas" (IoT), perfiles detallados, toma de decisiones algorítmica e "inteligencia artificial" (AI). Por lo tanto, se prepararon instrumentos de protección de datos, tanto en la UE como en el Consejo de Europa, nuevo o actualizado ("modernizado"), como se explica en esta sección.

1.4.1 El Reglamento General de Protección de Datos de la UE

La Comisión Europea propuso la adopción de un Reglamento general de protección de datos (RGPD) en 2012,[149] para enfrentar los desafíos planteados por las nuevas tecnologías y servicios. Consideró que la

[146] Véase el Protocolo 36 del Tratado de Lisboa y Emilio De Capitani, o.c. (nota 141).
[147] Véase también la nota 58.
[148] Reglamento (CE) nº 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 de enero de 2001, p. 1–22, disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32001R0045
[149] *Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos).*), COM (2012) 11 final, Bruselas, 25.01.2012, disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN
Al mismo tiempo, la Comisión también propuso un instrumento de protección de datos por separado, una Propuesta de Directiva sobre "la protección de las personas en relación con el tratamiento de datos personales por parte de las autoridades competentes con el fin de prevenir, investigar, detectar o tratar a los delincuentes. delitos o la ejecución de sanciones penales, y la libre circulación de dichos datos, (COM (2012) 10 final), pero esta directiva no se trata en este manual (Consulte la nota en el recuadro "Acerca de este manual", en la p. 1 del manual)

protección de datos sólida y de alto nivel era una condición esencial para ganar confianza en el entorno en línea, que a su vez es "*clave para el desarrollo económico*"; el nuevo y actualizado régimen de protección de datos de *la lex generalis* debía desempeñar *"un papel central en la Agenda Digital para Europa, y más en general en la Estrategia Europa 2020 "*.[150]

Los antecedentes, el estado y el enfoque y los elementos clave del RGPD se describen en detalle en la Parte Dos de este Manual. Basta con señalar aquí que el **RGPD amplía y refuerza significativamente los principios y reglas principales**; **añade** expresamente **datos genéticos y biométricos a la lista de datos sensibles** (esto se derivó del trabajo del Convenio del Consejo de Europa sobre protección de datos "modernizado", analizado a continuación, en el apartado 1.4.3); tiene como objetivo lograr una mayor armonización de la ley de protección de datos en los Estados miembros de la UE (al menos en las áreas donde se aplica, que en general es el área a la que anteriormente se hacía referencia como el "Primer pilar" de las Comunidades Europeas), en consonancia con la importante nueva jurisprudencia del Tribunal de Justicia, aunque sujeta a una amplia gama de "cláusulas de especificación" (es decir, disposiciones que dejan la regulación más detallada de determinadas cuestiones en manos de las leyes de los Estados miembros, dentro de los marcos generales de la RGPD, los tratados de la UE tal como los interpreta el TJCE y los propios sistemas constitucionales y jurídicos generales de los dichos Estados)[151]; permite una **cooperación transfronteriza mucho más estrecha** entre las agencias de protección de datos de los Estados miembros (APDs); y debe dar como resultado una **aplicación y cumplimiento mejores y más consistentes** de las reglas.

Más específicamente, como ya se señaló en la Introducción a este manual, el RGPD introduce (o al menos hace mucho más específico) el principio de "responsabilidad" en todos los estados miembros, y en muchos casos (incluso en relación a todas las autoridades públicas sujetas al Reglamento) ahora requiere la institución de responsables de la protección de datos nombrados por el responsable del tratamiento o por el encargado de la protección de datos(DPO).

Como se explica más detalladamente en la Parte Dos, los dos están vinculados: bajo el RGPD los DPD serán las personas que en la práctica deberán garantizar el cumplimiento del principio de responsabilidad por parte de las organizaciones a las que pertenecen y dentro de las mismas.

1.4.2 El Reglamento de privacidad electrónica de la UE propuesto

Aunque, como se señaló en la sub-sección anterior, uno de los principales objetivos de la propuesta de un RGPD era abordar los desafíos planteados por la **falta de confianza (en particular, la confianza del consumidor)** en el entorno en línea, la Comisión tardó otros cinco años en proponer un instrumento nuevo para reemplazar las reglas que son más específicamente relevantes para ese entorno, es decir, la Directiva de privacidad electrónica (Directiva 2002/58 / CE), discutida en la sección 1.3.4 anterior (que, por lo tanto, sigue vigente en cierta medida "huérfano").

Esto vino en forma de una propuesta publicada en enero de 2017, para reemplazar la Directiva de privacidad electrónica, también, con un reglamento, el **Reglamento de privacidad electrónico** propuesto.[152]

La propuesta aún se encuentra en las primeras fases del proceso legislativo: en el momento de redactar este documento (diciembre de 2018), todavía se estaba debatiendo internamente en el Consejo) y fue objeto de mucha atención por parte de ambos proponentes (grupos de libertades civiles, de consumidores y de derechos digitales) [153] y opositores (incluidos algunos de los principales "Gigantes de Internet" de EE. UU., que solicitan una retirada completa de la propuesta o su importante reducción).[154] Por lo tanto, es muy pronto

[150] Propuesta de un RGPD (nota ANTERIOR), pp. 1 – 2 (con los documentos sobre la Agenda Digital y la Estrategia Europa 2020). El sucesor de la Agenda Digital es el Mercado Único Digital) ("Estrategia DSM").
[151] Véase la segunda parte, sección 2.2, más adelante, bajo el subtítulo "... pero con "cláusulas de especificación".
[152] Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de datos personales en las comunicaciones electrónicas y por la que se deroga la Directiva 2002/58 / CE (Reglamento sobre la privacidad y las comunicaciones electrónicas), COM (2017) 10 final. , Bruselas, 10.01.2017, disponible en:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN
[153] Véase *Open letter to European member states on the ePrivacy reform*, enviada por un amplio grupo de organizaciones no-gubernamentales el 27 de marzo de 2018, disponible en:
https://edri.org/files/eprivacy/20180327-ePrivacy-openletter-final.pdf
[154] Véase: Corporate Europe Observatory, Shutting down ePrivacy: lobby bandwagon targets Council, 4 de junio, 2018, disponible en:
https://corporateeurope.org/power-lobbies/2018/06/shutting-down-eprivacy-lobby-bandwagon-targets- council

para discutir el reglamento propuesto aquí en detalle: sin duda, la versión final será, al menos en algunos aspectos, probablemente muy diferente de la propuesta.

Por lo tanto, para esta primera edición del Manual, será suficiente con presentar los **puntos clave de la propuesta de la Comisión**, tal como lo establece la propia Comisión:[155]

La propuesta de un reglamento sobre normas de alto nivel de privacidad para todas las comunicaciones electrónicas incluye:

- **Nuevos actores**: las reglas de privacidad [y protección de datos] también se aplicarán en el futuro a los nuevos actores [llamados "Over-The-Top" u OTT] que brindan servicios de comunicaciones electrónicas como WhatsApp, Facebook Messenger y Skype. Esto asegurará que estos servicios populares garanticen el mismo nivel de confidencialidad de las comunicaciones que los operadores de telecomunicaciones tradicionales.
- **Normas más estrictas**: todas las personas y empresas de la UE disfrutarán del mismo nivel elevado de protección de sus comunicaciones electrónicas a través de este reglamento directamente aplicable. Las empresas también se beneficiarán de un único conjunto de normas en toda la UE.[156]
- **Contenido y metadatos de comunicaciones**: la privacidad está garantizada para los metadatos y el contenido de las comunicaciones, por ejemplo, hora de una llamada y localización. Los metadatos tienen un alto componente de privacidad y deben anonimizarse o eliminarse si los usuarios no dieron su consentimiento, a menos que los datos sean necesarios para la facturación.[157]
- **Nuevas oportunidades de negocio**: una vez que se otorga el consentimiento para los datos de comunicaciones (contenido y/o metadatos) que se tratarán, los operadores de telecomunicaciones tradicionales tendrán más oportunidades para proporcionar servicios adicionales y desarrollar sus negocios. Por ejemplo, podrían producir mapas que indiquen la presencia de individuos; esto podría ayudar a las autoridades públicas y empresas de transporte en el desarrollo de proyectos de nuevas infraestructuras.
- **Reglas más simples para las cookies**: se simplificará la provisión de cookies, que ha resultado en una sobrecarga de solicitudes de consentimiento para los usuarios de Internet. La regla nueva será más fácil de usar, ya que la configuración del navegador proporcionará una forma fácil de aceptar o rechazar el seguimiento de cookies y otros identificadores. La propuesta también aclara que no se necesita consentimiento para que las cookies intrusivas no privadas mejoren la experiencia de Internet (por ejemplo, para recordar el historial del carrito de la compra) o las cookies utilizadas por un sitio web para contar el número de visitantes.
- **Protección contra el spam**: esta propuesta prohíbe las comunicaciones electrónicas no solicitadas por correo electrónico, SMS y máquinas de llamadas automáticas. Dependiendo de la legislación nacional, las personas estarán protegidas de forma predeterminada o podrán usar una lista de no llamar para no recibir llamadas de marketing.[158] Las personas que llaman de marketing deberán mostrar su número de teléfono o usar un prefijo especial que indique una llamada de marketing.
- **Aplicación más efectiva**: la aplicación de las normas de confidencialidad en el Reglamento será responsabilidad de las autoridades de protección de datos, que ya están a cargo de las normas en virtud del Reglamento general de protección de datos.

1.4.3. La Directiva de protección de datos de las fuerzas de seguridad de 2016 (LEDPD)

[155] https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation (en negrita en el original; no se han añadido las palabras entre paréntesis y en cursiva)

[156] Pero téngase en cuenta que esto dependerá de las reglas del Reglamento de privacidad electrónica que no contengan disposiciones "flexibles/ cláusulas de "especificación ", como las que se encuentran en el RGPD (Véase la Parte Dos, Sección 2.1, a continuación). Si el texto final del Reglamento de privacidad electrónica contuviera tales disposiciones "flexibles" (como es muy probable), sería crucial, especialmente para el entorno en línea, que es, por su propia naturaleza, transnacional, agregar una disposición de "ley aplicable".

[157] Pero ténganse en cuenta los intentos continuos de los Estados miembros y la Comisión para retener o reintroducir la retención obligatoria de comunicaciones electrónicas (metadatos): Véase Sección 1.3.4, más arriba.

[158] Esta es precisamente una disposición tan "flexible" como se menciona en nota 120, véase más arriba - e ilustra la necesidad de una regla de "ley aplicable" para aclarar cuál de las diferentes reglas nacionales se aplicará a los correos de marketing transfronterizos.

Introducción

El artículo 10, apartado 1, del Protocolo 36 del Tratado de Lisboa de 2009 preveía un período transitorio antes de que se aplicaran a los actos jurídicos de la UE en el ámbito de la cooperación policial y judicial en materia penal adoptados antes de la entrada en vigor del Tratado de Lisboa (el "*acervo del* antiguo tercer pilar") los plenos poderes de la Comisión y del Tribunal de Justicia. Esta fase de transición finalizó el 1 de diciembre de 2014.

En 2012, la Comisión presentó sus propuestas de directiva en este ámbito, junto con su propuesta de Reglamento general de protección de datos (que se ha introducido en la sección 1.4.1, y se ha debatido con más detalle en la segunda parte de este manual).[159] Sin embargo, al igual que el GDPR, la Directiva de protección de datos de las fuerzas de seguridad, el LEDPD (también conocida como la "Directiva de aplicación de la ley", el LED, la "Directiva de policía de protección de datos", o incluso como la "Directiva de policía") no se adoptó hasta 2016, el mismo día que el RGPD.[160] A diferencia del RGPD que, como reglamento, es en principio directamente aplicable en los ordenamientos jurídicos de los Estados miembros (aunque, en ese caso, con un número significativo de cláusulas que, de hecho, aún necesitan una mayor "especificación" en la legislación nacional),[161] el LEDPD, como directiva, no se aplica directamente (es decir, no tiene un "efecto directo"), sino que más bien **debe "transponerse" a la legislación nacional**. Esto debía hacerse en un plazo de dos años a partir de la entrada en vigor formal de la Directiva, es decir, antes del 6 de mayo de 2018 (sólo unas semanas antes de que el RGPD entrara en vigor, el 25 de mayo de ese año).

Obsérvese, sin embargo, que los largos períodos de aplicación previstos en los artículos 61 a 63 de la Directiva, debido a las diferentes circunstancias que rodean al gran número de operaciones de tratamiento de datos implicadas, que se tratarán brevemente al final de esta sección sobre el DIPD, bajo el epígrafe "*Retraso en la transposición*".

A este respecto, basta con tener en cuenta las principales características y requisitos del LEDPD.[162]

Una directiva en lugar de una decisión marco del Consejo

El primer punto que hay que señalar es que el establecimiento de las normas para el tratamiento de datos personales en una directiva es en sí mismo una **mejora significativa** con respecto a su inclusión en una Decisión marco del Consejo como la de 2008 revocada por el LEDPD.[163] Como directiva, puede ser invocada ante los tribunales nacionales (y, en última instancia, ante el Tribunal de Justicia) por los particulares en acciones contra el Estado, y está sujeta a los poderes de ejecución de la Comisión, que tienen por objeto garantizar que dichos instrumentos se transponen correctamente al Derecho nacional.

Alcance del LEDPD

i. Actividades cubiertas

En relación con el ámbito de aplicación, el LEDPD estipula lo siguiente:

Ámbito de aplicación

1. La presente Directiva se aplica al tratamiento de datos personales por las autoridades competentes[con fines de prevención, investigación, detección o

---

[159] Véase arriba la nota 149.

[160] 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 las autoridades competentes para la prevención, investigación, detección y enjuiciamiento de delitos o la ejecución de sanciones penales, y a la libre circulación de estos datos, y por la que se deroga la Decisión marco 2008/977/JAI* del Consejo, DO L 119 de 4 de mayo de 2016, pp. 89-131, disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG
La Directiva entró formalmente en vigor el día siguiente a su publicación en el Diario Oficial, es decir, el 5 de mayo de 2016, pero, como se señala en el texto, sólo tuvo que aplicarse en la práctica (mediante su transposición al Derecho interno de los Estados miembros) dos años después de esa fecha, es decir, el 6 de mayo de 2018.

[161] Véase la segunda parte, sección 2.2., más adelante.

[162] Como se explica al principio de este manual, esperamos ampliar la legislación de protección de datos de la UE fuera del RGPD en una segunda edición. Esto ampliaría, en particular, las normas del LEDPD que sólo se resumen brevemente a continuación.

[163] Véase Steve Peers, The Directive on data protection and law enforcement: ¿Una oportunidad perdida? Statewatch Analysis blog, abril de 2012, disponible en: https://www.statewatch.org/analyses/no-176-leas-data%20protection.pdf

enjuiciamiento de delitos o de ejecución de sanciones penales, incluida la protección y la prevención de amenazas a la seguridad pública].

2. La presente Directiva se aplicará al tratamiento total o parcialmente automatizado de datos de carácter personal, así como al tratamiento no automatizado de datos de carácter personal que formen parte de un fichero o estén destinados a formar parte de un fichero.

3. La presente Directiva no se aplicará al tratamiento de datos personales:

   (a) en el ejercicio de una actividad que no esté comprendida en el ámbito de aplicación del Derecho de la Unión;

   (b) por las instituciones, órganos y organismos de la Unión.[164]

En el seno de una "autoridad competente", las demarcaciones precisas entre el tratamiento de datos sujeto a la Directiva sobre desplazamiento de personas y los sujetos a la Directiva sobre desplazamiento de personas deben evaluarse teniendo en cuenta el considerando (12). Esto deja claro, en su última frase, que el tratamiento de datos personales en relación con "*otras tareas*" confiadas a las "autoridades competentes", que "*no se llevan a cabo necesariamente con fines de prevención, investigación, detección o enjuiciamiento de delitos, incluida la protección contra las amenazas a la seguridad pública y la prevención de las mismas*", está sujeto al RGPD y no al LEDPD.

El responsable del tratamiento deberá prestar especial atención a esta delimitación y a otras cuestiones, como la medida en que la recogida y el tratamiento ulterior de datos personales en relación con "incidentes" en los que *todavía no está claro* si se ha producido algún delito, o en relación con la adopción de medidas (incluidas las "*medidas coercitivas*") en manifestaciones o grandes acontecimientos deportivos que "*puedan dar lugar a un delito*" (*o no*), están sujetos al LEDPD, ya que las respuestas a estas preguntas tienen una repercusión importante en el nivel de protección de datos que debe garantizarse, por ejemplo, en los siguientes casos en términos de información a los interesados, limitaciones de conservación de datos, restricciones de los derechos de los interesados, etc. Mientras tanto, los responsables de la protección de datos que trabajan en el seno de las autoridades competentes deberían tratar de ayudar a las autoridades a tomar estas decisiones, con vistas a garantizar unos niveles adecuados de protección de datos en todos los contextos.

El concepto de "**seguridad pública**" se suele utilizar en el contexto de las excepciones a la legislación de la UE, es decir, para indicar los motivos que pueden utilizarse para justificar una actividad que, de otro modo, constituiría una infracción del Derecho de la Unión. Como señala Koutrakis, "l*a seguridad pública constituye un motivo de excepciones a las cuatro libertades en virtud de las normas primarias de la Unión* "[165]Citando un documento informativo elaborado a petición de la Comisión IMCO del Parlamento Europeo:[166]

> De todos los motivos de excepción a la libre circulación, la **seguridad pública está estrechamente relacionada con lo que tradicionalmente se ha entendido como el núcleo de la soberanía nacional, es decir, la esfera de actividad en la que el Estado tiene la responsabilidad primordial de proteger su territorio y a sus ciudadanos**. (énfasis añadido)

La principal **sentencia del CJEU** sobre la cuestión de la "seguridad pública" es el *caso Campus Oil*,[167] en el

[164] El tratamiento por parte de los órganos, oficinas y organismos de la UE con fines de prevención, detección, investigación y enjuiciamiento de delitos está sujeto a una serie de normas especiales, contenidas en el capítulo IX del nuevo Reglamento sobre el tratamiento de datos personales por las instituciones de la UE (etc.), el Reglamento (UE) 2018/1725, tal como se expone brevemente en la sección 1.4.5, a continuación.

[165] Panos Koutrakis, Public Security Exceptions and EU Free Movement Law, in: Koutrakos, P., Nic Shuibhne, N. and Sypris, P. (Eds.), Excepciones a la Ley de Libre Circulación de la UE, 2016 (pp. 190-217), p.2, disponible en:
http://openaccess.city.ac.uk/16192/
(Con referencia a los Arts. 36 (Bienes), 45(3) y 52 (Personas), 62 (Servicios) y 65 TFUE (Capital)).

[166] Excepción de seguridad pública en el ámbito de los datos no personales en la Unión Europea, documento informativo solicitado por la Comisión IMCO del Parlamento Europeo y preparado por Kristina Irion, PE. 618.986, abril de 2018, p. 3, disponible en:
https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/618986/IPOL_BRI(2018)618986_ES.pdf

[167] Sentencia del Tribunal de 10 de julio de 1984, *Campus Oil Limited y otros/Ministerio de Industria y Energía y otros*, asunto 72/83, Rec. 1984 -02727, disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:61983CJ0072rom=EN

que el Tribunal sostuvo que una medida nacional -*en el caso concreto*, un contingente nacional de aprovisionamiento de petróleo refinado en la República de Irlanda- estaba justificada porque se consideraba el petróleo refinado:

> **de importancia fundamental para la existencia de un país**, ya que de ellos dependen no sólo sus servicios, sino sobre todo sus instituciones, sus servicios públicos esenciales e incluso la supervivencia de sus habitantes. (párr. 34, cursiva añadida)

Esto deja claro que, por **un lado, el término "seguridad pública", tal como se utiliza en la legislación de la UE, no se limita a cuestiones relacionadas con la actividad delictiva, sino que se extiende a cuestiones como la protección de los "servicios públicos esenciales" y las medidas destinadas a garantizar "la supervivencia de los habitantes[de un país]"; pero, por otro lado, no es tan amplio como el término "orden público", un término que se utiliza a menudo en la legislación policial para referirse a cuestiones como el mantenimiento del orden en las manifestaciones, las manifestaciones, los desfiles y las festividades.[168] Más bien, como dice el Consejo, la cuestión a proteger debe estar relacionada con:[169]**

> **una amenaza real y suficientemente grave que afecte a uno de los intereses fundamentales de la sociedad, como una amenaza para el funcionamiento de las instituciones y los servicios públicos esenciales y la supervivencia de la población, así como un riesgo de perturbación grave de las relaciones exteriores o de coexistencia pacífica de las naciones, o un riesgo para los intereses militares.**

La evaluación de los límites precisos de lo que está y lo que no está cubierto por las amenazas (¿criminales?) a la "seguridad pública" plantea cuestiones difíciles de evaluar en circunstancias específicas. ¿Cuándo un desorden público -por ejemplo, una interrupción de los vuelos de personas que se manifiestan en contra de la expulsión forzada de solicitantes de asilo- equivale a una "amenaza para un servicio público esencial"?[170] ¿Y cuándo es un riesgo de "perturbación de las relaciones exteriores" - por ejemplo, una manifestación contra una visita de Estado de un jefe de Estado extranjero- lo suficientemente "serio" para ser clasificado como un riesgo para la seguridad pública? Sin embargo, las respuestas a estas preguntas determinan si el LEDPD se aplica o no a cualquier tratamiento de datos personales en relación con tales acciones.

Si bien muchas entidades -en particular las del sector público, como las autoridades locales o los organismos de protección del medio ambiente, el bienestar social o el bienestar de los animales- tienen atribuidas algunas autoridades públicas y algunos poderes públicos en relación con (ciertos) delitos y (ciertas) amenazas a la seguridad pública, las principales tareas de esas autoridades no estarán relacionadas con la investigación (etc.) de delitos dentro de sus competencias pertinentes, ni con las amenazas al orden público (tanto si se trata de delitos como si no).

Los responsables de la protección de datos de dichas autoridades u organismos públicos deberían examinar detenidamente hasta qué punto puede decirse que el tratamiento de datos personales por su propia organización u organizaciones está sujeto al RGPD, y hasta qué punto está sujeto al LEDPD. A menudo no será una cuestión fácil de aclarar, por lo que el RPD debería trabajar en ello junto con el responsable del tratamiento, el servicio jurídico pertinente y la autoridad de supervisión competente. Por otra parte, los datos personales tratados en operaciones de tratamiento que estén sujetas al DIPD tendrán que mantenerse generalmente separados de los datos personales tratados en operaciones sujetas al RGP, con normas y políticas específicas sobre cuándo los datos personales de una categoría o para un fin pueden utilizarse en otra categoría o para otro fin.[171]

---

[168] Cf., e.g.:
http://www.lokalepolitie.be/5371/contact/diensten/20-handhaving-openbare-orde (en holandés)

[169] Consejo de la Unión Europea, expediente interinstitucional: 2017/0228 (COD), considerando (12 bis), página 3, disponible en: http://www.consilium.europa.eu/media/32307/st15724-re01en17.pdf

[170] En el Reino Unido, hubo controversia sobre el enjuiciamiento y la condena de precisamente esos manifestantes en virtud de la legislación antiterrorista -es decir, en virtud de la ley de "seguridad pública"- en lugar de en virtud de la ley penal normal de allanamiento de morada, véase: https://www.theguardian.com/global/2019/feb/06/stansted-15-rights-campaigners-urge-judge-to-show-leniency
El caso es objeto de un recurso de apelación.

[171] Véase también el análisis que figura en el apartado 1.4.6, más adelante, sobre los intercambios de datos personales entre las diferentes entidades que trabajan en los diferentes regímenes de protección de datos de la UE.

Por último, se plantea un problema en relación con la frontera entre las actividades de los Estados miembros de la UE en el ámbito de la "*prevención, investigación, detección o enjuiciamiento de delitos*" y la "*protección y prevención de amenazas a la seguridad pública*", por una parte, y las actividades de los Estados miembros en materia de **seguridad nacional**, y las actividades de los organismos o unidades de los Estados miembros que se ocupan de cuestiones de seguridad nacional, por otra. Las líneas divisorias entre estos dos ámbitos de actividad -la primera nominalmente plena dentro de la UE, la segunda formalmente inexistente en su totalidad- son cada vez más borrosas (especialmente en relación con categorías de "terrorismo", "ciberdelincuencia", "ciberseguridad", etc.)[172] no muy definidas con precisión. De hecho:[173]

> En algunos países, los propios organismos se están convirtiendo en híbridos, con el doble papel de luchar contra la delincuencia y proteger la seguridad nacional. La Oficina Federal de Investigaciones de los Estados Unidos (FBI) es un buen ejemplo[174], pero también en el Reino Unido, Comunicaciones colabora cada vez más estrechamente con los organismos encargados de hacer cumplir la ley.[175]

Esta cuestión no puede discutirse en detalle aquí, pero se abordará más adelante en la sección 1.4.6, sobre las transmisiones de datos personales por parte de un responsable del tratamiento en un ámbito cubierto por una categoría de la legislación de protección de datos de la UE, a un responsable del tratamiento sujeto a otra categoría de legislación de la UE o, en el caso de las agencias nacionales de seguridad, no sujeto a la legislación de la UE en absoluto.

Por otra parte, la distinción entre el tratamiento de datos personales cubiertos por el LEDPD y el tratamiento de datos personales por parte de las instituciones, órganos y organismos de la UE es clara, y este último está cubierto por un nuevo reglamento adoptado en 2018, como se explica en la sección 1.4.6, más adelante.

ii. Entidades cubiertas

También en relación con la cuestión del ámbito de aplicación, el LEDPD define a las "**autoridades competentes**" a que se refiere el artículo 1, apartado 1, como:

> (a) cualquier autoridad pública competente para la prevención, investigación, detección o enjuiciamiento de delitos o la ejecución de sanciones penales, incluida la protección contra las amenazas a la seguridad pública y la prevención de las mismas; o
>
> (b) cualquier otro organismo o entidad al que la legislación de un Estado miembro encomiende el ejercicio de la autoridad y los poderes públicos con fines de prevención, investigación, detección o enjuiciamiento de delitos o de ejecución

---

[172] Douwe Korff, Ben Wagner, Julia Powles, Renata Avila y Ulf Buermeyer, Límites del Derecho: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes, informe comparativo que cubre Colombia, RD Congo, Egipto, Francia, Alemania, India, Kenia, Myanmar, Pakistán, Rusia, Sudáfrica, Turquía, Reino Unido y Estados Unidos, preparado para la Fundación World Wide Web, enero de 2017, en particular la sección 2.3.1, disponible en: https://ssrn.com/abstract=2894490

[173] *Idem*, p. 27. La ampliación del papel de la policía a la acción "preventiva" no es nueva. Véase Ian Brown y Douwe Korff, Privacy & Law Enforcement, FIPR study for the UK Information Commissioner, 2005, Paper No. 4, The legal framework, section 3.1. Los acontecimientos más recientes, en particular en relación con la difuminación de las líneas divisorias entre la actuación policial y las actividades relacionadas con la seguridad nacional, figuran en Douwe Korff, Protecting the right to privacy in the fight against terrorism, Issue Paper written for the Commissioner for Human Rights of the Council of Europe, 2008, disponible en: https://wcd.coe.int/ViewDoc.jsp?Ref=CommDH/IssuePaper(2008)3

[174] Una página en el sitio web del FBI sobre "*Abordar las amenazas a la ciberseguridad de la nación*" señala expresamente que el FBI está encargado tanto de proteger la seguridad nacional de los EE.UU. como de ser el principal organismo de aplicación de la ley de la nación, añadiendo que "*estas funciones son complementarias, ya que las amenazas a la ciberseguridad de la nación pueden emanar de los Estados-nación, las organizaciones terroristas y las empresas delictivas transnacionales, y las líneas divisorias entre ellas a veces se difuminan*". "Ver: www.fbi.gov/about-us/investigate/cyber/addressing-threats-to-the-nations-cybersecurity

El FBI ha cambiado recientemente una hoja informativa para describir su "*función principal*", que ya no es la de "*hacer cumplir la ley*", sino la de "*seguridad nacional*". Véase The Cable, 5 de enero de 2014, en: http://thecable.foreignpolicy.com/posts/2014/01/05/fbi_drops_law_enforcement_as_primary_mission #sthash.4DrWhlRV.dpbs

Para los peligros inherentes a la borrosidad de las líneas, véase: www.foreignpolicy.com/articles/2013/11/21/the_obscure_fbi_team_that_does_the_nsa_dirty_work

nota original]

[175] Ver Computer Weekly, "*GCHQ and NCA join forces to police dark web*", 9 Nov 2015, en: http://www.computerweekly.com/news/4500257028/GCHQ-and-NCA-join-forces-to-police-dark-web -[nota original]

> de sanciones penales, incluida la protección contra las amenazas a la seguridad pública y la prevención de las mismas.
>
> (Apartado 7 del artículo 3)

Como ya se ha señalado, esto puede extenderse mucho más allá de la policía y otros organismos de primera línea encargados de la aplicación de la ley, para incluir, dependiendo del enfoque constitucional nacional, organismos públicos locales y regionales, organismos de bienestar, salud y seguridad, organismos de supervisión de las instituciones financieras, de bienestar animal o del medio ambiente, organismos aduaneros y tributarios, y muchos más, siempre que se les conceda "*autoridad pública y poderes públicos*" en relación con delitos o amenazas a la seguridad pública que puedan implicar actividades delictivas que tengan lugar dentro de su ámbito de competencia.

Como ya se ha señalado, el tratamiento de datos personales por parte de dichos organismos en relación con actividades no relacionadas con asuntos penales está sujeto al RGPD y no al LEDPD, y lo mismo puede ocurrir con el tratamiento de datos personales por parte de dichas autoridades en relación con amenazas a la seguridad pública que no impliquen delitos penales, como tormentas, inundaciones o epidemias, o con la gestión de acontecimientos deportivos que no estén relacionados con posibles actos delictivos.

iii. Operaciones de tratamiento cubiertas

Por lo que se refiere a los medios utilizados para el tratamiento, el LEDPD se aplica, al igual que los demás instrumentos de protección de datos de la UE:

> el tratamiento total o parcialmente automatizado de datos de carácter personal, así como el tratamiento no automatizado de datos de carácter personal que formen parte de un fichero o estén destinados a formar parte de un fichero.

En otras palabras, el DIPD se aplica a **todo tratamiento automatizado de datos de carácter personal** y al tratamiento de todos los datos de carácter personal contenidos en **ficheros manuales estructurados** que se encuentren dentro de su ámbito de aplicación en cuanto a actividades y entidades cubiertas.

Es importante señalar que, a diferencia de la Decisión marco de 2008 anteriormente mencionada, en la sección 1.3.6, **el LEDPD se aplica** no sólo a los datos personales que se intercambian entre los Estados miembros, sino **también al tratamiento nacional de datos personales con fines policiales**. Como señala la Comisión, la Directiva debería, por consiguiente, "*facilitar la cooperación entre las autoridades policiales y judiciales de toda la UE*".[176]

Libre circulación de datos entre autoridades competentes de diferentes Estados miembros

Aunque la Directiva "*no impedirá que los Estados miembros ofrezcan garantías superiores a las establecidas en la presente Directiva*" (artículo 1, apartado 3), ningún Estado miembro que establezca normas más estrictas podrá invocarlas para "**restringir o prohibir**" el libre intercambio de datos personales entre Estados miembros, que es el objetivo mismo de la Directiva (artículo 1, apartado 2, letra b))). Por otra parte, si un Estado miembro, en su legislación, establece "**condiciones** específicas" para determinados tratamientos (por ejemplo, para la elaboración de perfiles) o, presumiblemente, para el tratamiento de determinados tipos de datos (por ejemplo, datos biométricos), entonces ese Estado miembro no sólo puede, sino que también debe ("deberá"):

> establecer que la autoridad competente que transmita los datos personales informe al destinatario de los mismos de dichas condiciones y de la obligación de cumplirlas.
> (Art. 9(3))

Sin embargo, los Estados miembros no pueden, en virtud de esta disposición, imponer condiciones a los destinatarios de otro Estado miembro que estén implicados en asuntos judiciales o policiales, salvo las que impongan en "transmisiones similares" a destinatarios nacionales de este tipo (apartado 4 del artículo 9).

[176] Comisión Europea, Ficha técnica - ¿Cómo ayudará la reforma de la protección de datos a combatir la delincuencia internacional? 30 de abril de 2018, disponible en: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en (Seguir enlace)

(Sobre la cuestión de las transferencias de datos personales a países no pertenecientes a la UE, véase más adelante bajo este epígrafe.)

Contenido

Muchas de las disposiciones del LEDPD son muy similares a las del RGPD, pero sólo hasta cierto punto, para reflejar el contexto especial de la aplicación de la ley y la prevención de amenazas criminales a la seguridad pública.

Las **definiciones** de los conceptos básicos del artículo 3 - "*datos personales*", "*tratamiento*", "*restricción del tratamiento*", "*elaboración de perfiles*, "*pseudonimización*", "*fichero*", "*responsable del tratamiento*", *"encargado del tratamiento*", "*destinatario*", "*violación de los datos personales*", "*datos genéticos*", "*datos biométricos*", "*datos relativos a la salud*"- son idénticas en la práctica a las definiciones de esos mismos conceptos en el RPDG.[177]

Los **principios básicos**, establecidos en el artículo 4, son también similares. En particular, el principio de **"legalidad**" -que no figuraba en la Decisión marco de 2008-se incluye ahora expresamente en el artículo 4, letra a), y se desarrolla en el artículo 8, apartado 1, con el principio de "transparencia" (que está directamente relacionado con el principio de legalidad y equidad en el RBPI), reflejado en cierta medida en el artículo 8, apartado 2 ("*la legislación de los Estados miembros que regule el tratamiento en el ámbito de aplicación de la presente Directiva especificará al menos los objetivos del tratamiento"), los datos personales que deben tratarse y las finalidades del tratamiento*") y en las disposiciones relativas a la información de los interesados y a la concesión del acceso a sus datos (si bien en el contexto especial del DIPD estos derechos están sujetos a restricciones más amplias).

El **principio de limitación de la finalidad está limitado** en el sentido de que los datos personales recogidos por cualquiera de las autoridades competentes antes mencionadas con fines policiales o de seguridad pública **pueden utilizarse para cualquier otro fin, siempre que esté "*autorizado por el Derecho de la Unión o de los Estados miembros***" (primera frase del apartado 1 del artículo 9), a reserva de lo dispuesto en la segunda frase del apartado 1 del artículo 9:

> Cuando se traten datos personales para otros fines, se aplicará el Reglamento (UE) 2016/679[el RGPD], a menos que el tratamiento se lleve a cabo en una actividad que quede fuera del ámbito de aplicación del Derecho de la Unión.[178]

De ello se deduce que cualquier dato policial puesto a disposición en virtud de dicha "ley de autorización" debe seguir limitándose a lo que es "pertinente" y "necesario" para el propósito "legítimo" perseguido por la ley de autorización. **En principio, los RPD que actúan en nombre de las entidades reveladoras y receptoras desempeñan un papel importante en este ámbito.** Sin embargo, en algunos países la ley puede simplemente estipular que, en determinadas circunstancias específicas (por ejemplo, cuando un funcionario de alto nivel lo autorice), determinados datos de las fuerzas del orden deben ponerse a disposición de los organismos no encargados de la aplicación de la ley.[179]

La Directiva exige a los Estados miembros que establezcan **límites de retención de datos** para los datos tratados en virtud de la Directiva (artículo 5); y que **establezcan distinciones claras** entre los datos personales de diferentes **categorías de interesados**, como sospechosos, personas condenadas por un delito penal, víctimas, testigos, etc. (Art. 6); y estipula que "*los Estados miembros dispondrán que los datos personales basados en hechos se distingan, en la medida de lo posible, de los datos personales basados en valoraciones personales*" (Art. 7(1)).

---

[177] Curiosamente, aunque todas las definiciones mencionadas anteriormente se presentan en términos esencialmente idénticos a los del RGPD, el LEDPD no define "tercero", aunque otra definición (de "destinatario") menciona expresamente a terceros.

[178] Véase también el apartado 2 del artículo 9. Esto se discute de nuevo en la subsección 1.4.6, más adelante.

[179] Cf. la discusión del (entonces propuesto) amplio intercambio de datos sobre menores en el Reino Unido entre las autoridades de bienestar social, educativas y policiales en Ross Anderson *et al*: A Report for the Information Commissioner (Informe para el Comisario de Información), preparado por la Foundation for Information Policy Research (FIPR) del Reino Unido, 2006, que incluye resúmenes de Douwe Korff no sólo de las normas legales de protección de datos relevantes en el Reino Unido (*Data Protection Rules and Principles Relating to Data Sharing*, pág. 100 y ss.), sino también (en un apéndice) una visión general de *Regulation Elsewhere in Europe*, específicamente en Alemania y Francia, disponible en:
https://www.cl.cam.ac.uk/~rja14/Papers/kids.pdf

El LEDPD también (al igual que el RGPD) exige que los controladores adopten una **seguridad "avanzada"**, teniendo en cuenta el contexto y los objetivos, etc., del tratamiento (apartado 1 del artículo 29), y debe llevar a cabo una **evaluación del riesgo** a este respecto, con el fin de determinar qué nivel de seguridad es adecuado (apartado 2 del artículo 29). También (de nuevo como el RGPD) requiere seguridad física y técnica (*ídem*) y la imposición de **deberes de confidencialidad** al personal (Art. 23).

También similar al RGPD, **las violaciones de datos personales** deben ser comunicadas a la autoridad supervisora en un plazo de 72 horas (o si no se hacen dentro de ese plazo, el retraso debe ser justificado) (Art. 30); y los interesados deben ser informados de ellas "*sin demora*", "*cuando la violación de los datos personales pueda dar lugar a un alto riesgo para los derechos y libertades de las personas físicas*" (Art. 31).

Las normas del LEDPD sobre el tratamiento de **datos sensibles** -es decir, de "datos que revelen el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas o la pertenencia a un sindicato", los datos genéticos, los datos biométricos (cuando se utilizan para identificar de manera única a una persona física), los "datos relativos a la salud" y los "datos relativos a la vida sexual o a la orientación sexual de una persona física"- se enmarcan de manera algo diferente a las del RGPB (art. 9), en la medida[180] en que el LEDPD permite el tratamiento de dichos datos:

> **únicamente** cuando **sea estrictamente necesario**, con sujeción a las **garantías adecuadas** de los derechos y libertades de la persona a la que se refieren los datos, y únicamente:
>
> (a) cuando así lo **autorice** la **legislación de la** Unión o de un Estado miembro;
>
> (b) para proteger los **intereses vitales** del interesado o de otra persona física; o
>
> (c) cuando el tratamiento se refiera a datos que **el interesado haya hecho manifiestamente públicos**.
>
> (Art. 10 LEDPD, con cursiva añadida)

Las dos últimas condiciones corresponden a excepciones en el RGPD (respectivamente, Art. letras c) y e) del apartado 2 del artículo 9).[181]

Cuando un Estado miembro se base en la otra condición -la **autorización** legal- debe poder demostrar que el tratamiento de datos es "***estrictamente necesario***" y que cualquier limitación relacionada con los derechos del interesado está "***sujeta a las garantías adecuadas***". Además (a diferencia de lo que ocurre con la Decisión marco del Consejo de 2008), los particulares pueden ahora confiar en la Directiva para hacer valer sus derechos, ya que, en última instancia, el Tribunal de Justicia de la UE puede determinar si alguna de las leyes nacionales adoptadas en este contexto cumple la norma de "*necesidad estricta*" e incorpora las "*salvaguardias adecuadas*", y la Comisión está facultada para adoptar medidas de ejecución si considera que la legislación de un Estado miembro por la que se autoriza el tratamiento de datos sensibles con fines policiales o de seguridad pública no cumple esas normas.

El LEDPD también, al igual que el RGPD, regula la **toma de decisiones automatizada, incluida la elaboración de perfiles**, pero con algunas diferencias. Concretamente, establece que dicho tratamiento debe estar "*autorizado por la legislación de la Unión o de los Estados miembros*" y sujeto a las "*garantías adecuadas*", que deben incluir "al *menos el derecho a obtener la intervención humana por parte del responsable del tratamiento*". Sin embargo, a diferencia del RGPD, el LEDPD no estipula que, cuando existe tal "intervención humana", el interesado debería poder "*expresar su punto de vista y... impugnar la decisión[automatizada/basada en perfiles]*".

---

[180] Es comprensible que el LEDPD no contenga una disposición similar a la primera frase del artículo 10 del RGPD, que estipula que el tratamiento de datos personales relativos a condenas y delitos penales debe estar "*bajo el control de la autoridad oficial o autorizado por la legislación de la Unión o de los Estados miembros que prevea las garantías adecuadas para los derechos y libertades de las personas a las que se refieren los datos*": el LEDPD y las propias legislaciones nacionales pertinentes así lo garantizan. Del mismo modo, no es necesario repetir en el LEDPD la disposición de la última frase del artículo 10 del RD-PIB, según la cual "*todo registro completo de condenas penales se llevará únicamente bajo el control de la autoridad oficial*".

[181] Salvo que la excepción relativa al tratamiento para proteger los intereses vitales del interesado o de otra persona con arreglo al artículo 9, apartado 2, letra c), del RGPD sólo se aplica si "el interesado es física o jurídicamente incapaz de dar su consentimiento", lo que no se exige en el marco de la Directiva sobre productos derivados de la madera.

En particular, el LEDPD afirma que:

> De conformidad con el Derecho de la Unión, se **prohibirá la elaboración de perfiles que den lugar a discriminación contra las personas físicas sobre la base de las categorías especiales de datos personales a que se refiere el artículo 10.** (énfasis añadido)

En relación con la cuestión de la "autorización por ley", también es importante tener en cuenta que la **autoridad de protección de datos** del Estado miembro pertinente **debe ser consultada** durante la elaboración de la propuesta legislativa sobre estas cuestiones (art. 28.2).

Las OPD de las autoridades competentes deben examinar detenidamente la cuestión de cómo estos nuevos e importantes requisitos del DIPD -la intervención humana y el deber de no discriminación- pueden aplicarse real y eficazmente en la práctica en diferentes contextos.

Dado su ámbito de aplicación, el LEDPD permite **limitaciones** bastante amplias de los **derechos del interesado** a ser informado del tratamiento, a tener acceso a sus datos y a rectificar o suprimir los datos que no cumplan las normas pertinentes de calidad de los datos o que se traten de otro modo contraviniendo las normas establecidas en el instrumento, pero dichas limitaciones deben limitarse a lo que es "necesario" y "proporcionado" en una sociedad democrática (véanse los artículos 12 a 16 del LEDPD y el artículo 15, en particular). El LEDPD también permite que el ejercicio de estos derechos se ejerza **indirectamente**, a través de la autoridad supervisora pertinente (art. 17). Cuando los datos personales "estén *contenidos en una resolución judicial o en un expediente o expediente procesado en el curso de investigaciones y procedimientos penales*", los derechos también pueden estar regulados por la legislación nacional pertinente (art. 18). Por lo general, las **leyes policiales** o los **códigos de procedimiento penal** regulan el acceso de los sospechosos, acusados, acusados, acusados o condenados a determinadas partes de los expedientes pertinentes, en determinadas fases de los procedimientos (por lo general, permitiendo un acceso limitado en las fases iniciales y un amplio acceso más adelante, especialmente una vez que la persona ha sido acusada formalmente), por lo que esas disposiciones pueden mantenerse.

Requisitos prácticos y formales

También en muchos otros aspectos, el LEDPD introduce requisitos prácticos y formales similares al RGPD.
En particular, es muy importante que el LEDPD, al igual que el RGPD, incluya el nuevo "**principio de responsabilidad**" (apartado 4 del artículo 4)[182] y exija que, "*teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de que los derechos y libertades de las personas físicas sean más o menos probables y más o menos graves*", todos los responsables del tratamiento sujetos a la Directiva deben hacerlo:

> ... aplicar las medidas técnicas y organizativas adecuadas **para garantizar y poder demostrar** que el tratamiento se realiza de conformidad con la presente Directiva.
>
> (Apartado 1 del artículo 19, con cursiva añadida)

El artículo añade que "*las medidas de protección de datos se revisarán y actualizarán cuando sea necesario*"; y que "*cuando proceda*", deberán incluir la (elaboración, adopción y) aplicación de "*políticas adecuadas de protección de datos*" por parte del responsable del tratamiento (artículo 19, apartados 1, última frase, y 2).

Además, al igual que el RGPD, el LEDPD requiere un amplio sistema de **registro y registro** (arts. 24 y 25), que son medios importantes para garantizar la verificabilidad de la legalidad del tratamiento, lo que supone un reto especial en el ámbito de aplicación del LEDPD.

El LEDPD establece los mismos requisitos que el RGPD en relación con los "**controladores conjuntos**" (apartado 1 del artículo 21) y el uso de procesadores (artículo 22).

El LEDPD requiere la realización de una **evaluación de impacto de la protección de datos (DPIA,** artículo 27**)** en circunstancias similares a las previstas en el RGPD, a saber

[182] Explicado en detalle en la segunda parte, sección 2.3, más adelante.

> Cuando un tipo de tratamiento, en particular, utilizando nuevas tecnologías, y teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento **pueda dar lugar a un riesgo elevado para los derechos y libertades de las personas físicas** (art. 27, cursiva añadida).

También debe consultarse a la **autoridad de control** competente (que puede ser la autoridad nacional general de protección de datos, pero que también podría ser una autoridad independiente, siempre que se cumplan las condiciones de independencia, etc.: véase más adelante), cuando una ADIP "*indique que el tratamiento daría lugar a un alto riesgo en ausencia de medidas adoptadas por el responsable del tratamiento para atenuar el riesgo*" o cuando (con independencia de tales medidas) "*el tipo de tratamiento, en particular, cuando el uso de nuevas tecnologías, mecanismos o procedimientos, suponga un alto riesgo para los derechos y libertades de los interesados*" (artículo 28, apartado 1, letras a) y b)).

Para contribuir a su aplicación efectiva, en particular en relación con el principio de responsabilidad, el LEDPD prevé el nombramiento de un responsable de la **protección de datos (RPD)** por cada responsable del tratamiento (artículo 32), aclara la posición del RPD (artículo 33) y enumera las tareas del RPD (artículo 34). Esto también está en consonancia con el RGPD, que exige la designación de un RPD por parte de todas las entidades del sector público sujetas a él.[183] Sin embargo, el LEDPD no estipula explícitamente que el RPD debe poder actuar de forma independiente.[184]

Los RPD de los organismos encargados de la aplicación de la ley y de cualquier otro organismo u organismo sujeto al DIPD desempeñarán un papel importante en relación con el cumplimiento por parte de sus organizaciones del principio de responsabilidad y las correspondientes revisiones en curso de las medidas adoptadas para cumplir este principio; la redacción de los "acuerdos" con cualquier controlador conjunto y de los contratos con los transformadores; la consulta con el APD; y la realización de las evaluaciones de impacto sobre el medio ambiente en el marco del DIPD.[185]

Transferencias internacionales de datos a las autoridades competentes de terceros países

Debido a la gran sensibilidad del contexto y de los datos personales en juego en este ámbito, el capítulo V del DIPD establece una serie de condiciones para la transferencia de datos personales a un tercer país ("tercer país") o a una organización internacional, similares a las condiciones para las transferencias en el RBPI, pero con normas adicionales sobre la transferencia a un tercer país o a una organización internacional por parte de un Estado miembro de la UE de los datos personales recibidos de otro Estado miembro, así como sobre las transferencias ulteriores desde y por parte del tercer país beneficiario a otro tercer país o a una organización internacional, y con excepciones más específicas por razones específicas, como las que se analizan más adelante.

Obsérvese, sin embargo, que, en particular por lo que se refiere a las transferencias internacionales de datos, el LEDPD permite retrasos prolongados en la plena aplicación de las normas que se exponen a continuación, por razones específicas, como se indica en el apartado "*Transposición tardía*" que figura al final de esta sección sobre el LEDPD.

Condiciones generales previas para cualquier transferencia de este tipo:

El artículo 35 del Decreto-LEDPD establece **tres condiciones previas** para las transferencias a un tercer país (aunque hay que tener en cuenta que *dos de ellas pueden dejarse de lado en algunas circunstancias*, como se indica):

- la transferencia debe ser "**necesaria**" para los fines establecidos en el apartado 1 del artículo 1, es decir, para la prevención, investigación, detección o enjuiciamiento de delitos o la ejecución de sanciones penales, o para protegerse contra las amenazas (penales y jurídicas) a la seguridad pública o para prevenirlas;

[183] Véase la segunda parte, sección 2.4.2, más adelante.
[184] Véase el artículo 38, apartado 3, del RGPD, que estipula lo siguiente: *"El responsable del tratamiento velará por que el responsable de la protección de datos no reciba instrucciones sobre el ejercicio de estas funciones. El responsable del tratamiento o el encargado del tratamiento no podrá despedirlo ni sancionarlo por el ejercicio de sus funciones. El responsable de la protección de datos dependerá directamente del más alto nivel de gestión del responsable del tratamiento o del encargado del tratamiento*".
[185] Véase el análisis detallado de las tareas del RPD en el marco del RGPD en la tercera parte de este manual.

- el traslado debe efectuarse **a una autoridad del tercer país o de una organización internacional competente para los fines antes mencionados** (en cuyo caso la Organización Internacional de Policía Criminal (Interpol) figura expresamente en el considerando 25)[186]. Del mismo modo que las "autoridades competentes" de la UE no se limitan a las fuerzas y cuerpos de seguridad de primera línea, las autoridades de los terceros países a las que pueden transferirse los datos tampoco tienen por qué ser las fuerzas y cuerpos de seguridad de primera línea, siempre que sean competentes (también) en relación con los asuntos penales pertinentes.

  Obsérvese que *esta condición previa puede eximirse en determinadas situaciones*, en determinadas condiciones, como se explica más adelante en el epígrafe "*Transferencias a otras autoridades*".

- *"cuando los datos personales se transmitan o se pongan a disposición desde otro Estado miembro, dicho Estado miembro haya dado su **autorización previa** a la transferencia de conformidad con su Derecho nacional*" (con una excepción, como se indica más adelante).

  Artículo 35, apartado 1, letras a) a c)

  Esta última disposición se refiere a la transferencia de un Estado miembro a un tercer país o a una organización internacional de datos personales recibidos originalmente de otro Estado miembro, es decir, la transferencia ulterior de tales datos requiere la "autorización previa" del Estado miembro que proporcionó los datos originalmente.

  Tenga en cuenta que *esta autorización previa no es necesaria si*:

  > la transferencia de datos personales es **necesaria para prevenir una amenaza inmediata y grave para la seguridad pública de un Estado miembro o de un tercer país o para los intereses esenciales de un Estado miembro** y la autorización previa no puede obtenerse a tiempo.

  En tal caso, "*léase: la autoridad responsable de conceder la autorización previa[la autoridad a la que se debería haber pedido su consentimiento previo si no hubiera existido tal amenaza inmediata] será **informada** sin demora*" (Art. 35(2), cursiva añadida).

Una vez cumplidas estas condiciones previas, los datos personales sólo podrán transmitirse a un tercer país o a una organización internacional si se cumple **alguna de las tres condiciones siguientes**:

- la Comisión haya adoptado una **decisión de adecuación** en relación con el tercer país u organización internacional beneficiario (según lo dispuesto en el artículo 36).

  Pero tenga en cuenta que *la Comisión Europea todavía no ha tomado ninguna decisión de este tipo en el marco de la Directiva*, por lo que esta cláusula todavía no puede ser invocada.

---

[186] A este respecto, cabe señalar que Interpol no es una "organización internacional" tal como se define normalmente en el derecho internacional público, es decir, una organización basada en un tratado o establecida de otro modo en virtud del derecho internacional: véase el artículo 2 del proyecto de artículos de la Comisión de Derecho Internacional sobre las responsabilidades de las organizaciones internacionales. En cambio, Interpol fue creada por las autoridades policiales de los Estados participantes. Sobre esta cuestión, véase la pregunta formulada a la Comisión por Charles Tannock, diputado al Parlamento Europeo, el 15 de octubre de 2013, disponible en: https://www.europarl.europa.eu/sides/getDoc.do?type=WQ&reference=E-2013-011707&language=EN -
y la respuesta de la Comisión, disponible en:
https://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2013-011707&language=EN
Pero Interpol sigue siendo tratada a menudo como una organización internacional, también en cierta medida por la UE, que ha adoptado una Posición Común del Consejo sobre el intercambio de datos de pasaportes con Interpol y los Estados miembros de Interpol, sujeta a garantías de protección de datos: Posición Común 2005/69/JAI del Consejo, de 24 de enero de 2005, relativa al intercambio de determinados datos con Interpol, DO L 27 de 29 de enero de 2005, p. 61, disponible en:
https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32005E0069 (sobre la protección de datos, véase el artículo 3)
Véase también la Decisión 2007/533/JAI del Consejo, de 12 de junio de 2007, relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II), DO L 205 de 7 de agosto de 2007, p. 63, que prohíbe la transferencia o puesta a disposición de datos del SIS-II a terceros países y organizaciones internacionales (artículo 54), pero hace una excepción en lo que se refiere a los intercambios de datos sobre pasaportes robados, sustraídos, extraviados, extraviados o invalidados con Interpol (artículo 55), disponibles en:
https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32007D0533

O:

- existen "**garantías adecuadas**" para garantizar que los datos personales, tras su transferencia, sigan siendo tratados con arreglo a las "garantías adecuadas" de protección de datos.

  Esto se aclara aún más en el artículo 37, que estipula que las salvaguardias pertinentes deben establecerse en un **instrumento jurídicamente vinculante** (que puede ser un tratado o un acuerdo administrativo vinculante) (artículo 37, apartado 1, letra a)) o "*el responsable del tratamiento[debe haber **evaluado**] todas las circunstancias que rodean a la transferencia de datos personales y[ha llegado a la conclusión] de que existen salvaguardias adecuadas con respecto a la protección de los datos personales*" (artículo 37, apartado 1, letra b))) - pero, en este último caso, debe informarse a **la autoridad supervisora** de las "categorías de transferencias" realizadas con arreglo a esta cláusula. Además, toda transferencia debe estar "*documentada y la documentación se pondrá a disposición de la autoridad supervisora a petición de ésta, incluyendo la fecha y hora de la transferencia, información sobre la autoridad competente receptora, la justificación de la transferencia y los datos personales transferidos*" - Art. 37(3)).

  Obsérvese que los "**instrumentos jurídicamente vinculantes**" mencionados incluyen los "*acuerdos internacionales que implican la transferencia de datos personales a terceros países u organizaciones internacionales celebrados por los Estados miembros antes del 6 de mayo de 2016*" a que se refiere el artículo 61 de la Directiva sobre protección de datos. Dichos acuerdos, dice dicho artículo, "*permanecerán en vigor hasta que sean modificados, sustituidos o revocados*" siempre que "*se ajusten al Derecho de la Unión aplicable con anterioridad a esa fecha*". El LEDPD no fija una fecha límite para la modificación, sustitución o revocación de estos acuerdos, si no se ajustan a las normas del LEDPD, o incluso para que los Estados miembros los revisen a tal efecto. Esto se discute más adelante, bajo el epígrafe "*Retraso en la aplicación*".

  Obsérvese también que las "**salvaguardias apropiadas**" alternativas se refieren únicamente a la protección de datos: no existe ningún requisito (como el que se impone en las dos primeras de las excepciones que se examinan a continuación) de que se realice una evaluación del posible impacto en los demás "derechos y libertades fundamentales" del interesado y, en caso afirmativo, de si tal vez estos deberían "prevalecer sobre el interés público de la transferencia";

  O:

- (a falta de una decisión de adecuación con arreglo al artículo 36 y de las garantías adecuadas de conformidad con el artículo 37) si se aplica una **excepción para una situación específica**. El artículo 38 permite tales excepciones si una transferencia es "**necesaria**" en **cinco situaciones**, dos de las cuales requieren una "ponderación" de intereses. En un orden diferente al del artículo, las situaciones y condiciones especiales son las siguientes:

- Los datos personales podrán transferirse a un tercer país sin una decisión de adecuación y sin las garantías adecuadas si ello es "**necesario**" para cualquiera de los fines establecidos en el artículo 1, apartado 1, es decir, para la **prevención, investigación, detección o enjuiciamiento de cualquier delito o la ejecución de cualquier sanción penal, o para protegerse o prevenir cualquier amenaza (penal-legal) a la seguridad pública** (artículo 38, apartado 1, letra d)), a menos que:

  la autoridad competente que transfiere los datos determina que los derechos y libertades fundamentales del interesado prevalecen sobre el interés público de la transferencia (apartado 2 del artículo 38).

- Los datos personales podrán transferirse a un tercer país sin una decisión de adecuación y sin las salvaguardias adecuadas si ello es "**necesario**" para **el establecimiento, ejercicio o defensa de acciones legales** relativas a cualquiera de los fines mencionados anteriormente (artículo 38, apartado 1, letra e)), a menos que:

  la autoridad competente que transfiere los datos determina que los derechos y libertades fundamentales del interesado prevalecen sobre el interés público de la transferencia (apartado 2 del artículo 38)

  Obsérvese que las dos situaciones anteriores se refieren a casos que plantean graves dilemas en materia de derechos humanos: por una parte, la transferencia es "necesaria" para un interés público importante, pero, por otra, afecta a los derechos y libertades fundamentales de la persona a la que se refieren los datos -quizás de maneras posiblemente terribles, como cuando la información sobre un sospechoso, testigo o

> víctima se transmite a las autoridades de un Estado que viola gravemente los derechos humanos; y no existen "salvaguardias adecuadas", ni siquiera en lo que se refiere al (ulterior) tratamiento de los datos personales de la persona a la que se refieren. **Es evidente que el RPD de la autoridad pertinente debe ser consultado sobre dichas transferencias y que tendrá que soportar una pesada carga de asesoramiento a este respecto.**

- Los datos personales pueden transferirse a un tercer país sin una decisión de adecuación y sin las salvaguardias adecuadas si ello es "**necesario**" **para prevenir una amenaza inmediata y grave a la seguridad pública de un Estado miembro o de un tercer país** (artículo 38, apartado 1, letra c)), *en este caso aparentemente con independencia de cualquier consideración de los derechos y libertades fundamentales del interesado (a menos que pueda interpretarse como un requisito de "necesidad")*.

- Los datos personales pueden transferirse a un tercer país sin una decisión de adecuación y sin las garantías adecuadas si ello es "**necesario**" para **proteger los intereses vitales del interesado o de otra persona** (artículo 38, apartado 1, letra a)).

- Los datos personales pueden transferirse a un tercer país sin una decisión de adecuación y sin las garantías adecuadas si ello es "**necesario**" **para salvaguardar los intereses legítimos del interesado**, *cuando así lo disponga la legislación del Estado miembro que transfiere los datos personales* (artículo 38, apartado 1, letra b)).

Los datos transferidos sobre la base de cualquiera de las cinco excepciones anteriores deben ser ***"estrictamente necesarios"*** (considerando 72), y estar **documentados**, y:

> la documentación se **pondrá a disposición de las autoridades de supervisión, previa solicitud**, incluyendo la fecha y hora de la transferencia, información sobre la autoridad competente receptora, la justificación de la transferencia y los datos personales transferidos. (Art. 38, apdo. 3, cursiva añadida)

El objetivo de esta documentación y de su puesta a disposición de la autoridad supervisora es permitir que ésta "*controle* (retrospectivamente) *la legalidad de la transferencia*" (considerando 72). El considerando 72 añade que:

> Las excepciones enumeradas anteriormente] deben **interpretarse de forma restrictiva** y **no deben permitir** transferencias **frecuentes, masivas y estructurales** de datos personales o transferencias de datos a gran escala, sino que deben limitarse a los datos estrictamente necesarios.

Una vez más, cualquier RPD de cualquier organización pertinente tendría responsabilidades importantes con respecto a esta documentación y a cualquier interacción sobre cuestiones pertinentes con la autoridad supervisora.[187]

Transferencias a otras autoridades de terceros países

Como se ha señalado anteriormente, en principio todos los tipos de transferencias mencionadas sólo pueden efectuarse a las autoridades del tercer país de que se trate a las que se conceden competencias en relación con los fines enumerados en el artículo 1, apartado 1, de la Directiva, a saber en relación con "*la prevención, investigación, detección o enjuiciamiento de delitos o la ejecución de sanciones penales, incluida la protección y prevención de amenazas[penales-legales] a la seguridad pública*" (artículo 35, apartado 1, letra b)) (aunque no es necesario que los destinatarios sean los organismos encargados de la aplicación de la ley propiamente dichos; entre ellos pueden figurar otras autoridades públicas con determinadas tareas y competencias en materia de delincuencia o seguridad pública).

Sin embargo, el artículo 39 del DIPD permite **excepciones** a esta regla, bajo el epígrafe "*Transferencias de datos personales a destinatarios establecidos en terceros países*" (entendiéndose por tales los

[187] Véase la tercera parte de este manual, Tareas del RPD, Tareas 1 - 5 y 12.

destinatarios distintos de las autoridades que, en el tercer país de que se trate, sean competentes para las materias enumeradas en el artículo 1, apartado 1, de la Directiva).

El considerando 73 explica las razones de estas excepciones (párrafos rotos y énfasis añadido):

> Las autoridades competentes de los Estados miembros aplicarán los acuerdos internacionales bilaterales o multilaterales vigentes, celebrados con terceros países en el ámbito de la cooperación judicial en materia penal y de la cooperación policial, para el intercambio de la información pertinente que les permita desempeñar las tareas legalmente asignadas. En principio, esto se lleva a cabo mediante la cooperación de las autoridades competentes de los terceros países afectados a efectos de la presente Directiva, o al menos con ellas, a veces incluso en ausencia de un acuerdo internacional bilateral o multilateral.
>
> **Sin embargo, en casos concretos, los procedimientos ordinarios que exigen ponerse en contacto con la autoridad del tercer país pueden ser ineficaces o inapropiados, en particular porque la transferencia no pudo llevarse a cabo a tiempo o porque dicha autoridad[léase: el organismo encargado de la aplicación de la ley pertinente] del tercer país no respeta el Estado de Derecho o las normas internacionales de derechos humanos, de modo que las autoridades competentes de los Estados miembros pueden decidir transferir datos personales directamente a los destinatarios[léase: otras entidades que no son responsables de la aplicación de la ley] establecidos en esos terceros países.**
>
> Este puede ser el caso cuando existe una necesidad urgente de transferir datos personales para salvar la vida de una persona que está en peligro de ser víctima de un delito o para prevenir la inminente comisión de un delito, incluido el terrorismo.
>
> Aunque dicha transferencia entre autoridades competentes y destinatarios establecidos en terceros países sólo debe tener lugar en casos concretos, la presente Directiva debe establecer las condiciones para regular tales casos.
>
> Estas disposiciones no deben considerarse excepciones a ningún acuerdo internacional bilateral o multilateral existente en el ámbito de la cooperación judicial en materia penal y de la cooperación policial. Estas normas deben aplicarse además de las demás normas de la presente Directiva, en particular las relativas a la legalidad del tratamiento y al capítulo V.

El apartado 1 del artículo 39 puede parafrasearse del siguiente modo:[188]

> La legislación de la Unión o de los Estados miembros podrá disponer que los organismos encargados de la aplicación de la ley, en casos individuales y específicos, transfieran directamente datos personales a destinatarios establecidos en terceros países que no sean competentes en materia penal y de seguridad pública, pero únicamente si se cumplen las demás disposiciones de la presente Directiva y se cumplen todas las condiciones siguientes: ....

El LEDPD no dice nada sobre la naturaleza exacta de las "otras autoridades" pertinentes. Dado que el artículo 39 se aplica a situaciones especialmente sensibles a los derechos humanos (véase la frase subrayada en negrita en la cita del considerando 73), se supone que lo que se prevé son destinatarios en el tercer país en el que la autoridad transmisora del Estado miembro de la UE de que se trate tiene **especial confianza**. En particular, la autoridad transmisora debe confiar en que el organismo receptor no encargado de la aplicación de la ley no transmitirá la información a un organismo de aplicación de la ley

[188] El texto del apartado 1 del artículo 39 es el siguiente :
" No obstante a lo dispuesto en la letra b) del apartado 1 del artículo 35, y sin perjuicio de cualquier acuerdo internacional mencionado en el apartado 2 del presente artículo, la legislación de la Unión o de los Estados miembros podrá disponer que las autoridades competentes mencionadas en la letra a) del apartado 7 del artículo 3, en casos individuales y específicos, transfieran datos personales directamente a destinatarios establecidos en terceros países[distintos de los servicios policiales] únicamente si se cumplen las demás disposiciones de la presente Directiva y se cumplen todas las condiciones siguientes:....".

en el tercer país que "*no respete el Estado de Derecho ni las normas internacionales de derechos humanos*". La evaluación pertinente caso por caso siempre será especialmente delicada, que deberá, como mínimo, **documentarse con el mayor cuidado** (incluidas las razones para suponer que los datos pueden transmitirse a la agencia de confianza sin temor a que acaben en manos de organismos menos salados del tercer país de que se trate).

Para las transferencias no cubiertas por acuerdos internacionales (que se examinan por separado más adelante), el apartado 1 del artículo 39 establece **cinco condiciones acumulativas** para las transferencias pertinentes. Los datos podrán transferirse a un destinatario pertinente no ejecutor de la ley en un tercer país si (énfasis, aclaraciones entre corchetes y notas en virtud de las cláusulas añadidas):

a. la transferencia es **estrictamente necesaria** para el cumplimiento de una misión de la autoridad competente que realiza la transferencia[en el Estado miembro de la UE de que se trate] según lo dispuesto en la legislación de la Unión o del Estado miembro a los efectos establecidos en el artículo 1, apartado 1[es decir, **en relación con asuntos penales o de seguridad pública de la UE o del Estado miembro**].

b. la autoridad competente que transfiere los **datos** determine que **ningún derecho o libertad fundamental del interesado prevalece sobre el interés público que requiera la transferencia en el caso de que se trate**.

Obsérvese que esta determinación no se limita a los intereses de protección de datos del interesado, sino que, más bien, debería considerar de forma más general si el tercer país en cuestión y los organismos específicos de ese país "*respetan el Estado de Derecho o las normas y estándares internacionales de derechos humanos*". Además, la determinación debe hacerse **caso por caso**.

c. la autoridad competente que realiza la transferencia considera que la **transferencia a una autoridad competente a los efectos mencionados en el apartado 1 del artículo 1**[en materia penal y de seguridad pública] en el tercer país es **ineficaz o inadecuada**, en particular porque *la transferencia no puede llevarse a cabo a su debido* tiempo

o, se debería añadir, porque esto sería "inapropiado" por otras razones: véase la nota de la cláusula siguiente.

d. **la autoridad competente en el tercer país para los fines mencionados en el apartado 1 del artículo 1 sea *informada*** sin demora injustificada, a menos que ello sea **ineficaz o inadecuado**.

Obsérvese que la referencia a la transmisión a un organismo (encargado de hacer cumplir la ley) que normalmente sería el más pertinente y apropiado como "**inapropiado**" puede interpretarse como una situación en la que ese organismo "*[no] respeta el estado de derecho ni las normas y estándares internacionales de derechos humanos*". La referencia a la "**ineficacia**" de esa agencia puede referirse a que es *ineficaz, lenta, incompetente o tal vez corrupta*.

e. **la autoridad competente que transfiere los datos informa al destinatario de la finalidad o finalidades especificadas, para las cuales los datos personales sólo serán tratados por este último*, siempre que dicho tratamiento sea necesario***.

Obsérvese que esto implica que la autoridad receptora del tercer país debe dar **garantías** (firmes y vinculantes) de que cumplirá estas estipulaciones y que realmente sólo utilizará los datos facilitados por el órgano de seguridad de la UE para el propósito o propósito específico estipulado y no para ningún otro; e incluso entonces sólo utilizará los datos en la medida en que sea (estrictamente) necesario para el propósito estipulado.

Además de cumplir estas disposiciones específicas, como ya se ha señalado, el apartado 1 del artículo 39 subraya que "*[todas] las demás disposiciones de la presente Directiva*" también deben cumplirse (véase también la última frase del considerando 73, citado anteriormente, que subraya que esto incluye "en particular las[disposiciones] sobre la legalidad del tratamiento y el capítulo V", es decir, las demás disposiciones sobre transferencia de datos).

Todo lo anterior, sin embargo, "**sin perjuicio de cualquier acuerdo internacional**" (Art. 39(1)), por el cual se entiende:

> cualquier acuerdo internacional bilateral o multilateral vigente entre los Estados miembros y terceros países en el ámbito de la cooperación judicial en materia penal y de la cooperación policial. (Art. 39(2))

Esto debe leerse conjuntamente con el artículo 61, que trata de la "*Relación con los acuerdos internacionales previamente celebrados en el ámbito de la cooperación judicial en materia penal y de la cooperación policial*" del LEDPD y que así lo estipula:

> Los acuerdos internacionales que impliquen la transferencia de datos personales a terceros países u organizaciones internacionales que hayan sido celebrados por los Estados miembros antes del 6 de mayo de 2016 y que se ajusten al Derecho de la Unión aplicable antes de esa fecha seguirán en vigor hasta que sean modificados, sustituidos o revocados.

El LEDPD no establece una fecha límite para la modificación, sustitución o revocación de estos acuerdos, en caso de que no se ajusten a las normas del LEDPD, o incluso para que los Estados miembros los revisen con el fin de adaptarlos a la Directiva.[189] Sin embargo, el artículo 62 del LEDPD estipula que:

> A más tardar **el 6 de mayo de 2022**, y posteriormente cada cuatro años, **la Comisión** presentará al Parlamento Europeo y al Consejo **un informe sobre la evaluación y revisión de la presente Directiva.** Los informes se harán públicos. (énfasis añadido)

Estas revisiones deben incluir "*en particular, la aplicación y el funcionamiento del capítulo V sobre la transferencia de datos personales a terceros países u organizaciones internacionales*" (artículo 62, apartado 2), con "especial atención" a las decisiones de adecuación con arreglo al artículo 36, apartado 3, y a las **transferencias a "otras autoridades" con arreglo al artículo 39**, como se acaba de debatir. Además, la Comisión puede, en este contexto, "*solicitar información a los Estados miembros y a las autoridades de supervisión*" (apartado 3 del artículo 62), incluyendo, presumiblemente, los acuerdos internacionales antes mencionados que hayan celebrado. También es de suponer que, sobre la base de la primera revisión, la Comisión puede **proponer** que se introduzcan **cambios** en dichos acuerdos o, al menos, hacer **sugerencias sobre la** forma de adaptarlos a las normas de la Directiva, pero esto no está estipulado en la misma (a diferencia de lo que ocurre con los actos de la Unión en este ámbito).[190]

Según la Comisión, el LEDPD conducirá a una "**cooperación internacional más fuerte":**[191]

> La cooperación entre las autoridades policiales y judiciales de la UE y las de terceros países también se verá reforzada[por el LEDPD], ya que habrá normas más claras para las transferencias internacionales de datos relacionadas con delitos penales. Las nuevas normas garantizarán que las transferencias se realicen con un nivel adecuado de protección de datos.

Sin embargo, como se indica más adelante bajo el epígrafe "*Transposición retardada*", todavía pasará algún tiempo antes de que las nuevas normas a las que se hace referencia se apliquen realmente en su totalidad.

Supervisión y ejecución

El capítulo VI del DIPD exige la creación de **autoridades de supervisión independientes** en los Estados miembros encargadas de supervisar y hacer cumplir las disposiciones de las leyes nacionales adoptadas para aplicar ("transponer") la Directiva, así como otras tareas conexas (véanse los artículos 41 a 46 del DIPD). La autoridad o autoridades de control pertinentes pueden ser, pero no es necesario que sean, la

---

[189] Tampoco tenemos conocimiento de ninguna revisión realizada antes de la introducción del DIPD, de si los acuerdos internacionales que implican la transferencia de datos personales a terceros países o a organizaciones internacionales que fueron celebrados por los Estados miembros antes de esa fecha cumplían con el Derecho de la Unión en la forma en que entonces era aplicable.

[190] El artículo 62, apartado 6, establece que, a más tardar **el 6 de mayo de 2019**, la Comisión deberá haber revisado los "*otros actos jurídicos adoptados por la Unión que regulen el tratamiento por las autoridades competentes para los fines establecidos en el artículo 1, apartado 1, incluidos los mencionados en el artículo 60, con el fin de evaluar la necesidad de adaptarlos a la presente Directiva y de hacer, en su caso, las propuestas necesarias para modificar dichos actos a fin de garantizar un enfoque coherente de la protección de los datos personales en el ámbito de aplicación de la presente Directiva.* "Véase también el apartado "*Retraso en la transposición*".

[191] Comisión Europea, Ficha técnica - ¿Cómo ayudará la reforma de la protección de datos a combatir la delincuencia internacional? (véase anterior nota de página 176).

autoridad o autoridades de control generales establecidas en virtud del Reglamento sobre el producto interior bruto (artículo 41, apartado 3): en algunos países existen autoridades de control especiales para supervisar el tratamiento de datos personales por parte de la policía y de los organismos encargados de la aplicación de la ley, mientras que en otros también se encomienda esta tarea a la autoridad general de protección de datos (DPA). Además, en algunos países (especialmente en los federales), existen diferentes autoridades nacionales (federales) y locales o regionales.

Al igual que las DPA generales designadas en el marco del RGPD, las autoridades de supervisión competentes en relación con los asuntos cubiertos por el LEDPD deben disponer de **amplios poderes**, incluido el derecho a exigir (y obtener) "***acceso a todos los datos personales*** *que se estén tratando y a* ***toda la información*** *necesaria para el desempeño de sus funciones*"; y la facultad de dirigir ***advertencias*** a un responsable del tratamiento, de ***ordenar*** al responsable del tratamiento o al encargado del tratamiento que ***modifique las*** operaciones para adaptarlas a la Directiva, "*cuando proceda, de una manera y en un plazo determinados, en particular ordenando la rectificación o la supresión de datos personales o la restricción de su tratamiento*", y de imponer ***una limitación temporal o definitiva, incluida la prohibición de su*** tratamiento; y la facultad de ***incoar procedimientos judiciales*** contra los responsables del tratamiento o los encargados del tratamiento que supuestamente hayan infringido la Directiva, o de someter estos asuntos a la atención de las autoridades competentes (art. 3, apartado 1, del artículo 3, apartado 1, del artículo 3, apartado 1, de la Directiva sobre la protección de datos personales). 47 (1), (2) y (5) LEDPD). Las autoridades de supervisión también tienen importantes **funciones de asesoramiento** y deben tener el derecho de hacerlo:

> emitir, por iniciativa propia o previa solicitud, **dictámenes dirigidos al Parlamento nacional y a su Gobierno** o, de conformidad con su legislación nacional, a otras instituciones y organismos, así como al público, sobre cualquier cuestión relacionada con la protección de datos personales. (Art. 47, apdo. 3, cursiva añadida)

También deben publicar un **informe anual** sobre sus actividades, "*que puede incluir una lista de los tipos de infracciones notificadas y los tipos de sanciones impuestas*" (art. 49).

No obstante, las decisiones de las autoridades de supervisión deben estar sujetas a las "*salvaguardias adecuadas, incluidos el recurso judicial efectivo y el respeto de las garantías procesales, según lo establecido en la legislación de la Unión y de los Estados miembros de conformidad con la Carta*" (apartado 4 del artículo 47).

En particular, el LEDPD estipula que:

> Los Estados miembros dispondrán que las autoridades competentes establezcan mecanismos eficaces para fomentar la notificación confidencial de las infracciones de la presente Directiva. (Art. 48)

Esta disposición se ajusta a la recientemente adoptada Directiva sobre denuncia de irregularidades.[192]

El artículo 50 prevé la **asistencia mutua** entre las autoridades de control de los Estados miembros de la UE, competentes en relación con el tratamiento de datos personales sujetos al LEDPD.

Además, el **Consejo Europeo de Protección de Datos**, creado en el marco del RGPD, también tiene competencia en relación con el tratamiento en el ámbito de aplicación del LEDPD (art. 51). Esto incluye la publicación de ***directrices, recomendaciones y mejores prácticas*** sobre cualquier cuestión planteada en el marco de la Directiva, así como la publicación de:

> Un **dictamen para la evaluación de la adecuación del nivel de protección en un tercer país, en un territorio o en uno o más sectores específicos dentro de un tercer país, o en una organización internacional**, incluida la evaluación de si dicho tercer país, territorio,

[192] Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas que denuncian infracciones del Derecho de la Unión, 2019. En el momento de preparar el presente manual, el texto aún no se había publicado en el Diario Oficial (y, por lo tanto, tampoco tiene número), pero el texto adoptado por el Parlamento Europeo el 16 de abril de 2019 (que es el texto definitivo, sujeto a revisión lingüística y traducción) está disponible en: https://www.europarl.europa.eu/doceo/document/TA-8-2019-0366_EN.html?redirect

> sector específico u organización internacional ya no garantiza un nivel de protección adecuado[letra g) del apartado 1 del artículo 51].

La Junta Directiva debe transmitir sus dictámenes, directrices, recomendaciones y mejores prácticas a la Comisión (y al Comité establecido en virtud del artículo 93 del RPI), y debe hacerlos públicos (apartado 3 del artículo 51); y la Comisión, a su vez, debe informar a la Junta Directiva de las medidas que haya adoptado en respuesta (apartado 4 del artículo 51).

Recursos, responsabilidad y sanciones

En el capítulo VIII se establecen las vías de recurso, las responsabilidades y las sanciones que deben preverse en las leyes nacionales por las que se transpone el DIPD. En resumen, de conformidad con el RDGP, todo interesado debe tener **derecho a presentar una reclamación** ante la autoridad de control competente si considera que el tratamiento de los datos personales que le conciernen infringe las disposiciones adoptadas en virtud de la presente Directiva (artículo 52), así como el derecho a obtener un **recurso judicial efectivo** contra cualquier decisión jurídicamente vinculante de una autoridad de control que le concierna (artículo 5, apartado 1, letra a), del Reglamento (CE) nº.../CE)..../CE del Parlamento Europeo y del Consejo. 53), y contra cualquier responsable o encargado de tratamiento sujeto al LEDPD (ley nacional de transposición), "*cuando considere que se han vulnerado los derechos que le confieren las disposiciones adoptadas en virtud de la presente Directiva como consecuencia del tratamiento de sus datos personales en violación de dichas disposiciones*" (art. 54). Por otra parte (de nuevo en línea con el RGPD):

> el interesado tiene **derecho a encomendar a un organismo, organización o asociación sin ánimo de lucro** debidamente constituido con arreglo a la legislación del Estado miembro, que tenga objetivos estatutarios de interés público y que actúe en el ámbito de la protección de los derechos y libertades del interesado en lo que respecta a la protección de sus datos personales**, que presente la reclamación en su nombre y ejerza en su nombre los derechos a que se refieren los artículos 52, 53 y 54**. (Art. 55, cursiva añadida)

Los interesados también tienen **derecho a una indemnización** por los daños materiales y morales causados por un tratamiento contrario a la Directiva (art. 56).

Por último, los Estados miembros deben prever **sanciones "efectivas, proporcionadas y disuasorias"** para las infracciones del DIPD (art. 57).

Retraso en la transposición

Como ya se ha mencionado en los apartados anteriores, no todo el tratamiento de datos personales con fines policiales y de seguridad pública tiene que ser todavía conforme con el DIPD o con las leyes nacionales que transponen el DIPD: la Directiva contiene una serie de disposiciones que permiten que determinados instrumentos y operaciones sólo se ajusten a la Directiva en una fecha futura (o incluso en un futuro indefinido). Las disposiciones que permiten una aplicación tardía se refieren a los "actos jurídicos" de la UE, a los tratados entre los Estados miembros de la UE y terceros países u organizaciones internacionales (incluida Interpol), y a los sistemas especiales de tratamiento automatizado de datos de los Estados miembros en el ámbito del Derecho penal y la seguridad pública.

Retraso en la aplicación de los actos jurídicos de la UE:

El artículo 60 del Decreto-LEDPD establece, en relación con los aproximadamente 123 instrumentos de la UE ("actos jurídicos" de diverso tipo) relativos a la Justicia y los Asuntos de Interior (JAI), lo que importa[193]:

> Las disposiciones específicas para la protección de datos personales de los **actos jurídicos de la Unión que hayan entrado en vigor a más tardar el 6 de mayo de 2016** en el ámbito de la cooperación judicial en materia penal y de la cooperación policial, que regulan el tratamiento entre Estados miembros y el acceso de las autoridades designadas de los Estados miembros a los sistemas de información establecidos en virtud de los Tratados en el ámbito de aplicación de la presente Directiva, **no se verán afectadas**. (énfasis añadido)

[193] Véase Emilio De Capitani, o.c. (nota 141).

Sin embargo, el artículo 62, apartado 6, del Decreto-LEDPD estipula que, **para el 6 de mayo de 2019**, la Comisión debe haber **procedido a una revisión**:

> todos los demás actos jurídicos[es decir, distintos del propio LEDPD] adoptados por la Unión que regulen el tratamiento por parte de las autoridades competentes a los efectos establecidos en el apartado 1 del artículo 1, incluidos los mencionados en el artículo 60, con el fin de **evaluar la necesidad de adaptarlos a la presente Directiva y de presentar, en su caso, las propuestas necesarias para modificar dichos actos** a fin de garantizar un enfoque coherente de la protección de los datos personales en el ámbito de aplicación de la presente Directiva. (énfasis añadido)

De lo anterior se deduce que **estos aproximadamente 123 "otros actos jurídicos" no necesitan ser adaptados al LEDPD antes del 6 de mayo de 2019**: todo lo que se requiere es que sean ***revisados*** antes de esa fecha, con vistas a ***proponerles*** cambios cuando sea necesario. **No se ha fijado ninguna fecha para la realización de las modificaciones realmente necesarias**, ni siquiera para la presentación de las correspondientes propuestas detalladas instrumento por instrumento.[194]

Mientras tanto, como establece el artículo 60, las normas de protección de datos de esos aproximadamente 123 actos jurídicos siguen en vigor sin cambios y pueden servir de base para la transferencia de datos personales en el ámbito del Derecho penal y de la seguridad pública, incluso si no cumplen los requisitos del LEDPD, siempre que se cumplan **las tres condiciones previas** para dicha transferencia establecidas en el LEDPD: que la transferencia es (en opinión de la entidad de la UE que la transfiere) "necesaria" a efectos de Derecho penal o de seguridad pública; que la transferencia se realiza a una autoridad del tercer país con competencia en estos ámbitos (a menos que dicha autoridad sea ineficaz o demasiado lenta o peor): viola los derechos humanos); y, si los datos transmitidos se obtuvieron originalmente de un Estado miembro, que ese Estado miembro autorizó la transferencia (o, en casos urgentes, fue informado al menos de ello); y siempre que el instrumento jurídico pertinente contenga salvaguardias "adecuadas" de protección de datos, ***o*** (si el instrumento no contiene tales salvaguardias) "*la autoridad competente de la UE que transfiere los datos determine que los derechos y libertades fundamentales del interesado*" no "*prevalecen sobre el interés público en la transferencia*".

Fundamentalmente, en virtud del nuevo principio de "**responsabilidad**", **las evaluaciones realizadas por la entidad** -es decir, si el instrumento jurídico pertinente contiene salvaguardias "adecuadas" de protección de datos, o si, y por qué, el interés público en la transferencia supera la necesidad de proteger los derechos y libertades fundamentales del interesado- deben **registrarse** ahora y, previa solicitud, ponerse a disposición del Supervisor Europeo de Protección de Datos (y del Tribunal).

Por supuesto, cualquier RPD de una entidad competente de la UE también debe desempeñar un papel importante en este sentido: en primer lugar, alertando a la organización de la necesidad de realizar estos ensayos y, a continuación, verificando internamente que se aplican y se aplican correctamente, y consultando al Supervisor Europeo de Protección de Datos en caso necesario en caso de desacuerdo interno o de preguntas sobre estos asuntos.

Retraso en la aplicación de los tratados entre los Estados miembros de la UE y terceros países u organizaciones internacionales:

Como se señaló anteriormente, el artículo 61 estipula que

> Los acuerdos internacionales que impliquen la transferencia de datos personales a terceros países u organizaciones internacionales que hayan sido celebrados por los Estados miembros antes del 6 de mayo de 2016 y que se ajusten al Derecho de la Unión aplicable antes de esa fecha seguirán en vigor hasta que sean modificados, sustituidos o revocados.

Por lo tanto, las transferencias en virtud de cualquier tratado anterior a mayo de 2016 entre un Estado miembro, un tercer país o una organización internacional también pueden continuar por el momento, siempre que se cumplan las tres condiciones previas para tales transferencias establecidas en

[194] En el momento de la última revisión de esta primera edición del manual, a principios de mayo de 2019, la Comisión todavía no había presentado ninguna propuesta de este tipo.

el DIPD: que la transferencia sea (en opinión de la autoridad que realiza la transferencia) "necesaria" para fines de Derecho penal o de seguridad pública; que la transferencia se efectúe a una autoridad del tercer país con competencia en estos ámbitos (a menos que dicha autoridad sea ineficaz, demasiado lenta o peor): viola los derechos humanos); y, si los datos transmitidos se obtuvieron originalmente de otro Estado miembro de la UE, que ese otro Estado autorizó la transferencia (o, en casos urgentes, fue informado al menos de ello); y siempre que el tratado contenga salvaguardias "adecuadas" de protección de datos, ***o*** (si el tratado no contiene tales salvaguardias) "*la autoridad competente que transfiere los datos determine que los derechos y las libertades fundamentales de la persona interesada*" no "*prevalecen sobre el interés público en la transferencia*".

Pero de nuevo, bajo el principio de "**responsabilidad**", las evaluaciones de la autoridad -es decir, si el tratado contiene salvaguardias "adecuadas" de protección de datos, o si cumple con la legislación de la Unión anterior a mayo de 2016, o si, y por qué, el interés público en la transferencia supera la necesidad de proteger los derechos y libertades fundamentales de la persona de que se trate- deben **registrarse** ahora y, previa solicitud, ponerse a disposición de la autoridad supervisora (y de los tribunales).

Además, cualquier RPD de una autoridad competente pertinente de un Estado miembro tendrá un papel importante que desempeñar en este sentido.

Retraso en la aplicación de los sistemas especiales de tratamiento automatizado de datos de los Estados miembros en el ámbito del Derecho penal y la seguridad pública

El artículo 63, que trata específicamente de la transposición del LEDPD a la legislación nacional, estipula en su primer apartado que:[195]

> Los Estados miembros adoptarán y publicarán, a más tardar el 6 de mayo de 2018, las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva. Notificarán inmediatamente a la Comisión el texto de dichas disposiciones. Aplicarán dichas disposiciones a partir del **6 de mayo de 2018**. (énfasis añadido)

De ello se deduce, en principio, que las "disposiciones legales, reglamentarias y administrativas" en cuestión tenían que cumplir plenamente el LEDPD para esa fecha.

Sin embargo, el artículo prevé la siguiente **excepción** en el párrafo siguiente, sujeta a condiciones:

> No obstante lo dispuesto en el apartado 1, un Estado miembro podrá prever, ***excepcionalmente, cuando ello suponga un esfuerzo desproporcionado***, que los sistemas de tratamiento automatizado creados antes del 6 de mayo de 2016 se ajusten a lo dispuesto en el artículo 25, apartado 1, a más tardar **el 6 de mayo de 2023**. (énfasis añadido)

El tercer párrafo permite demoras aún mayores, sujetas a otras condiciones:

> No obstante lo dispuesto en los apartados 1 y 2 del presente artículo, un Estado miembro podrá, ***en circunstancias excepcionales***, ajustar un sistema de tratamiento automatizado contemplado en el apartado 2 del presente artículo a lo dispuesto en el artículo 25, apartado 1, **dentro de un plazo determinado** tras el plazo mencionado en el apartado 2 del presente artículo, ***si de otro modo causara graves dificultades para el funcionamiento de dicho sistema de tratamiento automatizado***. El Estado miembro de que se trate **notificará a la Comisión** los motivos de esas dificultades graves y los motivos en los que se basa para el plazo especificado en el que deberá adaptar su sistema de tratamiento automatizado de datos a lo dispuesto en el apartado 1 del artículo El plazo especificado no podrá en ningún caso ser posterior al **6 de mayo de 2026**. (énfasis añadido)

[195] El último párrafo del cuarto párrafo estipula que: "Los Estados miembros comunicarán a la Comisión el texto de las principales disposiciones de Derecho interno que adopten en el ámbito regulado por la presente Directiva. "La disposición más específica del primer apartado subraya que la plena aplicación del LEDPD es, de hecho, un trabajo que debe progresar a lo largo de varios años, más que una transposición única.

Todo lo anterior significa que la plena aplicación de todos los requisitos del LEDPD, incluidos en particular los relativos a la transferencia de datos a terceros países y organizaciones internacionales, todavía llevará algún tiempo.

No obstante, conviene recordar que, en virtud de la Directiva (contrariamente a lo que ocurría en la anterior Decisión marco del Consejo), el cumplimiento de las normas y acciones de la Unión y de los Estados miembros en materia penal y de seguridad pública es ahora justiciable. Esto incluye, en última instancia, la verificación de si tales normas y acciones cumplen con el DIPD -incluyendo si se cumplen las pruebas antes mencionadas (si un tratado contiene salvaguardias "adecuadas" de protección de datos o si cumple el Derecho de la Unión anterior a mayo de 2016; o si, en un caso específico, el interés público en la transferencia superó realmente la necesidad de proteger los derechos y libertades fundamentales de la persona o personas a las que se refieren los datos); y, en relación con cualquier retraso en la adaptación de las operaciones anteriormente mencionadas a la Directiva, si se cumplen las condiciones especiales para tales retrasos, establecidas en los apartados citados anteriormente.

1.4.4 Nuevos instrumentos de protección de datos en el ámbito de la Política Exterior y de Seguridad Común (PESC)

Como explica la Comisión:[196]

> El Tratado de Lisboa de 2009 contribuyó en gran medida a reforzar las actividades de la Unión en el ámbito de la acción exterior. En primer lugar, creó el cargo de **Alto Representante (AR) de la Unión para Asuntos Exteriores y Política de Seguridad**. …
>
> Y, en segundo lugar, el Tratado estableció el **Servicio Europeo de Acción Exterior (SEAE)**. En funcionamiento desde 2011, es esencialmente el nuevo servicio diplomático de la UE, que asiste al Alto Representante en la conducción de la política exterior de la UE. En particular, el SEAE gestiona la red de **141 delegaciones de la UE** en todo el mundo.
>
> El SEAE trabaja para garantizar la coherencia y la coordinación de la acción exterior de la Unión, preparando propuestas políticas y aplicándolas tras su aprobación por el Consejo Europeo. …
>
> Junto con el SEAE, se creó un nuevo servicio de la Comisión, el Servicio de **Instrumentos de Política Exterior (FPI)**, para asumir la responsabilidad de los gastos operativos.
>
> Hoy, bajo la autoridad de[el AR], y en estrecha colaboración con las delegaciones del SEAE y de la UE, el FPI tiene la tarea de .... ejecutar el
>
> presupuesto de la Política Exterior y de Seguridad Común (PESC)[y una variedad de otros instrumentos y acciones]. …[197]
>
> El presupuesto para la amplia gama de actividades gestionadas por el IFS asciende a 733 millones de euros en 2014.

El trabajo realizado por el AR, el SEAE y el personal del servicio FPR implicará a menudo el tratamiento de datos personales, por ejemplo, en relación con la imposición de sanciones a las personas o la congelación de sus activos.[198]

Sin embargo, este tratamiento no está sujeto a las mismas normas del Tratado de la UE que el tratamiento por parte de las entidades sujetas al RGPD, al LEDPD o incluso a las demás instituciones de la UE. Todos los demás están cubiertos por la garantía general de protección de datos personales consagrada en el artículo 16 del TFUE:

Artículo 16

[196] Ver:
https://ec.europa.eu/fpi/about-fpi_en

[197] Para una lista con enlaces a cada instrumento o acción específica, véase la página web a la que se hace referencia en la nota anterior.

[198] Véanse los dictámenes y observaciones del SEPD sobre estas cuestiones, que se enumeran a continuación:
https://edps.europa.eu/data-protection/our-work/subjects/common-foreign-and-security-policy_en

1. Toda persona tiene derecho a la protección de los datos personales que la conciernan.

2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas relativas 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, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y las normas relativas a la libre circulación de estos datos. El cumplimiento de estas normas estará sujeto al control de autoridades independientes.

Sin embargo, esto no se aplica al tratamiento de datos personales por parte de los organismos de la PESC mencionados anteriormente porque, después de lo anterior, la última frase del artículo 16 del TFUE lo estipula:

> Las normas adoptadas sobre la base del presente artículo se **entenderán sin perjuicio de las normas específicas** establecidas en el **artículo 39** del Tratado de la Unión Europea.

Este último artículo del TUE estipula lo siguiente:

Artículo 39

> De conformidad con el artículo 16 del Tratado de Funcionamiento de la Unión Europea y no obstante lo dispuesto en su apartado 2, **el Consejo adoptará una decisión por la que se establezcan las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del presente capítulo**[es decir, en relación con la PESC], así como las normas relativas a la libre circulación de dichos datos. El cumplimiento de estas normas estará sujeto al control de autoridades independientes.

Este no es el lugar para seguir discutiendo estos asuntos.[199] Baste señalar que, en el ámbito de la PESC, se aplica el Reglamento que cubre el tratamiento de datos personales por parte de las instituciones de la UE (etc.), el Reglamento 2018/1725, que se examina en la sección siguiente, pero sólo de forma limitada; y que, para conocer las normas específicas de protección de datos relativas a cada una de las actividades de tratamiento de datos en el contexto de la PESC, incluida la autoridad de protección de datos competente sobre qué y si debe designarse a un responsable de la protección de datos, es necesario conocer la decisión concreta del Consejo relativa a la misma.

[199] Véanse los dictámenes y observaciones del SEPD sobre estas cuestiones, que se enumeran a continuación: https://edps.europa.eu/data-protection/our-work/subjects/common-foreign-and-security-policy_en

- SEPD, Dictamen conjunto sobre las notificaciones de control previo recibidas del responsable de la protección de datos del Consejo de la Unión Europea en relación con el tratamiento de datos personales con vistas a la adopción de medidas restrictivas en relación con la congelación de activos, Bruselas, 7 de mayo de 2014 (2012-0724, 2012-0725, 2012-0726), p. 10, disponible en: https://edps.europa.eu/sites/edp/files/publication/14-05-07_processing_personal_data_council_en.pdf

1.4.5 Protección de datos para las instituciones de la UE: un nuevo reglamento

Como se indica en la sección 1.3.6, el primer instrumento de la UE sobre protección de datos en relación con el tratamiento de datos personales por las propias instituciones de la UE, el Reglamento 45/2001, fue derogado por el Reglamento (UE) 2018/1725, que entró en vigor el **11 de diciembre de 2018**[200] (aunque con algunas **excepciones** y algunos **retrasos en su aplicación**, como se indica más adelante en esos epígrafes).

Dos regímenes

Aparte de estas excepciones y retrasos, el Reglamento 2018/1725 crea en realidad **dos regímenes de protección de datos distintos**: uno para todas las ***instituciones y organismos de la UE que no participan en la cooperación policial y judicial***, y otro para las ***instituciones y organismos de la UE que participan en dicha cooperación*** (véase el art. V, apartado 2, del Reglamento (CE) nº 179/1999). 2, párrs. (1) y (2))

El régimen de protección de datos aplicable a las instituciones y organismos de la UE que no participan en la cooperación policial y judicial:

Este régimen, establecido en los capítulos I a VIII del nuevo Reglamento, es **en gran medida el mismo que el establecido por el Reglamento General de Protección de Datos (RGP)** para el tratamiento sujeto a este último instrumento. Así, el Reglamento 2018/1725, al igual que el RGPD, incluye el nuevo principio de "**responsabilidad**" (art. 4(2); cf. también Art. 26) y establece las **obligaciones de los controladores y procesadores (capítulo IV), en los mismos términos que las de los controladores y procesadores sujetos al RGPD.**

Concretamente, el capítulo IV incluye disposiciones sobre el principio de "**protección de datos por diseño y por defecto**" (artículo 27); sobre las disposiciones que deben establecerse en relación con los "**responsables del tratamiento**" (artículo 28), **los encargados del tratamiento** (artículo 29) y **las personas que actúan bajo la autoridad del responsable del tratamiento o del encargado del tratamiento** (artículo 30); sobre la obligación ("relacionada con la responsabilidad") de llevar un **registro** detallado de **las actividades de tratamiento** (artículo 30). 31); sobre la **seguridad del tratamiento** (artículo 33), la **notificación de las violaciones de datos** al **Supervisor Europeo de Protección de Datos (SEPD)** (que es la autoridad de control en relación con las instituciones y órganos de la UE) (artículo 34) y la **comunicación de las violaciones de datos a los interesados** (artículo 35), todo ello en la misma línea que el RBPI.

El Reglamento 2018/1725 (al igual que su predecesor, el Reglamento 45/2001, analizado en la sección 1.3.6) exige que cada institución u organismo de la Unión nombre a un responsable de **la protección de datos (RPD)** (artículo 43), lo que también está en consonancia con el requisito del Reglamento de protección de datos en relación con los responsables del sector público. Las disposiciones sobre la **posición del RPD** (artículo 44) y sobre las **tareas del RPD** (artículo 45) también están en consonancia con el RD-PIB, con ***algunas estipulaciones adicionales*** sobre el acceso al RPD por parte de cualquier persona y la protección frente a los prejuicios por ello (artículo 2). 44)(7) y sobre la duración del nombramiento de un RPD (art. 45(8)); y en relación con la misión del RPD, una estipulación algo más estricta (que no figura en el RPD) de que el RPD "*garantizará de manera independiente la aplicación interna del presente Reglamento*" (art. 45(1)(b)).[201]

El Reglamento 2018/1725 también exige la realización de una **evaluación de impacto sobre la protección de datos (EIAP)**, en las mismas circunstancias que las previstas en el RPI, a saber en relación con el tratamiento "que pueda suponer un riesgo elevado para los derechos y libertades de las personas físicas" (artículo 39); y estipula que debe haber "**consulta previa**" con el SEPD en circunstancias similares

[200] 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 estos datos, y por el que se derogan el Reglamento (CE) nº 45/2001 y la Decisión nº 1247/2002/CE, DO L 295 de 21 de noviembre de 2018, pp. 39-98, disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725

[201] Esto es más fuerte porque, aunque el RGPD estipula que "el responsable del tratamiento y el encargado del tratamiento velarán por que el responsable de la protección de datos no reciba instrucciones sobre el ejercicio de esas tareas" y que "el responsable del tratamiento o el encargado del tratamiento no podrá despedirlo ni sancionarlo por el desempeño de sus funciones" (art. 5), el responsable del tratamiento o el encargado del tratamiento no podrán ser despedidos o sancionados por ello. 38(3) RGPD), que garantiza efectivamente que el RPD puede actuar "de forma independiente", el RGPD dice que el RPD debe "controlar el cumplimiento de[el RGPD y otras normas pertinentes]" e "informar y asesorar" al responsable del tratamiento y a sus empleados (y a cualquier transformador) de sus obligaciones (artículo 39, apartado 1, letras b) y a), respectivamente), el RGPD no exige que el RPD "garantice" el cumplimiento interno, es decir, la responsabilidad legal que le queda al responsable del tratamiento.

a las estipuladas para la consulta previa con la autoridad de control competente en el RDGP, es decir, si el ADPD indica que esos riesgos no pueden mitigarse suficientemente (artículo 40) (última frase del artículo 40 del RDGP). 40 añade que "*El responsable del tratamiento pedirá el asesoramiento del responsable de la protección de datos sobre la necesidad de una consulta previa*", pero que, por supuesto, también es aconsejable en relación con el tratamiento en el marco del RGPD.)

En cuanto al contenido sustantivo, el Reglamento 2018/1725 también se basa en las mismas ***definiciones*** (art. 3) y ***principios básicos*** (art. 4) que el Reglamento RGPD, y contiene en realidad las mismas normas sobre cuestiones como el ***consentimiento y otros fundamentos jurídicos para el tratamiento de datos no sensibles y sensibles*** (véanse los artículos 3 y 4 del Reglamento RGPD). 5 - 13), pero con más detalles sobre el "***tratamiento compatible***" (artículo 6) y sobre la ***transmisión de datos personales a los destinatarios en los Estados miembros*** (artículo 9);[202] y sobre ***los derechos de los interesados*** (artículos 14 a 24), incluso en relación con la adopción de ***decisiones y la elaboración de perfiles totalmente automatizados*** (artículo 24).

También establece esencialmente las mismas ***restricciones*** permitidas ***sobre los derechos de los interesados y sobre el deber de comunicar una violación de los datos personales al interesado*** (artículo 25, apartado 1), pero las amplía también al ***deber de garantizar la confidencialidad de las comunicaciones electrónicas*** (véase más adelante) y, lo que es más importante, establece normas más específicas sobre lo que cualquier "***acto jurídico o norma interna***" que prevea tales restricciones debe aclarar específicamente (véase el artículo 25, apartado 2, del Reglamento (CE) nº.../2004 del Parlamento Europeo y del Consejo). 25(2)). Además, el Supervisor Europeo de Protección de Datos debe ser consultado sobre los proyectos de dichas normas (apartado 2 del artículo 41), lo que constituye una garantía significativa de que se limitarán efectivamente a lo que es "*necesario y proporcionado... en una sociedad democrática*".

El Reglamento 2018/1725 incluye una sección especial (capítulo IV, sección 3) sobre la **confidencialidad de las comunicaciones electrónicas**. Esto estipula que

> Las instituciones y organismos de la Unión **garantizarán la confidencialidad de las comunicaciones electrónicas**, en particular protegiendo sus redes de comunicaciones electrónicas (artículo 36, sin cursiva en el original).

y que lo harán:

> **proteger** la información transmitida, almacenada, procesada y recogida por los equipos terminales de los usuarios que acceden a sus sitios web y aplicaciones móviles disponibles al público, de conformidad con el apartado 3 del artículo 5 de la Directiva 2002/58/CE[es decir, la Directiva sobre intimidad en las comunicaciones electrónicas, tratada en la sección 1.3.3, anterior] (artículo 37, énfasis añadido).

El último artículo de esta sección se refiere a **las guías de usuarios**, tal como se definen en el apartado 24 del artículo 3, es decir, a cualquier guía:

> una guía de usuarios a disposición del público o una guía interna de usuarios disponible en una institución u organismo de la Unión o compartida entre instituciones y organismos de la Unión, ya sea en forma impresa o electrónica.

A este respecto, el artículo 38 estipula que los datos personales contenidos en dichas guías deben "*limitarse a lo estrictamente necesario para los fines específicos de la guía*" (apartado 1 del artículo 38), y que las instituciones y organismos deben hacerlo:

> adoptar todas las medidas necesarias para evitar que los datos personales contenidos en dichas guías sean utilizados con fines de venta directa, independientemente de que sean accesibles al público o no.

Las normas de esta sección reflejan algunas de las normas de la Directiva sobre privacidad en las comunicaciones electrónicas, que se han tratado en la sección 1.3.3 anterior.

Las normas sobre **transferencias de datos personales a terceros países u organizaciones internacionales**, contenidas en el capítulo V del Reglamento 2018/1725, siguen de nuevo el mismo esquema que el que figura en el Reglamento RGPD: tales transferencias sólo pueden tener lugar:

- sobre la base de una **decisión de adecuación adoptada** por la Comisión en el marco del PBI; o
- si se proporcionan las "**garantías adecuadas**" por medio de:
  - un instrumento jurídicamente vinculante y ejecutorio entre autoridades u organismos públicos;
  - cláusulas estándar de protección de datos adoptadas por la Comisión;

[202] Véase la subsección 1.4.6, más adelante.

- cláusulas estándar de protección de datos adoptadas por el SEPD y aprobadas por la Comisión;

- en relación con las transferencias a un transformador que no sea una institución u organismo de la Unión: Reglas Corporativas Vinculantes (BCRs), códigos de conducta o certificaciones emitidas bajo el RGPD; o

a reserva de la autorización del SEPD:

- cláusulas contractuales entre las entidades pertinentes; o

- disposiciones de protección de datos insertadas en acuerdos administrativos (acuerdos) entre autoridades u organismos públicos.

- (Art. 48)

El Reglamento 2018/1725 también contiene la estipulación, idéntica a la del RGPD, de que:

> Toda sentencia de un órgano jurisdiccional y toda decisión de una autoridad administrativa de un tercer país por la que se exija a un responsable del tratamiento que transmita o divulgue datos personales sólo podrá ser reconocida o ejecutada de cualquier forma si se basa en un acuerdo internacional. (Art. 49)

Por último, a este respecto, el artículo 50 del Reglamento 2018/1725 prevé transferencias sobre la base de "**excepciones para situaciones específicas**", en las mismas líneas que las establecidas en el RBPI, es decir, cuando el interesado haya "**dado su consentimiento explícito**" a la transferencia propuesta (artículo 50, apartado 1, letra a)), o cuando la transferencia sea "**necesaria**" en un ***contexto contractual*** (artículo 50, apartado 1, letras b) y c)), por ***razones importantes de interés público reconocidas en el Derecho de la Unión*** (artículo 50, apartado 1, letra d), leído en relación con el artículo 50, apartado 1, letra d), del RBGI). 50(3)), para el establecimiento, ejercicio o defensa de ***acciones legales*** (artículo 50(1)(e), o para proteger los ***intereses vitales del interesado o de otras personas***, cuando el interesado sea física o jurídicamente incapaz de dar su consentimiento (artículo 50(1)(f); o cuando la transferencia se efectúe a partir de un **registro accesible al público** (siempre que se cumplan las condiciones de acceso) (artículo 50(1)(g)).

El Reglamento 2018/1725, al igual que el RGPD en relación con las autoridades públicas, estipula que las tres primeras de estas excepciones especiales (consentimiento expreso del interesado; contextos contractuales) "*no se aplicarán a las actividades realizadas por las instituciones y organismos de la Unión en el ejercicio de sus poderes públicos*" (art. 50(2)).

El capítulo VI del Reglamento 2018/1725 se refiere al **establecimiento, las normas, la posición, las funciones y los deberes del SEPD**. Esencialmente, el SEPD cumple, en relación con el tratamiento de datos personales por parte de las instituciones y organismos de la Unión, la misma función que las autoridades de control (autoridades de protección de datos, APD) establecidas en virtud del Reglamento sobre protección de datos personales en relación con el tratamiento de datos personales por parte de las autoridades públicas nacionales pertinentes del Estado miembro (o región de un Estado miembro) para el que son competentes.

El capítulo VII se refiere a la **cooperación entre el Supervisor Europeo de Protección de Datos y las autoridades nacionales de supervisión**, **así como a la supervisión coordinada de las mismas.** El Reglamento también, al igual que el Reglamento RGPD, **fomenta la cooperación con terceros países y organizaciones internacionales** para la protección de datos personales (artículo 51).[203]

Por último, el Capítulo VIII trata de los **remedios, la responsabilidad y las sanciones**, que también son similares a los exigidos por el RGPD. Baste señalar que cualquier interesado cuyos datos personales sean o hayan sido tratados por una institución u organismo de la UE puede presentar una reclamación ante el SEPD (artículo 63) (del mismo modo que cualquier interesado puede presentar una reclamación en virtud del RGPD ante la DPA nacional pertinente) y (de nuevo como en el caso del RGPD) tiene derecho a una indemnización por cualquier daño material o moral causado por cualquier infracción del Reglamento (artículo 65). Además, al igual que en el Reglamento RGPD, los interesados pueden estar representados en tales casos por organizaciones sin ánimo de lucro que actúen en relación con los datos personales (artículo 67), a las que el Reglamento añade una disposición adicional sobre las reclamaciones del personal de la UE (artículo 68). Por el contrario, todo funcionario de la UE que incumpla las obligaciones impuestas por el Reglamento puede ser objeto de medidas disciplinarias (art. 69).

[203] Al igual que en el RGPD, la disposición pertinente (artículo 50 del RGPD) se sitúa de forma un tanto extraña en el capítulo que trata de las transferencias de datos y no en el que trata de las tareas y competencias de las autoridades de supervisión.

El Tribunal de Justicia de la UE tiene jurisdicción sobre cualquier conflicto relacionado con el Reglamento, incluso en relación con la indemnización (artículo 64). Además, **el SEPD puede imponer multas administrativas** a las instituciones y organismos de la Unión que no cumplan lo dispuesto en el Reglamento (artículo 66) (aunque el nivel de
las multas es muy inferior al previsto en el Reglamento sobre el producto interior bruto).[204]

[204] Las multas máximas que el SEPD puede imponer a las instituciones u organismos de la UE por incumplimiento del Reglamento 2018/1725 son, respectivamente, de 25.000 euros por infracción y hasta un total de 250.000 euros al año para algunas infracciones, y de 50.000 euros por infracción y hasta un total de 500.000 euros al año para otras infracciones (véase el artículo 5, apartado 2, del Reglamento). 66(2) y (3)). Esto se compara con las multas administrativas de hasta 10.000.000 euros, o en el caso de una empresa (empresa privada), hasta el 2% del volumen de negocios total anual a nivel mundial (el que sea más alto) para algunas infracciones, y hasta 20.000.000 euros, o en el caso de una empresa, hasta el 4% del volumen de negocios total anual a nivel mundial (el que sea más alto) para otras infracciones que puedan imponerse con arreglo al Reglamento sobre el producto interior bruto (RBP) (art. 2, apartado 1, letra a). 83, apartados 4 y 5] -aunque el Reglamento sobre el producto interior bruto también permite a los Estados miembros reducir estos importes o incluso excluir totalmente a las autoridades públicas y a los organismos establecidos en su territorio de las multas administrativas (artículo 83, apartado 7) (pero las autoridades exentas de multas o sujetas a multas reducidas deben seguir estando sujetas a las facultades de las autoridades de protección de datos pertinentes de conformidad con el artículo 58, apartado 2, del Reglamento sobre el producto interior bruto).

Dado que el principal régimen de protección de datos del Reglamento 2018/1725 está tan estrechamente alineado con el Reglamento RGPD, las orientaciones y opiniones -a menudo muy detalladas y prácticas- que el Supervisor Europeo de Protección de Datos emita a las instituciones y organismos de la UE sujetos a este régimen también tendrán una importancia directa para los responsables del tratamiento que traten datos personales con arreglo al Reglamento RGPD, especialmente en el sector público, y, por lo tanto, deberán ser estudiadas atentamente por cualquier responsable de la protección de datos que trabaje para dicho responsable del tratamiento (junto, por supuesto, con las orientaciones y dictámenes de la Junta Europea de Protección de Datos, de la que forma parte del SEPD): los puntos de vista del SEPD y del EDPB se comunican entre sí).

- **El régimen de protección de datos aplicable a las instituciones y organismos de la UE que participan en la cooperación policial y judicial:**

General:

Como se ha señalado anteriormente, el Reglamento 2018/1725 crea **un régimen separado de protección de datos para las instituciones y organismos de la UE que participan en la cooperación policial y judicial** (es decir, que participan en "*actividades que entran en el ámbito de aplicación de los capítulos 4 o 5 del título V de la tercera parte del TFUE*"). Este régimen separado se establece **en el capítulo IX del Reglamento**, que comprende los artículos 70 a 95 (el apartado 2 del artículo 2 deja claro que las **definiciones** establecidas en el artículo 3 también se aplican a este capítulo).[205]
El régimen especial regula el tratamiento de "**datos personales operativos**" por parte de las instituciones u organismos competentes. Estos se definen en el apartado 2 del artículo 3 como:

> todos los datos personales tratados por los órganos u organismos de la Unión en el ejercicio de actividades comprendidas en el ámbito de aplicación de los capítulos 4 o 5 del título V de la tercera parte del TFUE, con el fin de cumplir los objetivos y tareas establecidos en los actos jurídicos por los que se crean dichos órganos u organismos.

Básicamente, el tratamiento de estos **datos personales operativos** está sujeto al régimen especial del capítulo IX, mientras que el tratamiento de todos los datos personales "no operativos", como los datos sobre recursos humanos relativos al personal de las instituciones y organismos pertinentes, está sujeto al régimen principal establecido en los capítulos anteriores del Reglamento 2018/1725, tal como se describe en el subtítulo anterior.

Bajo este subtítulo anterior, observamos que las normas para el régimen principal están estrechamente alineadas con el RGPD. Del mismo modo, las normas del capítulo IX del Reglamento 2018/1725 se ajustan a menudo a la Directiva sobre protección de datos de las autoridades policiales y aduaneras (LEDPD), examinada en la sección 1.4.3 (o a la vez a la Directiva y al RGPD y a las normas del régimen principal con arreglo al Reglamento 2018/1725), pero el capítulo IX no está tan estrechamente alineado con la LEDPD como el régimen principal con el RGPD. Las cosas pueden ser bastante complicadas.[206]
Dado que este manual está destinado a los RPD de los organismos públicos de los Estados miembros, no es necesario debatir aquí los detalles de la correspondencia o divergencia entre las normas del capítulo IX y las de la parte anterior del Reglamento 2018/1725, así como las de los principales instrumentos de protección de datos de la UE, el RD-PIB y el DEDPD. No obstante, en los siguientes epígrafes pueden señalarse dos cuestiones especiales.

Derechos, supervisión y ejecución:

En el capítulo IX **no se hace referencia** al derecho del interesado a ***ser indemnizado por los daños causados por un tratamiento ilícito*** (lo que *en su caso* significaría un tratamiento contrario a las

[205] Sobre la cuestión de si los capítulos VII y VIII se aplican a la transformación en virtud del capítulo IX, y en caso afirmativo en qué medida, véase más adelante, bajo los epígrafes "*Derechos, vigilancia y ejecución*".

[206] Por poner sólo un ejemplo: estrechamente relacionado con el nuevo principio de "responsabilidad" que se aplica a todos los instrumentos modernos de protección de datos de la UE, es el deber de los responsables del tratamiento llevar **registros**. Sin embargo, tanto el Reglamento RGPD como las normas que se aplican al régimen principal en virtud del Reglamento 2018/1725 exigen el mantenimiento de registros detallados de todas las operaciones de tratamiento (artículo 30 del Reglamento RGPD; artículo 31 del Reglamento 2018/1725), pero no exigen el mantenimiento de registros. El LEDPD requiere registros detallados y registros de detalles (arts. 24 y 25). Sin embargo, el capítulo IX del Reglamento 2018/1725 sólo exige que se lleven registros en relación con el tratamiento de datos personales operativos (artículo 88), sin mencionar los registros.

disposiciones de dicho capítulo), al derecho de los interesados a ser ***representados*** por un organismo sin ánimo de lucro o a la facultad del SEPD de imponer ***multas administrativas***.

Las disposiciones del capítulo IX mencionan repetidamente una obligación por parte de un responsable del tratamiento sujeto al capítulo IX de **informar a los interesados** de su ***derecho a presentar una reclamación ante el SEPD*** (véanse los artículos 2 y 3 del Reglamento (CE) n.º.../2004). 79, apartado 1, letra d), 80, letra f), y 81, apartado 2, y de la posibilidad de interponer ***un recurso judicial ante el Tribunal de Justicia*** (artículo 81, apartado 2). Los responsables del tratamiento sujetos al capítulo IX también pueden disponer que los **derechos de los interesados** en algunos casos se "*ejerzan a través del Supervisor Europeo de Protección de Datos*" (apartado 1 del artículo 84, es decir, sólo indirectamente, y en este caso también deben hacerlo:

> **informar al interesado de la posibilidad de ejercer sus derechos a través del** con **Supervisor Europeo de Protección de Datos** 84, arreglo al apartado 1 (artículo apartado 2)

El responsable del tratamiento también debe poner **a disposición del SEPD**, previa solicitud, los **registros de** sus operaciones de tratamiento (artículo 88, apartado 3) y **notificar al SEPD las violaciones de datos personales** (artículo 92, apartados 1 y 4).

Sin embargo, del artículo 2, apartado 2, se deduce claramente que el capítulo del Reglamento que prevé la tramitación de las reclamaciones por el SEPD y la jurisdicción del Tribunal de Justicia de la UE, así como la acción coercitiva del SEPD, también en caso de violación de datos personales (capítulo VIII), y el capítulo en el que se detallan las funciones y competencias del SEPD a este respecto (capítulo VI), no se aplica al tratamiento de datos operativos, que sólo está sujeto al capítulo IX.

Parece que, en la práctica, el SEPD asume poderes de supervisión y asesoramiento, también en relación con el tratamiento de datos personales operativos por parte de las instituciones y organismos de la UE en virtud del capítulo IX del Reglamento 2018/1725, y estará dispuesto a aceptar reclamaciones de los interesados en relación con dicho tratamiento. Queda por ver si permitirá que los interesados estén representados por ONG en tales casos, o si estará dispuesto a ordenar una compensación, o incluso a imponer multas administrativas a las instituciones y organismos pertinentes, y si el Tribunal de Justicia respaldará el ejercicio de las competencias del SEPD en relación con dicho tratamiento.

Excepciones y retrasos en la aplicación del Reglamento 2018/1725

En principio, el Reglamento 2018/1725 se aplica a ***todo el tratamiento de datos personales por parte de todas las instituciones y organismos de la Unión*** (apartado 1 del artículo 2), aunque, como hemos visto, mediante la creación de dos regímenes jurídicos distintos. Sin embargo, el Reglamento también contiene algunas excepciones a su aplicación y prevé un retraso en la aplicación de sus disposiciones en otros contextos, como se discute a continuación.

- **Exenciones:**

El apartado 4 del artículo 2 estipula que:

> **El presente Reglamento no se aplicará al tratamiento de datos personales por las misiones a que se refieren el artículo 42, apartado 1, y los artículos 43 y 44 del Tratado UE.** (énfasis añadido)

Las misiones y tareas cubiertas por la exención son las siguientes

- misiones fuera de la Unión para el mantenimiento de la paz, la prevención de conflictos y el refuerzo de la seguridad internacional de conformidad con los principios de la Carta de las Naciones Unidas (apartado 1 del artículo 42); y

- operaciones conjuntas de desarme, tareas humanitarias y de rescate, tareas de asesoramiento y asistencia militar, tareas de prevención de conflictos y mantenimiento de la paz, tareas de las fuerzas de combate en la gestión de crisis, incluidas la pacificación y la estabilización posconflicto. Todas estas tareas (Art. 43, en el que se amplía el Art. 44).

La segunda frase del artículo 43 añade que todas las operaciones y tareas mencionadas en dicho artículo "*podrán contribuir a la lucha contra el terrorismo, incluso apoyando a terceros países en la lucha contra el terrorismo en sus territorios*".

- **Retraso en la ejecución:**

Aparte de la mencionada exclusión de la aplicación del Reglamento en relación con operaciones específicas para las que pueden especificarse normas específicas, el Reglamento también establece los procesos para adaptar las operaciones de tratamiento de algunas otras instituciones y organismos de la UE al Reglamento 2018/1725, con plazos para las revisiones pertinentes (pero no para la adaptación efectiva de estas operaciones al Reglamento). Concretamente, en primer lugar, el apartado 3 del artículo 2 establece que:

> El presente Reglamento no se aplicará al tratamiento de datos personales operativos por parte de **Europol** y de la **Fiscalía Europea** hasta que se adapten los reglamentos anteriores a Lisboa que regulan sus actividades, de conformidad con[207] el artículo 98 del presente Reglamento. (énfasis añadido)

[207] Respectivamente: Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia Europea de Cooperación para el Cumplimiento de la Ley (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, DO L 135, de 24 de mayo de 2016, p. 1. 53, y el Reglamento (UE) 2017/1939 del Consejo, de 12 de octubre de 2017, relativo a la aplicación de una cooperación reforzada para la creación de la Fiscalía Europea (DO L 283 de 31 de octubre de 2017, p. 1).

Además, el artículo 98 estipula que:

1. **A más tardar el 30 de abril de 2022**, la Comisión **revisará los** actos jurídicos adoptados sobre la base de los Tratados que regulan el tratamiento de datos personales operativos por los órganos u organismos de la Unión en el ejercicio de actividades comprendidas en el ámbito de aplicación de los capítulos 4 o 5 del título V del título V del tercer TFUE[es decir, que se refieren a la cooperación policial o judicial], a fin de:

   (a) **evaluarán** su coherencia con[la Directiva relativa a la protección de datos de los servicios de seguridad (como se ha indicado en la sección 1.4.3)] y con el capítulo IX del presente Reglamento;

   (b) **identificar** cualquier divergencia que pueda obstaculizar el intercambio de datos personales operativos entre los órganos u organismos de la Unión en la realización de actividades en esos ámbitos y entre las autoridades competentes; y

   (c) **identificar** cualquier divergencia que pueda crear una fragmentación jurídica de la legislación sobre protección de datos en la Unión.

2. Sobre la base de la revisión, con el fin de garantizar una protección uniforme y coherente de las personas físicas en materia de tratamiento, **la Comisión podrá presentar las propuestas legislativas adecuadas, en particular con vistas a aplicar el capítulo IX del presente Reglamento a Europol y a la Fiscalía Europea** e incluir, en su caso, adaptaciones del capítulo IX del presente Reglamento.

   (énfasis añadido)

En otras palabras, los reglamentos relativos a las **actividades de Europol y de la OEPP**, así como de cualquier otra institución u organismo contemplado en el artículo 98, deberán ser ***revisados*** **antes del 30 de abril de 2022**, y la Comisión podrá entonces ***proponer*** nuevas normas con vistas a adaptar el tratamiento de datos personales por parte de estos organismos a la Directiva sobre el desarrollo económico de las personas con discapacidad (discutida en la sección 1.4.3) y a las normas especiales del capítulo IX del Reglamento (discutidas anteriormente). Sin embargo, **no** se ha fijado **ninguna fecha** para la adopción efectiva de estas nuevas normas, que requerirán una acción legislativa por parte del Consejo de Ministros y, posiblemente, del nuevo Parlamento Europeo, y la obtención de los dictámenes del Supervisor Europeo de Protección de Datos y del Comité Europeo de Protección de Datos, lo que llevará algún tiempo. Hasta que se modifiquen dichos reglamentos con este fin, es decir, al menos durante los próximos años, el tratamiento de datos personales por parte de Europol y de la OEPPJ (y de cualquier otra institución u organismo contemplado en el artículo 98 del Reglamento (CEE) nº 2018/1725) seguirá rigiéndose por sus propias normas de protección de datos vigentes (anteriores a 2018).

1.4.6 Transmisión de datos personales entre los distintos regímenes de protección de datos de la UE

i. Los diferentes regímenes de protección de datos

De las diversas secciones anteriores se deduce claramente que, de hecho, hay un número considerable de **regímenes de protección de datos diferentes, generales o más específicos dentro de los principales instrumentos y marcos de protección de datos de la UE**, y **algunos más fuera de ellos** (e incluso **fuera de la legislación de la UE en su conjunto**), incluidos los que se exponen a continuación. El régimen que se aplique a una determinada actividad u operación de tratamiento dependerá de la evaluación de cada una de ellas y de su finalidad específica, en particular si la cuestión es competencia de la UE o no, si tiene lugar en el sector público o privado, si en ella intervienen instituciones nacionales o de la UE que actúen en relación con asuntos económicos o penales, etc.

Normativa General de Protección de Datos:

- El régimen de RGPD aplicado al procesamiento por entidades privadas.
- El régimen de RGPD que se aplica al procesamiento por parte de entidades públicas que no están involucradas en asuntos penales, legales, de seguridad pública o de seguridad nacional (o cuando no están involucradas en tales asuntos) (por lo que la "seguridad pública" debe ser interpretada como una categoría muy limitada).

Directiva sobre la privacidad en las comunicaciones electrónicas y propuesta de Reglamento sobre la privacidad en las comunicaciones electrónicas:

- Las normas específicas aplicadas a los proveedores de servicios de comunicaciones electrónicas (y, en el futuro, a otros proveedores, como los operadores que superan las expectativas).

- Las normas específicas aplicables a todos los webhosts (incluidas las autoridades públicas con páginas web propias) en relación con la confidencialidad de las comunicaciones, el uso de "cookies", etc....

Directiva de protección de datos de las fuerzas de seguridad:

- El LEDPD se aplica a las entidades públicas ("autoridades competentes") cuando tratan datos personales "*con fines de prevención, investigación, detección o enjuiciamiento de delitos o de ejecución de sanciones penales, incluida la protección y la prevención de amenazas a la seguridad pública*", ya sea como tarea principal u ocasionalmente, aparte de otras tareas públicas.

Áreas exentas del LEDPD (por el momento):

- Las normas de los aproximadamente 123 instrumentos jurídicos de la UE relativos a lo que antes se denominaba "Justicia y Asuntos de Interior" (JAI) entraron en vigor antes del 6 de mayo de 2016 (que siguen aplicándose aunque todavía no se ajusten al LEDPD).

- Las normas de los "*acuerdos internacionales que implican la transferencia de datos personales a terceros países u organizaciones internacionales celebrados por los Estados miembros antes del 6 de mayo de 2016 y que se ajustan al Derecho de la Unión aplicable antes de esa fecha*" (que también siguen aplicándose aunque todavía no se ajusten al LEDPD).

- Las normas sobre la utilización de "*sistemas de tratamiento automatizado creados antes del 6 de mayo de 2016*" en los Estados miembros, si todavía no se han adaptado a la Directiva porque ello habría supuesto un "*esfuerzo desproporcionado*".

Tratamiento de datos personales en el ámbito de la PESC:

- Tramitación por el Alto Representante de la UE para Asuntos Exteriores y Política de Seguridad, el Servicio Europeo de Acción Exterior (SEAE) y las 141 delegaciones de la UE en todo el mundo, y el Servicio de Instrumentos de Política Exterior (SIF) y tramitación por los Estados miembros en relación con estos asuntos (incluida la adopción de decisiones del Consejo en el ámbito de la PESC), *que todavía no están sujetos a ningún instrumento específico de protección de datos de la UE*. [Pero fíjense en el tercer guión bajo el siguiente encabezado]

Tratamiento de datos personales por las instituciones u organismos de la UE con arreglo al Reglamento 2018/1725:

- El régimen de protección de datos aplicable a las instituciones y organismos de la UE que no participan en la cooperación policial y judicial.

- El régimen de protección de datos aplicable a las instituciones y organismos de la UE que participan en la cooperación policial y judicial.

- Tratamiento por la Secretaría del Consejo en la aplicación de las decisiones del Consejo de la PESC: el ámbito de actividad limitado relativo a la PESC que está sujeto a las normas de protección de datos, es decir, al Reglamento 2018/1725.

Zonas exentas del Reglamento 2018/1725 (por el momento):

- Tratamiento de datos personales por las misiones de la UE destinadas al **mantenimiento de la paz**, la prevención de conflictos y el refuerzo de la seguridad internacional, o encargadas de **operaciones** conjuntas de **desarme**, **humanitarias y de rescate**, de tareas de asesoramiento y asistencia militar, de **tareas de prevención de conflictos y de mantenimiento de la paz**, de tareas de **fuerzas de combate en la** gestión de **crisis**, incluidas las de establecimiento de la paz y de **estabilización posconflicto** (incluso cuando dichas tareas se refieran a la lucha contra el terrorismo, incluido el apoyo a terceros países en la lucha contra el terrorismo en sus territorios).

- El tratamiento de datos personales por parte de Europol y de la Oficina del Fiscal Europeo (OPPE) y de otros "*órganos u organismos de la Unión en el ejercicio de actividades comprendidas en el ámbito de aplicación de los capítulos 4 o 5 del título V del tercer TFUE[es decir, que se refieren a la cooperación policial o judicial]*", que seguirá teniendo lugar sobre la base de los instrumentos

jurídicos de la UE relativos a Europol o a la OPPE, o de otro modo, a la cooperación policial o judicial, adoptados con anterioridad al Reglamento 2018/1725.

Seguridad nacional:

- El tratamiento de datos personales por parte de los Estados miembros en relación con la seguridad nacional, **que está totalmente fuera del ámbito de aplicación de la legislación de la UE**, e incluso de la Carta de los Derechos Fundamentales (aunque, por supuesto, dicho tratamiento está sujeto al Convenio Europeo de Derechos Humanos y a la jurisdicción del Tribunal Europeo de Derechos Humanos).[208]
-

No siempre es fácil trazar líneas claras entre estos muchos regímenes diferentes, por ejemplo, entre la acción policial contra la delincuencia, la acción policial para garantizar el orden, las acciones de la policía y otras autoridades para garantizar la "seguridad interior", la "seguridad pública" y la "seguridad nacional", y entre estas acciones y las acciones de la UE en relación con el "terrorismo",[209] las tareas de las misiones de la UE antes mencionadas y la "seguridad internacional".

Este no es el lugar para explorar estas distinciones en profundidad. Baste señalar que, cuando se aplican regímenes diferentes a las distintas actividades (actividades que corresponden a más de una de las categorías anteriores), tal vez incluso por los mismos agentes, será importante que los agentes pertinentes, en su calidad de responsables del tratamiento (y a menudo también como encargados del tratamiento, por ejemplo, al apoyar a otros agentes de este tipo), **aclaren por sí mismos qué régimen jurídico se aplica a qué operación de tratamiento de datos personales y a qué datos personales, mediante el análisis de cada una de las operaciones de tratamiento de datos específicas en cuestión.** La legalidad del tratamiento y el alcance y las excepciones a cuestiones tan importantes como los derechos de los interesados dependen siempre de manera crucial de tales aclaraciones.

Las autoridades públicas que participan en diferentes actividades sujetas a diferentes regímenes de protección de datos deben distinguir siempre cuidadosamente sus diferentes actividades, las diferentes operaciones de tratamiento y los diferentes datos personales utilizados para las diferentes operaciones en sus registros de tratamiento de datos personales y en sus evaluaciones de dicho tratamiento.[210] Los responsables de la protección de datos de estos organismos públicos tendrán que desempeñar un papel crucial a este respecto.[211]

[208] El Tribunal Europeo de Derechos Humanos ha dictado varias sentencias importantes a este respecto. Ver: División de Investigación del Tribunal Europeo de Derechos Humanos, *Seguridad nacional y jurisprudencia europea*, Consejo de Europa, 2013, disponible en: https://www.echr.coe.int/Documents/Research_report_national_security_ENG.pdf

[209] Véase John Vervaele, *Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law?* in: Utrecht Law Review, volumen 1, número 1 (septiembre de 2005), disponible en: http://www.utrechtlawreview.org/

[210] Véase el artículo 74 del Reglamento 2018/1725 sobre la relación entre los datos personales operativos y la verificación de la calidad de los datos personales operativos, que es un buen ejemplo de lo que debería ser una buena práctica general cuando un responsable del tratamiento realiza actividades sujetas a diferentes regímenes de protección de datos.

[211] Vea la Tercera Parte de este manual.

ii. Transmisión de datos personales

Surgen problemas especiales cuando se propone o se solicita que los datos personales obtenidos para un fin determinado con arreglo a las normas de uno de los regímenes jurídicos mencionados sean utilizados por el mismo responsable del tratamiento para un fin distinto, para su tratamiento con arreglo a un régimen jurídico distinto, o que sean transmitidos o puestos a disposición de otro organismo (otro responsable del tratamiento) para un fin distinto, para su tratamiento con arreglo a un régimen jurídico distinto.[212]

Por ejemplo, el departamento de educación de una autoridad local puede recopilar datos personales sobre los escolares con fines educativos, en el marco del RGPD, pero su agencia de policía local puede solicitar el acceso a (algunos de) esos datos, para ayudar a resolver la delincuencia local (por ejemplo, para comprobar qué niños han estado ausentes de la escuela en un día determinado). El tratamiento propuesto de los datos para el segundo propósito se realizaría en el marco del DIPD (o, para ser más precisos, de las disposiciones legales nacionales por las que se transpone el DIPD, así como en el marco de la legislación pertinente en materia de policía o de procedimiento penal). A veces, las leyes o las normas legales aplicables aclaran cuándo pueden tener lugar tales revelaciones (por ejemplo, sólo en relación con ciertos delitos, o sólo si había sospechas razonables contra niños identificados, o sólo si un juez emitió una orden judicial). Sin embargo, a menudo, esta es una cuestión que debe decidir la autoridad local competente a la luz de las normas de los distintos instrumentos aplicables. **El RPD de la autoridad local desempeñará un papel importante en el asesoramiento sobre este asunto (y deberá consultar al APD en caso de duda).**

El Reglamento 2018/1725 proporciona alguna orientación sobre las transmisiones de datos personales por parte de una institución u organismo de la UE a "*destinatarios establecidos en la Unión distintos de las instituciones y organismos de la Unión*", que suelen ser las autoridades públicas de los Estados miembros. Las instituciones y organismos de la UE están autorizados a transmitir datos a una entidad de un Estado miembro que solicite los datos facilitados:

(a) el destinatario[es decir, la entidad de un Estado miembro que solicita los datos] establece que los datos son necesarios para el desempeño de una tarea realizada en interés público o en el ejercicio del poder público conferido al destinatario[es decir, a esa entidad]; o bien

(b) el destinatario establece que es necesario que los datos se transmitan para un fin específico de interés público y el responsable del tratamiento[es decir, la institución u organismo de la UE a la que se solicitan los datos], cuando haya motivos para suponer que los intereses legítimos del interesado podrían verse perjudicados, establece que es proporcionado transmitir los datos personales para ese fin específico después de haber sopesado de forma demostrable los diversos intereses en conflicto.

(Art. 9(1))

Las instituciones u organismos de la UE pueden transmitir (enviar) tales datos a entidades de los Estados miembros sin que se les pida, es decir, de oficio, si pueden:

demostrar que la transmisión de datos personales es necesaria y proporcionada a los fines de la transmisión, aplicando los criterios establecidos en el apartado 1, letras a) o b).

(Art. 9(2))

Sin embargo, hay que tener en cuenta varias cuestiones a este respecto. En primer lugar, lo anterior se aplica a las instituciones y organismos de la UE que no participan en el tratamiento en relación con la cooperación policial y judicial, es decir, sólo se aplica al tratamiento -y a las transmisiones- en el marco del "régimen principal" establecido por el Reglamento 2018/1725 para las instituciones y organismos de la UE; y, como se ha señalado en la sección 1.4.5, el régimen "principal" de protección de datos de dicho Reglamento está estrechamente alineado con el Reglamento RGPD. En el capítulo IX del Reglamento

[212] Obsérvese que las transmisiones de datos que aquí se tratan son diferentes de las transmisiones de datos personales realizadas por una entidad a otra entidad en el mismo país o en otro Estado miembro para los mismos fines, con arreglo al mismo régimen de protección de datos[de la UE] - por ejemplo, por parte de un organismo encargado de la aplicación de la ley en un Estado miembro a otro LEA en ese Estado miembro o a un LEA en otro Estado miembro-, y de las transferencias de datos personales a terceros países (que están sujetas a las normas especiales sobre tales transferencias, pero hay que tener en cuenta que éstas difieren también entre los diferentes regímenes).

2018/1725 no existe ninguna disposición correspondiente sobre la transmisión de datos personales a organismos de los Estados miembros, que cubre el tratamiento de datos personales "operativos" por parte de las instituciones y organismos de la UE que participan en la cooperación policial y judicial.

En segundo lugar, las normas del artículo 9, citado anteriormente, se entienden "sin perjuicio" de los principios fundamentales de la protección de datos, incluida la limitación de la finalidad y la norma sobre el tratamiento "compatible" (véase el artículo 6 del Reglamento, que añade condiciones significativas), la pertinencia de los datos, etc., y de las estipulaciones sobre el tratamiento lícito (véase la cláusula introductoria del apartado 1 del artículo 9). Asimismo, se entenderán sin perjuicio de las normas especiales sobre el tratamiento de datos personales sensibles (*ídem*).

No obstante, el artículo 9 del Reglamento 2018/1725 ilustra que **siempre que los datos personales tratados en el marco de uno de los regímenes mencionados deban transmitirse a otra entidad (o incluso ser utilizados por la misma entidad) para su tratamiento en el marco de otro régimen, deben abordarse cuestiones importantes sobre la especificación de la finalidad, la pertinencia y la adecuación de los datos, así como sobre la legalidad, la necesidad y la proporcionalidad de la modificación de la finalidad.**

A este respecto, es fundamental recordar, en primer lugar, que la "transmisión" de datos, al igual que cualquier otra forma de "divulgación" de datos personales (incluida la "puesta a disposición de[datos personales]", por ejemplo, en línea), constituye una forma de tratamiento (véase el art. IV, apartado 1, del Convenio de Estocolmo). 4(2) RGPD, repetido *literalmente* en todos los demás instrumentos de protección de datos de la UE). En segundo lugar, es crucial que cualquier "transmisión" de datos personales entre diferentes entidades tenga siempre dos aspectos:

- para la entidad transmisora, es una forma de **divulgación** de los datos (véase más arriba); pero
- para la entidad receptora, constituye la **recogida de** datos personales, que es un acto separado cubierto por el concepto general de "tratamiento", distinto de la "divulgación", "transmisión" o "puesta a disposición" de datos personales.

Si, en relación con sus respectivas actividades relacionadas con la transmisión de los datos, las dos entidades están sujetas a regímenes de protección de datos diferentes, cada una de ellas debe evaluar la compatibilidad de su acción pertinente con las normas de protección de datos que le son aplicables.

Así, en el ejemplo anterior, el departamento educativo local estará sujeto a la RGPD y a cualquier "especificación adicional" sobre cómo deben aplicarse las disposiciones de la RGPD, establecida en la ley nacional de protección de datos pertinente (o tal vez en una sección apropiada de la ley sobre las tareas y competencias de los departamentos educativos locales, que debería seguir estando en línea con la RGPD).

Por otra parte, la agencia de policía local estará sujeta a las disposiciones legales nacionales adoptadas para aplicar el LEDPD (así como a cualquier norma pertinente de las leyes nacionales de policía o de procedimiento penal, que debería estar en consonancia con el LEDPD).

En ese caso, el departamento educativo local debe comprobar (con la ayuda de su responsable de la protección de datos y, si es necesario, con el asesoramiento de la autoridad de protección de datos pertinente) si las normas de protección de datos a las que está sujeto le permiten revelar los datos personales a la agencia de policía (o no, o si está sujeto a qué condiciones).

Por el contrario, antes de solicitar los datos al departamento de educación, la agencia de policía local debe comprobar (con la ayuda de su responsable de la protección de datos y, en caso necesario, con el asesoramiento de la autoridad de protección de datos pertinente) si las normas de protección de datos a las que está sujeta le permiten solicitar o exigir los datos personales a la autoridad de educación local (o no, o con sujeción a qué condiciones).

A menudo será útil que los dos RPD debatan estas cuestiones entre ellos (y consulten conjuntamente al APD cuando proceda).

A menudo, las normas pertinentes serán compatibles entre sí y se referirán entre sí. Por ejemplo, la ley de policía puede establecer cuándo y bajo qué condiciones la agencia de policía local puede pedir información a "otras autoridades públicas" (en general, y/o sobre niños); y las normas aplicables al departamento de educación pueden estipular que el departamento puede - o debe - proporcionar información solicitada por "otra autoridad

pública" (o específicamente por la policía), siempre que la solicitud sea legal. Ello requeriría que el organismo policial siguiera las normas y cumpliera las condiciones pertinentes, y que el departamento de educación pidiera al menos garantías (y pruebas) de que la solicitud presentada por la policía es legal y cumple las condiciones pertinentes. Pero aparte de estas cuestiones, no hay ningún problema en lo que respecta a la transmisión de los datos.

Cuando tanto el organismo transmisor como el organismo solicitante están sujetos a las últimas normas de protección de datos de la UE descritas anteriormente -en particular, la RGPD, el LEDPD y el Reglamento 2018/1725-, normalmente no debería haber problemas en este sentido (aunque los casos individuales pueden requerir aún un análisis y una atención serios).

Las cuestiones son menos claras cuando una entidad -en particular una entidad solicitante- no está sujeta a las normas más recientes, sino sólo a normas heredadas menos exigentes, aunque éstas seguirán basándose al menos en los principios generales de protección de datos en los que se basa toda la legislación de protección de datos de la UE.

Sin embargo, en la práctica, las cosas pueden complicarse seriamente cuando una entidad solicitante no está sujeta a ninguna norma adecuada de protección de datos, como es el caso, como hemos visto, en relación con asuntos de la PESC, asuntos relacionados con el mantenimiento de la paz de la UE u otras misiones militares, o con la seguridad nacional. En este contexto, las normas "apropiadas" son normas que se basan claramente en los principios generales de protección de datos y los reconocen; que se apartan de las normas ordinarias basadas en esos principios sólo en la medida específicamente estipulada en un instrumento jurídico pertinente (disponible al público, claro y preciso) que sea "previsible" en su aplicación, y sólo en la medida en que sea "estrictamente necesario" para el fin pertinente, y que tales desviaciones sean claramente "proporcionadas" al contexto[213] especial; y que prevean el control del cumplimiento de las normas especiales por una autoridad independiente[214].

Este no es el lugar para discutir esto en detalle. Pero se pueden hacer algunos comentarios generales.

Así pues, cualquier transmisión de datos personales por parte de una autoridad pública nacional (o de una institución u organismo de la UE) que esté sujeta a las últimas normas de protección de datos de la UE (es decir, el RGPD, el LEDPD o el Reglamento 2018/1725) a cualquier entidad nacional o de la UE que no esté sujeta a ninguna ley de protección de datos adecuada es potencialmente tan erosiva de la protección de datos de la UE como lo es cualquier transferencia de tales datos a un país que no cuente con normas de protección de datos adecuadas ("adecuadas"), lo que en principio está prohibido, a menos que se adopten las "salvaguardas oportunas" (véase el capítulo V de la Directiva de protección de datos de la UE).

Las entidades sujetas a cualquiera de los últimos instrumentos de protección de datos de la UE mencionados anteriormente deben, por tanto, tener cuidado antes de facilitar los datos personales que tratan con arreglo a dichos instrumentos a una entidad solicitante que no esté sujeta a ninguna norma adecuada en materia de protección de datos. Deberían comprobar cuidadosamente -como siempre, con la ayuda de su RPD y, en caso necesario, consultando al APD pertinente- si el instrumento que se les aplica permite (en absoluto) tal transferencia, la prohíbe o le impone condiciones; y deberían negarse a transmitir los datos a menos que el instrumento que se les aplica lo permita, en términos suficientemente claros.

No basta con que una entidad solicitante que no esté sujeta a las normas de protección de datos adecuadas indique a la entidad requerida que se le permite (la entidad solicitante) obtener (recopilar) los datos que solicita con arreglo a las normas que se aplican a dicha agencia solicitante: esto puede legitimar la recogida de datos con arreglo a dichas normas, pero no legitima la divulgación de datos ("transmisión") por parte de la entidad solicitada con arreglo a las normas de protección de datos que se aplican a la entidad solicitada (especialmente si esas normas se establecen o se adoptan con arreglo a los últimos instrumentos de protección de datos de la UE antes mencionados).

A veces, los Estados todavía tienen leyes que otorgan a algunas de sus agencias -en particular, a sus **agencias de inteligencia**- el derecho a exigir información o acceso a la información, incluidos los datos personales, en los términos más amplios; y a veces, las leyes están redactadas de tal manera que anulan cualquier restricción sobre

[213] Estos son los requisitos del Estado de Derecho desarrollados por el Tribunal Europeo de Derechos Humanos y aplicados igualmente por el Tribunal de Justicia de la UE y reflejados en la Carta de los Derechos Fundamentales de la UE (CFR), que debe ser respetada por cualquier Estado democrático en cualquier actividad que pueda afectar a los derechos y libertades fundamentales de la persona.
[214] Tal como se establece expresamente en el Art. 8(3) CFR.

la revelación de información personal por parte de otras entidades que están sujetas a las leyes de protección de datos, y que (las leyes demasiado amplias estipulan) deben cumplir con tales demandas independientemente de lo que digan las normas de protección de datos relevantes que normalmente se aplican a ellas. Esto incluye las leyes de los Estados miembros.[215]

Por lo que se refiere a las agencias nacionales de seguridad, el Estado miembro en cuestión puede alegar que las normas con arreglo a las cuales dichas agencias pueden exigir información (o acceso a bases de datos) quedan fuera del ámbito de aplicación del Derecho de la UE, por lo que la transmisión de datos a dichas agencias con arreglo a sus normas también queda fuera del ámbito de aplicación del Derecho de la UE y queda fuera del ámbito de aplicación del Derecho comunitario y de las competencias de las autoridades de protección de datos o del Tribunal de Justicia de la UE.

Pero eso sería una interpretación errónea de la situación legal. Incluso si la recogida de información personal por parte de dichas agencias está fuera del ámbito de aplicación de la legislación de la UE (o de las competencias de la APD o del TJUE), la transmisión de los datos a dichas agencias por parte de cualquier entidad que esté sujeta a los instrumentos de protección de datos de la UE está dentro del ámbito de aplicación de la legislación de la UE. Los controladores de dichas entidades y sus RPD deben ser conscientes de ello y consultar a sus APD cuando surjan tales casos contenciosos.

1.4.7 El Convenio "Modernizado" del Consejo de Europa para la protección de datos de 2018

Aunque el Convenio del Consejo de Europa de 1981 se ajustó (en términos generales) a la Directiva de protección de datos de la CE de 1995, mediante la adición de reglas sobre flujos de datos transfronterizos y autoridades independientes de protección de datos en su Protocolo adicional, adoptado en 2001 (según lo discutido en 1.3.2, arriba), todavía, como esa Directiva, se estaba desactualizando en cierto modo a fines de la primera década del siglo XXI. El trabajo para "modernizar" el Convenio comenzó en 2011, y el "Convenio Modernizado" fue adoptado y abierto a la firma el 18 de octubre de 2018.[216] En el momento de redactar este documento, aún no ha entrado en vigor: eso sucederá tres meses después de que cinco Estados miembros del Consejo de Europa se hayan adherido al Convenio Modernizado (Art. 26 (2)) - pero por supuesto incluso de esa manera solamente respecto de dichos Estados miembros; con respecto a otros Estados-partes en el Convenio de 1981 (y, cuando corresponda, su Protocolo adicional), el antiguo Convenio (y el Protocolo) continuará aplicándose.[217]

El propio Consejo de Europa ha proporcionado un **resumen muy útil de lo que es nuevo en el Convenio Modernizado**, que se proporciona a continuación:[218]

> Las principales novedades[219] del Convenio modernizado se pueden presentar de la siguiente manera:
>
> **<u>Objeto y finalidad del Convenio (artículo 1):</u>**
> En virtud del artículo 1, el objetivo del Convenio está claramente subrayado, es decir, garantizar a todas las personas dentro de la jurisdicción de una de las Partes

---

[215] Véase Douwe Korff y otros, Boundaries of Law (nota 172, anterior), parte 4.

[216] Véase: https://www.coe.int/en/web/data-protection/background-modernisation
El Convenio modernizado estaba preparado en 2014, pero su apertura formal a la firma se retrasó, en parte para facilitar la coherencia con el RGPD, y en parte para abordar cuestiones planteadas por un Estado miembro del Consejo de Europa relevante.
El *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, CETS 223, está disponible en: https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/223
El texto consolidado del Convenio modernizado está disponible en:
https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf –

[217] A mediados de diciembre de 2018, el Convenio modernizado había sido firmado por 22 estados, pero no había sido ratificado por ninguno.
Véase: https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/223/signatures?p_auth=ZmXAeCCF
El Relator Especial de la ONU sobre el Derecho a la Privacidad ha recomendado la ratificación mundial del Convenio "modernizado" desde 2018.

[218] Tomado de: https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808acCons.8
Los detalles completos de todos los cambios textuales específicos en forma de gráfico comparativo están disponibles en https://rm.coe.int/cahdata-convention-108-table-e-april2018/16808ac958 (26 páginas)

[219] Este [resumen] presenta las novedades y no repite las disposiciones ya existen desde la Convención de 1981 y su Protocolo adicional de 2001. Para una vista completa de la Convención modernizada, lea la versión consolidada publicada en el sitio web [del Consejo de Europa]. (Nota original con ediciones)

(independientemente de su nacionalidad o lugar de residencia) la protección de sus datos personales cuando se procesan, contribuyendo así al respeto, por sus derechos y libertades fundamentales, y en particular su derecho a la privacidad.

Con esta redacción, el Convenio destaca el hecho de que el tratamiento de datos personales puede permitir positivamente el ejercicio de otros derechos y libertades fundamentales, lo que puede facilitarse garantizando el derecho a la protección de datos.

Definiciones y ámbito de aplicación (artículos 2 y 3)
Si bien las nociones esenciales, como la definición de datos personales y la de los sujetos de datos no se modifican en absoluto[220], se proponen otros 127 cambios en las definiciones: se abandona el concepto de "archivo". "Controlador de un archivo de datos" se reemplaza por "controlador de datos", además de que se utilizan los términos "procesador" y "destinatario".

El ámbito de aplicación incluye tanto el tratamiento automatizado como el no automatizado de datos personales (tratamiento manual en el que los datos forman parte de una estructura que permite la búsqueda por parte del interesado de acuerdo con criterios predeterminados) que está bajo la jurisdicción de una parte a la convención. La naturaleza general de la Convención se conserva y el alcance, naturalmente, continúa cubriendo el tratamiento en los sectores público y privado de manera indistinta, ya que esta es una de las grandes fortalezas de la Convención.

Por otro lado, el Convenio ya no se aplica al tratamiento de datos realizado por una persona física para el ejercicio de actividades puramente personales de nuestro hogar.[221]

Además, a las Partes ya no se les brinda la posibilidad de hacer declaraciones destinadas a eximir de la aplicación del Convenio ciertos tipos de tratamiento de datos (por ejemplo, seguridad nacional y fines de defensa).

Deberes de las Partes (artículo 4)
Cada Parte debe adoptar en su legislación nacional las medidas necesarias para dar cumplimiento a las disposiciones del Convenio.

Además, cada Parte debe demostrar que tales medidas se han tomado y son efectivas y aceptar que el Comité del Convenio puede verificar que se cumplan estos requisitos. Este proceso de evaluación [nuevo] de las Partes (“mecanismo de seguimiento”) es necesario para garantizar que las Partes realmente puedan garantizar el nivel de protección establecido por el Convenio.

Es importante tener en cuenta que las organizaciones internacionales ahora tienen la posibilidad de adherirse a la Convención (artículo 27), al igual que la Unión Europea (artículo 26).

Legitimidad del tratamiento de datos y calidad de los datos (Artículo 5)
El artículo 5 aclara la aplicación del principio de proporcionalidad para subrayar que debe aplicarse durante todo el amiento, y en particular con respecto a los medios y métodos utilizados en el tratamiento. Además, está reforzado por el principio de minimización de datos.

Se introduce una disposición nueva para establecer claramente la base legal del tratamiento: el consentimiento (que debe ser válido debe satisfacer varios criterios) del interesado o alguna otra base legítima establecida por la ley (contrato, interés vital de los datos), asunto, obligación legal del controlador, etc.).

[220] Pero téngase en cuenta que se ha agregado una amplia glosa en el Memorando Explicativo de la Convención Modernizada (nota añadía).
[221] Este "tratamiento puramente personal" se excluyó por primera vez de las normas de protección de datos en la Directiva de protección de datos de 1995, con el fin de garantizar el respeto del derecho a la vida privada; Se repite en el RGPD. (Nota añadida).

Datos confidenciales (artículo 6)
El catálogo de datos confidenciales se ha ampliado para incluir datos genéticos y biométricos (que influyeron en la UE), así como datos tratados para la información que revelan en relación con la afiliación sindical o el origen étnico (esas dos últimas categorías se están agregando a las existentes). [en principio] prohibición del tratamiento de datos personales que revelen el origen racial, las opiniones políticas o las creencias religiosas o de otro tipo, la salud o la vida sexual y los datos personales relacionados con delitos, procesos penales y condenas.

Seguridad de los datos (artículo 7)
En términos de seguridad de datos, se introduce el requisito de notificar, sin demora, cualquier infracción de seguridad. Este requisito se limita a los casos que pueden interferir seriamente con los derechos y libertades fundamentales de los interesados, los cuales deben ser notificados, al menos, a las autoridades de supervisión.

Transparencia del tratamiento (artículo 8)
Los controladores tendrán la obligación de garantizar la transparencia del tratamiento de los datos y, para ello, deberán proporcionar un conjunto de información requerida, en particular en relación con su identidad y lugar de residencia o establecimiento habitual, sobre la base legal y los fines del procesado, los destinatarios de los datos y en las categorías de datos personales tratados. Además, deben proporcionar cualquier información adicional necesaria para garantizar un tratamiento justo y transparente. El Controlador está exento de proporcionar dicha información cuando el tratamiento esté expresamente establecido por la ley o esto resulte imposible o implique esfuerzos desproporcionados.

Derechos del titular de los datos (artículo 9)
A los titulares de los datos se les otorgan derechos nuevos para que tengan un mayor control sobre sus datos en la era digital.

El Convenio modernizado amplía el catálogo de información que se transmite a los interesados cuando ejercen su derecho de acceso. Además, los titulares de los datos tienen derecho a conocer el razonamiento que subyace en el tratamiento de los datos, cuyos resultados se aplican a él/ella. Este nuevo derecho es particularmente importante en términos de perfiles de individuos.[222]

Debe asociarse con otra novedad, a saber, el derecho a no estar sujeto a una decisión que afecte al sujeto de los datos, que se basa únicamente en un tratamiento automatizado, sin que el interesado tenga sus opiniones en cuenta.

Los titulares de datos tienen el derecho de objetar en cualquier momento que sus datos personales sean tratados, a menos que el controlador demuestre razones legítimas y convincentes para el tratamiento que invalida sus intereses o derechos y libertades fundamentales.

Obligaciones adicionales (artículo 10)
El Convenio modernizado impone obligaciones más amplias a aquellos que procesan datos o que tienen datos tratados en su nombre.

La responsabilidad se convierte en una parte integral del esquema de protección, con la obligación de que los controladores puedan demostrar el cumplimiento de las reglas de protección de datos.

Los controladores deben tomar todas las medidas apropiadas, incluso cuando el tratamiento se subcontrata, para garantizar que se garantice el derecho a la protección de datos (privacidad por

[222] Sobre este tema, véase la Recomendación (2010) 13 sobre la protección de las personas en relación con el tratamiento automático de datos personales en el contexto de la elaboración de perfiles y su memorando explicativo. (Nota original)

diseño, análisis del posible impacto del tratamiento de datos previsto en los derechos y libertades fundamentales de los interesados ("evaluación del impacto de la privacidad" y privacidad por defecto).

Excepciones y restricciones (artículo 11)
Los derechos establecidos en el Convenio no son absolutos y pueden limitarse cuando así lo prescribe la ley y constituyen una medida necesaria en una sociedad democrática sobre la base de motivos específicos y limitados. Entre esos motivos limitados se incluyen ahora "objetivos esenciales de interés público", así como una referencia al derecho a la libertad de expresión.

La lista de disposiciones del Convenio que pueden restringirse se ha ampliado ligeramente (véanse las referencias a los artículos 7.1 sobre seguridad y 8.1 sobre transparencia en el artículo 11.1) y el párrafo nuevo de este artículo trata específicamente las actividades de tratamiento con fines de seguridad nacional y defensa, para lo cual se pueden limitar los poderes de "supervisión" del Comité, así como algunas misiones de las autoridades de supervisión. El requisito de que las actividades de tratamiento para fines de seguridad y defensa nacional estén sujetas a una revisión y supervisión independientes y efectivas está claramente establecido.

Es importante recordar una vez más que, contrariamente a las disposiciones anteriores del Convenio 108, las Partes en el Convenio modernizado ya no podrán excluir del ámbito de aplicación del Convenio ciertos tipos de tratamiento.

Flujos transfronterizos de datos personales (artículo 14)[223]

El objetivo de esta disposición es facilitar, cuando corresponda, el libre flujo de información independientemente de las fronteras, al tiempo que se garantiza una protección adecuada de las personas con respecto al tratamiento de datos personales.

En ausencia de normas armonizadas de protección compartidas por los Estados que pertenecen a una organización internacional regional y que gobiernan los flujos de datos (véase, por ejemplo, el marco de protección de datos de la Unión Europea), los flujos de datos entre las Partes deberían funcionar libremente.

Con respecto a los flujos transfronterizos de datos a un receptor que no está sujeto a la jurisdicción de una Parte, se debe garantizar un nivel apropiado de protección en el Estado u organización receptor. Como esto no puede suponerse ya que el receptor no es una Parte, el Convenio establece dos medios principales para garantizar que el nivel de protección de datos sea realmente adecuado; ya sea por ley, o por salvaguardias estandarizadas ad hoc o aprobadas que son legalmente vinculantes y ejecutables (en particular cláusulas contractuales o reglas corporativas vinculantes), así como debidamente implementadas.

Autoridades de supervisión (artículo 15)
Sobre la base del artículo 1 del protocolo adicional, el Convenio modernizado complementa el catálogo de los poderes de las autoridades con una disposición que, además de sus poderes para intervenir, investigar, entablar procesos judiciales o informar a las autoridades judiciales sobre violaciones de disposiciones de protección de datos, las autoridades también tienen el deber de crear conciencia, brindar información y educar a todos los participantes (datos, controladores, procesadores, etc.). También permite a las autoridades tomar decisiones e imponer sanciones. Además, se recuerda que las autoridades de supervisión deben ser independientes en el ejercicio de estas tareas y poderes.

Formas de cooperación (artículo 17)
El Convenio modernizado también aborda el tema de la cooperación (y la asistencia mutua) entre las autoridades de supervisión.

[223] A este respecto, la Convención Modernizada se basa en el Protocolo Adicional y las normas de la UE.

Las autoridades de supervisión tienen que coordinar sus investigaciones, llevar a cabo acciones conjuntas y proporcionarse información y documentación sobre sus leyes y prácticas administrativas relacionadas con la protección de datos.

La información intercambiada entre las autoridades de supervisión incluirá datos personales solo cuando dichos datos sean esenciales para la cooperación o cuando el interesado haya dado el consentimiento específico, libre e informado.

Las autoridades de supervisión tienen que coordinar sus investigaciones, llevar a cabo acciones conjuntas y proporcionarse información y documentación sobre sus leyes y prácticas administrativas relacionadas con la protección de datos.

La información intercambiada entre las autoridades de supervisión incluirá datos personales solo cuando dichos datos sean esenciales para la cooperación o cuando el interesado haya dado el consentimiento específico, libre e informado.

Por último, el Convenio proporciona un foro para una mayor cooperación: las autoridades de supervisión de las Partes tienen que formar una red para organizar su cooperación y realizar sus tareas según lo especificado por el Convenio.

Comité del Convenio (artículos 22, 23 y 24)
El Comité del Convenio desempeña un papel crucial en la interpretación del Convenio, alentando el intercambio de información entre las Partes y desarrollando normas de protección de datos.

El rol y los poderes de este Comité se fortalecen con el Convenio Modernizado. Ya no se limita a una función "consultiva", sino que también tiene poderes de evaluación y supervisión. [Aparte de proporcionar] opinión [es] sobre el nivel de protección de datos provisto por un estado [como antes, ahora también lo hará con respecto a] organización internacional [s] antes de la adhesión al Convenio. El Comité también puede [ahora] evaluar el cumplimiento de la legislación nacional de la Parte interesada y determinar la efectividad de las medidas adoptadas (existencia de una autoridad de supervisión, responsabilidades, existencia de recursos legales efectivos).

También es capaz de evaluar si las normas legales que rigen las transferencias de datos proporcionan una garantía suficiente de un nivel adecuado de protección de datos.

Este no es el lugar para analizar estas novedades en detalle. Basta con señalar que **acercan el nuevo régimen de la Convención, "modernizado" al nuevo régimen establecido para la UE bajo el RGPD**. Esto significa que cuando la UE evalúe la "adecuación" de un régimen de protección de datos en un tercer país (como se analiza en la Parte Dos, sección 2.1), el hecho de que ese tercer país sea parte del Convenio Modernizado sería un asunto importante para ser tenidos en cuenta.

De hecho, en términos del **alcance**, el Convenio Modernizado excede el RGPD, ya que, como queda claro tanto en el texto del Convenio Modernizado como en el resumen anterior, los Estados-partes en el Convenio Modernizado ya no podrán excluir cualquier tipo de tratamiento de sus obligaciones, como la ***seguridad y la defensa nacionales***, que son asuntos que están fuera del alcance de los instrumentos de protección de datos de la UE.[224]

Ya sea en otros aspectos, el Convenio Modernizado, o para ser más precisos, las leyes nacionales de los Estados Partes en el Convenio Modernizado que implementan ese Convenio, siempre estarán totalmente en línea con el RGPD, o para ser más precisos, con el RGPD como será interpretado y aplicado en el futuro

[224] Véase Sección 1.3.1, más arriba, bajo el título "*Naturaleza y limitaciones de las directivas de la CE*", en lo que respecta a esta limitación en relación con las directivas de protección de datos de 1995 y 2002 de la CE, y la Parte Dos, Sección 2.1, a continuación, en relación con el RGPD. En relación con el tratamiento para fines de aplicación de la ley (etc.), y el tratamiento por parte de las instituciones de la UE de los estados mismos, la UE, por supuesto, tiene reglas vigentes que se ajustan esencialmente a las normas RGPD (y, por lo tanto, a la Convención Modernizada) (o en relación con a las instituciones de la UE, lo harán una vez que se hayan ajustado al RGPD).

por el nuevo Consejo Europeo de Protección de Datos de la UE, las agencias de protección de datos de los Estados miembros de la UE, la Comisión Europea y el TJUE, es un asunto que está por ver.

Por ejemplo, las nuevas reglas sobre los flujos de datos transfronterizos en el Convenio Modernizado permiten transferencias a terceros países que brindan un nivel de protección "***apropiado***" (Art. 14), que a primera vista puede parecer similar al requisito de un "***adecuado***" nivel de protección en el RGPD (como en la Directiva de protección de datos de 1995), pero queda por ver si el nuevo Comité del Convenio nuevo siga el CJEU al considerar que este término "apropiado" debe interpretarse en el sentido de que el tercer país en cuestión debe proporcionar protección "***esencialmente equivalente***" (como el TJUE dictaminó al interpretar el término "adecuado").[225]

En otros aspectos, por ejemplo, en relación con el **consentimiento de los niños**, el Convenio Modernizado no es tan detallado o específico como el RGPD.

Pero aparte de estos asuntos, es claro que, entre ellos, el Consejo de Europa y la Unión Europea están liderando el camino para establecer los "estándares de oro" globales para la protección de datos, tanto aplicables dentro de los estados como relacionados con los flujos de datos transnacionales.

Por último, cabe señalar que el Convenio Modernizado (a diferencia de su antecesora) está abierto a la adhesión de organizaciones internacionales, por lo que la UE también puede suscribirla formalmente.

- o – O – o -

.

[225] CJEU, sentencia Schrems (nota 73, véase más arriba), para. 73 Sentencia del Tribunal de Justicia de las Comunidades Europeas en el asunto C-362/14, de 6 de diciembre de 2015.

PARTE 2

El Reglamento General de Protección de Datos.

2.1 Introducción

Como ya se señaló en el punto 1.4.1, se adoptó el Reglamento general de protección de datos (RGPD o "el Reglamento"), en parte porque la Directiva de protección de datos de 1995 no había dado lugar a un nivel suficiente de armonización de las leyes en los Estados miembros; en parte en respuesta a la expansión masiva en el tratamiento de datos personales desde la introducción de la Directiva de protección de datos de 1995; y en parte en respuesta a la jurisprudencia del TJUE. Queda por verse si será suficiente para abordar completamente el desarrollo de tecnologías cada vez más intrusivas, como Big Data, el Internet de las cosas, la toma de decisiones algorítmicas y el uso de inteligencia artificial.

El Reglamento se basa en la Directiva de protección de datos de 1995, pero se amplía significativamente y, al hacerlo, refuerza considerablemente el principal régimen de protección de datos de la UE. Aporta una mayor armonización, derechos más sólidos para los interesados, una cooperación más estrecha entre las autoridades de protección de datos, mayores poderes de ejecución y más.

El Anexo 1 a este Manual proporciona un Índice de los capítulos, secciones y artículos del RGPD, para una fácil referencia. El anexo 2 contiene el texto completo del Reglamento publicado en el Diario Oficial de la UE, incluidos los considerandos.

La Sección 3.2 explica el estado y el enfoque del RGPD, y analiza con cierto detalle las implicaciones del hecho de que contiene muchas cláusulas que permiten una mayor regulación a nivel nacional (por lo tanto, socavan el objetivo de una armonización más completa).
La Sección 3.3 proporciona un resumen capítulo por capítulo, sección por sección y artículo por artículo del RGPD. A su debido tiempo, se proporcionará un Breve Comentario sobre esas disposiciones, que se centrará en las disposiciones del Reglamento que son nuevas o se amplían significativamente o aclaran o regulan aún más las cuestiones que no estaban reguladas, o que no estaban reguladas con tanto detalle, en la Directiva de protección de datos de 1995.
Luego pasamos a los dos temas centrales para los DPD: el nuevo principio de "responsabilidad" (el deber de demostrar el cumplimiento) (sección 3.4) y las reglas sobre nombramiento, requisitos, condiciones y tareas (etc.) del DPD (sección 3.5), y explicar el enlace entre esos dos.

2.2 Estado y enfoque del RGPD: aplicabilidad directa con "clausulas de especificación".

Un reglamento…

El RGPD es un **reglamento**, es decir: una ley de la UE que es ***directamente aplicable*** en los ordenamientos jurídicos de los Estados miembros de la UE (y los estados del EEE que no pertenecen a la UE), sin tener que ser "transpuesta" a la legislación nacional, como es el caso de directivas como la Directiva de Protección de Datos de 1995.

El legislador de la UE eligió esta ruta precisamente porque la implementación de la directiva de 1995 había sido desigual: se implementó de manera diferente en diferentes Estados miembros, lo que llevó a una falta de armonización.[226]

Además, se implantó deficientemente en al menos algunos de ellos, como el Reino Unido.[227]

---

[226] Esta fue la conclusión a la que llegó en un estudio encargado por la UE por Douwe Korff para la Universidad de Essex, Informe sobre un estudio de la UE sobre la implementación de la directiva de protección de datos [1995], 2002, disponible en: http://papers.ssrn.com/sol3/papers.Cons.m?abstract_id=1287667 –
pero a la UE le llevó otros 10 años abordar esto al proponer un reglamento.

[227] Según la Comisión de la UE, en 2011, casi un tercio de los 34 artículos de la Directiva en ese momento no habían sido implementados adecuadamente por el Reino Unido, Véase:
http://amberhawk.typepad.com/amberhawk/2011/02/european-commission-explains-why-uks-data- protection-act-is-deficient.html

En teoría, un reglamento, que es directamente aplicable, debería llevar a una **armonización plena** de la ley en el área que cubre. En el caso del RGPD, esto se ve reforzado por acuerdos mucho más fuertes para el **intercambio de información y la cooperación** entre los reguladores (las autoridades nacionales de supervisión o protección de datos, APD) y un **mecanismo especial de "coherencia",** como se explica a continuación, bajo ese encabezado.

Sin embargo, como se muestra en el siguiente punto, al mismo tiempo el RGPD todavía deja muchos temas para ser regulados aún más en las leyes nacionales de los Estados miembros de la UE, de acuerdo con su sistema jurídico o institucional interno. Esto podría, en algunas áreas, socavar el objetivo de una armonización total, pero como veremos en los encabezados "Requisitos de clausulas de espedificación" y *'Cooperación y coherencia'*, también existen límites a la libertad de los Estados miembros a este respecto y significa nuevos medios de supervisión a nivel de la UE, también del ejercicio de estas "flexibilidades" (al menos en teoría).

… pero con "clausulas de especificación"[228]

Aunque el Reglamento pretende lograr una mayor armonización, todavía contiene numerosas disposiciones que se refieren a la ley en los Estados miembros (las denominadas disposiciones "flexibles"), en particular en relación con el sector público, pero también en relación con los derechos impuestos por la legislación nacional en empresas sujetas a la jurisdicción del Estado Miembro correspondiente (por ejemplo, en virtud de la legislación laboral o las normas de aplicación de la ley) y a la composición de la APD.

Tipos de disposiciones "*clausulas de especificación*"

La agencia italiana de protección de datos, el *Garante della Privacy*, ha identificado cuatro tipos de cláusulas diferentes (aunque un tanto superpuestas) que dejan margen para una mayor regulación por parte de la legislación de los Estados miembros:[229]

- **Otras especificaciones**

  Estas son disposiciones según las cuales los Estados miembros pueden mantener o introducir "disposiciones más específicas para adaptar la aplicación" de la disposición pertinente en el Reglamento (se utilizan varias frases a este efecto).

  Ejemplos

  Los Estados miembros pueden especificar qué operaciones de tratamiento requieren autorización previa, o regular el uso de ***números de identidad nacionales*** o el ***tratamiento de datos personales de los empleados***.

  Los Estados miembros pueden "mantener o introducir condiciones adicionales, incluidas limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud", más allá de las condiciones y limitaciones impuestas por el propio RGPD en el Artículo 9(1)-(3) (el artículo que trata de "categorías especiales de datos personales", generalmente denominado "datos confidenciales") (Art. 9(4)). Por lo tanto, pueden, por ejemplo, estipular que siempre se requiere un consentimiento previo para el tratamiento de datos genéticos.

- **Opciones y elecciones**

A pesar de que la Comisión amenazó con tomar medidas de cumplimiento, en realidad no persiguió esto a pesar de que las deficiencias nunca fueron remediadas de manera adecuada o total.

[228] Véase la subsección "Relación entre la Directiva sobre intimidad en las comunicaciones electrónicas y el Reglamento sobre el producto interior bruto", más arriba.

[229] Antonio Caselli, empleado de Garante ,presentación a la primera sesión de formación "T4DATA", junio de 2018, sobre "RGPD y las normas nacionales". El contenido de esta presentación está escrito y ampliado con cierto detalle en el Anexo 4 del manual (en el Volumen Dos), donde también se proporcionan más ejemplos.

En algunos aspectos, el RGPD permite a los Estados miembros, a través de su legislación nacional, **elegir** entre ciertas opciones específicamente establecidas en el Reglamento, o extender una obligación o prohibición que bajo el RGPD se aplica solo en ciertos casos, a otros casos.

> **Por ejemplo**, los Estados miembros pueden permitir que los **niños** mayores de 13, 14 o 15 años ***den su consentimiento a ciertos servicios de información***, en lugar de hacerlo solo a partir de los 16 años establecidos en el RGPD; o puede ***requerir el nombramiento de un DPD*** donde el RGPD no lo haga.

- **Restricciones y derogaciones**

Sujeto a ciertas *condiciones* bastante amplias (discutidas a continuación, bajo los encabezados "Requisitos de *"clausulas de especificación"* y 'Problemas planteados por *"clausulas de especificación"*), el Artículo 23 del RGPD permite **restricciones radicales** en prácticamente todos los derechos de los titulares de datos en relación **a objetivos importantes de interés público ampliamente definidos: seguridad nacional, defensa, seguridad pública, aplicación de la ley e independencia judicial**- pero también ***protegiendo los intereses económicos o financieros del estado***, la aplicación de la ***ética profesional***, cualquier tipo de "***supervisión, inspección o función reguladora relacionada, incluso ocasionalmente, con el ejercicio de la autoridad oficial***" en cualquiera de los principales intereses protegidos, "***la protección del interesado o los derechos y libertades de los demás***" y **la ejecución de demandas civiles.**

Los artículos 85, 86 y 89 del RGPD contienen disposiciones que, por un lado, permiten (y en algunos aspectos, exigen) **excepciones** a ciertas reglas del RGPD para proteger la **libertad de expresión**, permiten la libertad de información (acceso a los documentos). y la información en poder de las autoridades públicas) y **archivar** y facilitar la **investigación** (beneficiosa para el público), mientras que, por otro lado, impone ciertas **condiciones** a esas excepciones (como también se discute en los encabezados "Requisitos de *"clausulas de especificación"* y 'Problemas planteados por *"clausulas de especificación"*, véase más abajo).

Nota: Algunas de estas reglas especiales sirven para proteger los intereses de "otros", mientras que otras pueden considerarse de interés general o público, y otras, como la libertad de información, pueden servir a ambas. Estas son cuestiones en las que hasta ahora no se han armonizado las normas, aunque en algunos Estados miembros de la UE la supervisión de la protección de datos y la libertad de información se ha puesto en manos de las mismas autoridades. Dado que tales asuntos son cada vez más transnacionales, por ejemplo, las solicitudes transfronterizas de acceso a datos públicos; la libertad de expresión frente a la protección de datos y cuestiones de privacidad relacionadas con las publicaciones en línea; y la investigación médica transaccional: se espera que el EDPB emita más orientación sobre estas cuestiones, en particular en relación con dichas actividades transnacionales. La Comisión también podría proponer nuevas iniciativas en estos ámbitos.

- **Deberes regulatorios**

En algunos aspectos distintos a los mencionados anteriormente, en particular en relación con el establecimiento de organismos de supervisión independientes (agencias de protección de datos, APD) y el establecimiento de esquemas de certificación, el RGPD requiere que los Estados miembros adopten normas y reglamentos detallados, implementando Los requisitos relevantes para las APDs en su ordenamiento jurídico nacional. Estos son problemas técnicos en gran medida (aunque también requieren el cumplimiento de normas importantes, por ejemplo, sobre independencia y la provisión de recursos suficientes).

Requisitos de "clausulas de especificación"

En muchos aspectos, incluidos los mencionados en los encabezados "especificaciones adicionales" y "opciones y alternativas" anteriores, pero especialmente los señalados en el encabezado "restricciones y excepciones", el RGPD **exige** a los Estados miembros que adopten normas legales para abordar las cuestiones pertinentes que ***cumplen con ciertas normas democráticas/derechos legales.***

Otras disposiciones (no incluidas en esos títulos) también **implican la necesidad de una regulación**, ya que requieren que los Estados miembros adopten "***salvaguardias apropiadas***", "***salvaguardias adecuadas"*** o "***medidas adecuadas***". Dado que el propio RGPD a menudo no aclara cuáles podrían ser esas salvaguardas o medidas, los Estados miembros tendrán que aclarar esto en las leyes nacionales, que nuevamente deberán cumplir ciertos estándares democráticos / del estado de derecho.

Es importante tener en cuenta que, **en esto, a los Estados miembros no se les otorga simplemente una discreción sin restricciones** – dado que queda claro a partir de los requisitos de que ciertas medidas o garantías sean "apropiadas" o "adecuadas". En otros aspectos, en el RGPD se especifican expresamente ciertas normas y condiciones de ley de aplicación general, pero, de hecho, se aplican normas y condiciones similares a todas las regulaciones pertinentes

Por lo tanto, el RGPD estipula expresamente que las excepciones radicales en principio permitidas en virtud del Artículo 23 (resumidas anteriormente bajo el encabezado "Restricciones y derogaciones") [137] deben estar establecidas en **la ley** (una "***medida legislativa***") que debe "***respetar*** [] ***la esencia de los derechos*** y ***libertades fundamentales*** y [ser] una ***medida necesaria y proporcionada*** en una sociedad democrática para "salvaguardar" el interés relevante. Estos requisitos son reflejos directos de los requisitos que debe cumplir cualquier limitación de cualquiera de los principales derechos protegidos por el Convenio Europeo de Derechos Humanos(CEDH) y la Carta de los Derechos Fundamentales de la UE(CDF). Para citar este último:

> Cualquier limitación al ejercicio de los derechos y libertades reconocidos por esta Carta debe estar prevista por la ley y respetar la esencia de esos derechos y libertades. Sujeto al principio de proporcionalidad, solo se pueden establecer limitaciones si son necesarias y cumplen genuinamente los objetivos de interés general reconocidos por la Unión o la necesidad de proteger los derechos y libertades de los demás.
> (Art.52(1),énfasis añadido)

Dado que cualquier ley de un Estado Miembro que limite o restrinja los derechos de los titulares de datos en virtud de cualquiera de las "clausulas de especificación"del RGPD debe considerarse como una limitación inherente del derecho a la protección de datos garantizada en el CFR (Artículo 8), todos deben cumplir con los estándares anteriores.

Más específicamente, bajo la ECHR (Convención Europea de Derechos Humanos) y el CFR, y por lo tanto también bajo el RGPD, la ley relevante debe cumplir con ciertos requisitos cruciales de "calidad": las normas de la ley deben ser "compatibles con el estado de derecho" (lo que significa en particular que pueden no ser discriminatorios o arbitrarios, y deben ser imputables y estar sujetos a recursos efectivos) y, más en particular, accesibles (es decir, publicados) y suficientemente claros y precisos para ser "previsibles" en su (y su) aplicación.[230]

La referencia al "respeto [por] la **esencia**" de los derechos y libertades en cuestión debe interpretarse como **una prohibición de cualquier norma legal tan fuerte en un derecho que lo haga inútil.**
Por ejemplo, el Tribunal de Justicia de la UE ha sostenido que:[231]

> debe considerarse que la legislación que permite a las autoridades públicas tener acceso de forma generalizada al contenido de las comunicaciones electrónicas compromete la esencia del derecho fundamental al respeto de la vida privada, como lo garantiza el Artículo 7 de la Carta...

Las excepciones de los Estados miembros en virtud del Artículo 23 RGPD en particular, incluidas las excepciones a las normas de protección de datos para salvaguardar la seguridad y la defensa nacionales,

---

[230] Véase: Harris, O'Boyle & Warbrick, *Law of the European Convention on Human Rights*, 2ª ed., 2009, Capítulo 8, Sección 3, Limitaciones. Para un resumen sencillo de los requisitos relevantes de la ECHR, véase: Douwe Korff, *The standard approach under Articles 8 – 11 ECHR and Article 2 ECHR* (material didáctico), disponible en:
https://www.pravo.unizg.hr/_download/repository/KORFF_-_STANDARD_APPROACH_ARTS_8 11_ART2.pdf
Véase en particular, el texto de las preguntas 3 (Ley) y 5 (Necesario y proporcionado) en ese material

[231] CJEU, Sentencia *Schrems* (nota 73), párrafo 94

por lo tanto, nunca pueden equivaler a excepciones excesivas, nunca justificadas ni nunca aceptables, de las normas principales.

Más específicamente, cualquier excepción en virtud del Artículo 23, y de hecho cualquier otra desviación de cualquiera de las reglas normales en el RGPD bajo cualquiera de las "clausulas de especificación", debe cumplir con la prueba de "necesaria y proporcionada en una sociedad democrática". Esto significa que cualquier desviación de las reglas normales o la restricción de cualquier derecho de titulares de datos no absolutos, basado en una "clausula de especificación"debe realmente estar en la búsqueda del ***"objetivo legítimo" / "objetivo importante de interés público"*** reclamado, responda a una "necesidad social apremiante", y ser "***razonablemente proporcional"*** a esa necesidad. Al juzgar qué se necesita exactamente en esos términos, a los Estados se les puede otorgar un cierto ***"margen de apreciación"***[232], pero este margen está limitado por el requisito de que la medida (la derogación o limitación) debe ser necesaria "***en una sociedad democrática***".

En términos generales, si existe una **orientación clara** sobre un tema en particular, como lo ha proporcionado la Directiva de protección de datos de 1995 por parte del Grupo de trabajo Artículo 29 y la SEPD (Autoridad Supervisora Independiente), y ahora está siendo proporcionada por el European Data Protection Board (que incluye el SEPD) - y/o si existe una **notable convergencia** de puntos de vista sobre el asunto entre los Estados miembros (o las APDs de los Estados miembros), es probable que cualquier divergencia de dicha orientación o consenso por parte de un Estado Miembro indique que las medidas divergentes (excepciones) o las limitaciones que van más allá de lo que se considera necesario o proporcional en otros Estados miembros) no son "necesarias" o "proporcionadas" en una sociedad democrática.

Sin embargo, como se señala en el siguiente encabezado, estos asuntos no pueden resolverse por medio de los "mecanismos de cooperación y coherencia" (discutidos por separado, más adelante).

Problemas planteados por las *"clausulas de especificación"*

Nos hemos centrado en las "clausulas de especificación"con cierto detalle porque plantean problemas en la aplicación efectiva del RGPD. Se presentan de dos formas.

En primer lugar, las "clausulas de especificación"conducirán por su propia naturaleza a normas **diferentes (o más o menos detalladas), que reflejen las singularidades nacionales, sobre cuestiones idénticas en los diferentes Estados miembros**. Esto no plantea un problema tan grande en relación con el tratamiento que se lleva a cabo en su totalidad dentro de un Estado Miembro y que se relaciona solo con los interesados en ese Estado Miembro. Sin embargo, como se señaló anteriormente, en el siglo XXI, cada vez más actividades estatales tienen implicaciones internacionales e involucran operaciones transfronterizas de tratamiento de datos personales, también en el sector público, y no solo en relación con la aplicación de la ley o las fronteras. Este es especialmente el caso dentro de la UE, debido a las “cuatro libertades” que son fundamentales para el proyecto europeo: la libre circulación de bienes, servicios, personas y finanzas.

Cuando se ofrecen y compran bienes o servicios a través de la frontera, dentro de la UE como fuera de ellos, los datos personales siguen (y son esenciales para) las transacciones. Cuando las personas se mudan, también lo hacen sus datos: sus datos sobre impuestos, prestaciones de bienestar y pensiones, sus datos médicos, matrimonios, nacimientos, divorcios, defunciones y registros de residencia. Cuando se realizan los pagos (entre individuos, o entre individuos y entidades privadas, o entre individuos y agencias estatales, ya sea la oficina de impuestos, residencia o pensión), esto implica flujos de sus datos financieros y de otro tipo. Este es el caso *a fortiori* cuando el tratamiento, o parte del tratamiento, tiene lugar en línea.

---

[232] La doctrina del "margen de apreciación", que está fuertemente arraigada en la jurisprudencia del Tribunal Europeo de Derechos Humanos, está enunciada menos claramente por el Tribunal de Justicia de la UE que, en todo caso, tiende a referirse a la "discreción" o “margen de discreción” otorgado a los Estados miembros en ciertos asuntos. Pero a los efectos del presente manual, la doctrina puede considerarse como reflejada en la jurisprudencia de los tribunales de Estrasburgo y de Luxemburgo, aunque quizás en grados algo diferentes y algo dependiente del contexto. Véase: Francisco Javier Mena Parras, *From Strasbourg to Luxembourg? Transposing the margin of appreciation concept into EU law*, Brussels, 2008, disponible en: http://www.philodroit.be/IMG/pdf/fm_transposing_the_margin_of_appreciation_concept_into_eu_law_-_2015-7.pdf

Cuando, en tales circunstancias, existen diferentes normas en los diferentes Estados miembros interesados en el tratamiento de los datos en cuestión, esto da lugar a posibles **aspectos legales** (y potencialmente graves) que tendrán que resolverse caso por caso (lo que a menudo no será fácil). Los siguientes ejemplos pueden ilustrar esto con referencia a algunas de las excepciones y limitaciones específicas que se pueden introducir bajo las "clausulas de especificación"mencionadas anteriormente:

Ejemplos:

- Si un Estado Miembro impone restricciones sobre el uso del número de identidad nacional que no están impuestas en otro Estado Miembro, ¿esas restricciones aún deben ser respetadas por un receptor en el último Estado Miembro (incluido un receptor del sector público) si el número se transfiere a ese destinatario?

- Si un Estado Miembro impone "condiciones adicionales" o "limitaciones" adicionales en el tratamiento de todos o ciertos tipos de datos confidenciales (por ejemplo, en el uso de datos biométricos o genéticos) que no se imponen en otro Estado Miembro, ¿deben esas condiciones o limitaciones respetarse por cualquier receptor en los últimos Estados miembros (incluido un destinatario del sector público) si los datos se transfieren a ese destinatario?

- Si un Estado Miembro establece la edad de consentimiento para el uso de servicios de información para niños a la edad de, digamos, 14 años, y otro Estado Miembro la deja a la edad de 16 años propuesta por el RGPD, ¿puede proporcionar un proveedor de servicios de información en el Estado Miembro anterior su servicio a un niño de 14 años en el último Estado Miembro, sobre la base del consentimiento del niño de 14 años? ¿Debería el proveedor distinguir en función de la dirección IP del niño (aunque se puede "falsificar" fácilmente mediante una VPN (Red Virtual Privada), incluso en los de 14 años)?

- Si un Estado Miembro requiere la obtención de una autorización previa de la APD para su tratamiento en relación con la protección social y la salud pública, pero otro Estado Miembro no lo hace, puede una autoridad pública en el último Estado Miembro tratar datos personales en relación con los titulares de datos en el antiguo Estado Miembro para tales fines, sin dicha autorización previa, como podría ocurrir fácilmente en relación con los hijos de migrantes que dejan a su cónyuge e hijos en su país de origen mientras trabajan en otro Estado Miembro, pero con la prestación por hijos, etc. que se les paga a los cónyuges en el país de origen ? (NB: En el contexto de proporcionar dicha autorización previa, la APD pertinente presumiblemente impondrá o exigirá la imposición de ciertas salvaguardas y restricciones. ¿Debe la agencia estatal en el otro Estado Miembro cumplir con esas también? ¿La agencia incluso estaría al tanto de ellas?)

Estas cuestiones se ven seriamente agravadas por la **ausencia en el RGPD de una disposición de "ley aplicable"** similar a la contenida en la Directiva de protección de datos de 1995, aun cuando dicha disposición, el artículo 4, planteara cuestiones en relación con la traducción en diferentes lenguas y en términos de eficacia.[233]Presumiblemente, una disposición de este tipo quedó fuera del RGPD porque se asumió que, como regulación, se aplicaría de manera totalmente armonizada, pero como se muestra arriba, en las (muchas) áreas cubiertas por "clausulas de especificación" (a ser tratado a nivel nacional en leyes específicas) este no será el caso, evidentemente.

La segunda cuestión se relaciona con el **cumplimiento de los requisitos del estado de derecho** establecidos anteriormente, bajo el subtítulo anterior. Es probable que surjan preguntas sobre si ciertas leyes en ciertos Estados Miembros que restringen ciertos derechos o relajan ciertas reglas cumplen con esas pruebas, es decir, si son lo suficientemente accesibles, precisos y previsibles en su aplicación, necesarias o proporcionales a los pertinentes (legítimas / importantes) fines.

Esos problemas a menudo no pueden resolverse, ni siquiera abordarse, bajo el "Mecanismo de Estabilidad y Coherencia" que se discute más adelante, ya que dichos mecanismos se limitan a la cooperación en

[233] Véase Douwe Korff, The question of "applicable law", en: Guía de Cumplimiento 3 - Informe provisional, Privacy Laws & Business, noviembre de 1999.

relación con las medidas adoptadas o propuestas para ser tomadas por las autoridades de protección de datos: no puede utilizarse para remediar deficiencias en las leyes de los Estados miembros. Esto puede crear un problema grave, especialmente en relación con la transferencia de datos personales de una agencia estatal en un Estado miembro de la UE a una agencia estatal en otros Estados miembros, si en este último estado los datos se tratarán según las leyes que posiblemente no cumplan los requisitos de un estado de derecho. Sin embargo, la experiencia en otras áreas (como las reglas de Justicia y Asuntos de Interior, no discutidas en esta primera edición del manual) muestra que, cuando sea necesario, se pueden tomar medidas para abordar tales problemas, especialmente sobre la base de sugerencias propuestas por la Comisión o el EDPB.

Implicaciones para los DPD

Por todo lo anterior, debe quedar claro que los DPD deben conocer y estudiar, **no solo las reglas del RGPD, sino también cualquier regla nacional relevante que se base en las "clausulas de especificación"del RG**PD, y hasta cierto punto, de hecho, las leyes relevantes y normas en otros Estados miembros y en terceros países, si su organización revela datos personales a otros estados.

Estos pueden tomar muchas formas. En algunos casos, es posible que los Estados miembros simplemente hayan retenido las reglas que ya existían antes de la entrada en vigor del RGPD, incluidas excepciones especiales para proteger intereses públicos importantes o para facilitar la investigación, aunque **es posible que no siempre cumplan con los requisitos del estado de derecho establecidos en las "clausulas de especificación" o "apropiadas" o "adecuadas" en los términos del RGPD** (como se discutió anteriormente). En otros casos, su Estado miembro puede haber adoptado leyes o normas legales específicas para "regular aún más" los asuntos dejados al Estado miembro en virtud del RGPD, o para aclarar qué opciones se utilizan, etc. En otros casos, es posible que el Estado miembro todavía no haya aclarado la aplicación nacional de las cláusulas pertinentes.

Por supuesto, los DPDs no pueden rectificar por ellos mismos cualquier diferencia o problema a este respecto. No obstante, dentro de sus propias redes de los DPDs y en sus interacciones con sus agencias nacionales de protección de datos[234], ellos **pueden señalar tales problemas y proponer un curso de acción adecuado**. También deberían, de nuevo, preferiblemente, junto con otros DPD que trabajan en organizaciones similares, alertar a los niveles más altos de sus propias organizaciones (en el sector público, por ejemplo, los ministros de gobierno relevantes) de tales deficiencias percibidas. En tales situaciones, los DPD deben desarrollar enfoques estratégicamente eficientes.

2.3 Resumen del RGPD

A continuación, se presenta una descripción general de RGPD capítulo por capítulo, sección por sección y artículo por artículo.*

*Se espera que en una segunda edición más detallada de este manual se puedan elaborar comentarios breves de cada artículo de las disposiciones del RGPD, que se centrarán en la aplicación concreta y práctica de las disposiciones pertinentes. Entretanto, se recomienda a los delegados consultar algunos de los comentarios académicos principales que se han publicado en diferentes idiomas, así como las orientaciones publicadas por las APD nacionales, el EDPB y los tribunales europeos y nacionales.

REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS DE 2018

Capítulo I:

Disposiciones generales (Artículos 1 – 4):

- Objeto y objetivos del Reglamento;

[234] Cons. La "extranet" de los DPD franceses, que podría ser de utilidad en tales contextos. Véase nota 456 posterior.

- Ámbito de aplicación material; - Ámbito territorial - Definiciones
<u>Capítulo II</u>: **Principios (Artículos 5 – 11):** - Principios relativos al tratamiento de datos personales; - Licitud del tratamiento [bases legales]; - Condiciones para el consentimiento; - Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información - Tratamiento de categorías especiales de datos personales [datos sensibles]; - Tratamiento de datos personales relativos a condenas e infracciones penales; - Tratamiento que no requiere identificación.
<u>Capítulo III</u>: **Derechos del interesado**
Sección 1 (Artículo 12): **Transparencia y modalidades:** - Transparencia de la información, comunicación y modalidades del ejercicio de los derechos del interesado
Sección 2 (Artículos 13 – 15): **Información y acceso a los datos personales:** - Información que deberá facilitarse cuando los datos personales se obtengan del interesado; - Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado; - Derecho de acceso del interesado.
Sección 3 (Artículos 16 – 20): **Rectificación y supresión:** - Derecho de rectificación; - Derecho de supresión (“el derecho al olvido”); - Derecho a la limitación del tratamiento [“bloqueo”]; - Obligación de notificación relative a la rectificación o supresión de datos personales o la limitación del tratamiento; - Derecho a la portabilidad de datos.
Sección 4 (Artículos 21 – 22):

Derecho de oposición y decisiones individuales automatizadas:

- Derecho de oposición;
- Decisiones individuales automatizadas, incluida la elaboración de perfiles.

Sección 5 (Artículo 23):

Limitaciones

CAPÍTULO IV:

Responsable del tratamiento y encargado del tratamiento

Sección 1 (Artículos 24 – 31):

Obligaciones generales:

- Responsabilidad del responsable del tratamiento;
- Protección de datos desde el diseño y por defecto;
- Corresponsables del tratamiento;
- Representantes de responsables o encargados del tratamiento no establecidos en la Unión;
- Encargado del tratamiento;
- Tratamiento bajo la autoridad del responsable o del encargado del tratamiento;
- Registro de las actividades de tratamiento;
- Cooperación con la autoridad de control.

Sección 2 (Artículos 32 – 34):

Seguridad de los datos personales:

- Seguridad del tratamiento;
- Notificación de una violación de la seguridad de los datos personales a la autoridad de control;
- Comunicación de una violación de la seguridad de los datos personales al interesado.

Sección 3 (Artículos 35 – 36):

Evaluación de impacto relativa a la protección de datos y consulta previa:

- Evaluación de impacto relativa a la protección de datos;
- Consulta previa.

Sección 4 (Artículos 37 – 39):

Delegado de protección de datos:

- Designación del delegado de protección de datos;
- Posición del delegado de protección de datos;
- Funciones del delegado de protección de datos.

Sección 5 (Artículos 40 – 43):

Códigos de conducta y certificación:

- Códigos de conducta;
- Supervisión de códigos de conducta aprobados;
- Certificación;
- Organismo de certificación.

CAPÍTULO V (Artículos 44 – 50):

Transferencias de datos personales a terceros países u organizaciones internacionales:

- Principio general de las transferencias;
- Transferencias basadas en una decisión de adecuación;
- Transferencias mediante garantías adecuadas;
- Normas corporativas vinculantes;
- Transferencias o comunicaciones no autorizadas por el Derecho de la Unión;
- Excepciones para situaciones específicas;
- Cooperación internacional en el ámbito de la protección de datos personales.

CAPÍTULO VI:

Autoridades de control independientes:

Sección 1 (Artículos 51 – 54):

Independencia:

- Autoridad de control;
- Independencia;
- Condiciones generales aplicables a los miembros de la autoridad de control;
- Normas relativas al establecimiento de la autoridad de control.

Sección 2 (Artículos 55 – 59):

Competencia, funciones y poderes:

- Competencia;
- Competencia de la autoridad de control principal;
- Funciones;
- Poderes;
- Informe de actividad.

CAPÍTULO VII:

Cooperación y coherencia

Sección 1 (Artículos 60 – 62):

Cooperación:

- Cooperación entre la autoridad de control principal y las demás autoridades de control interesadas;
- Asistencia mutua;
- Operaciones conjuntas de las autoridades de control.

Sección 2 (Artículos 63 – 67):

Coherencia:

- Mecanismo de coherencia;
- Dictamen del Comité;
- Resolución de conflictos por el Comité;
- Procedimiento de urgencia;
- Intercambio de información.

Sección 3 (Artículos 68 – 76):

Comité europeo de protección de datos:

- Comité Europeo de Protección de Datos;
- Independencia;
- Funciones del Comité;
- Informes;
- Procedimiento;
- Presidencia;
- Funciones del presidente;
- Secretaría;
- Confidencialidad.

CAPÍTULO VIII (Artículos 77 – 84):

Recursos, responsabilidad y sanciones:

- Derecho a presentar una reclamación ante una autoridad de control;
- Derecho a la tutela judicial efectiva contra una autoridad de control;
- Derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento;
- Representación de los interesados;
- Suspensión de los procedimientos;
- Derecho a indemnización y responsabilidad;
- Condiciones generales para la imposición de multas administrativas;
- Sanciones.

CAPÍTULO IX (Artículos 85 – 91):

Disposiciones relativas a situaciones específicas de tratamiento:

- Tratamiento y libertad de expresión y de información;
- Tratamiento y acceso del público a documentos oficiales;
- Tratamiento del número nacional de identificación;
- Tratamiento en el ámbito laboral;
- Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos;
- Obligaciones de secreto;
- Normas vigentes sobre protección de datos de las iglesias y asociaciones religiosas.

CAPÍTULO X (Artículos 92 – 93):

Actos delegados y actos de ejecución:

- Ejercicio de la delegación;
- Procedimiento de comité.

CAPÍTULO XI (Artículos 94 – 99):

Disposiciones finales:

- Derogación de la Directiva 95/46/CE;
- Relación con la Directiva 2002/58/CE;
- Relación con acuerdos celebrados anteriormente;
- Informes de la Comisión;
- Revisión de otros actos jurídicos de la Unión en materia de protección de datos;
- Entrada en vigor y aplicación.

2.4 El principio de rendición de cuentas[235]

2.4.1 La nueva obligación de poder demostrar el cumplimiento

Si bien esto puede parecer nada nuevo (y puede decirse que está inspirado en el enfoque legal estadounidense, que se reflejó en las directrices de la OCDE de 1980), es una de las características principales del Reglamento General de Protección de Datos (RGPD nuevo de la UE, quizás incluso la principal, que pone un gran énfasis en el hecho de que:

> El controlador será responsable de, y [deberá] ser capaz de demostrar el cumplimiento de, [los principios relacionados con el tratamiento de datos personales] ("responsabilidad") "(Art. 5(2)).

Como dice la agencia italiana de protección de datos, el *Garante della Privacy*: [236]

> Hacer que una entidad sea responsable significa asignar acciones y decisiones a esa entidad y esperar que esa entidad sea responsable de esas acciones y decisiones. Por lo tanto, la responsabilidad es el estado de ser responsable de las acciones y decisiones que se han asignado.

La novedad no radica en el organismo a cargo del tratamiento responsable de su cumplimiento - por supuesto, ese ya era el caso en virtud de la Directiva de protección de datos de 1995 (aunque esa directiva no utiliza el término "responsabilidad"). Más bien, la novedad radica en el énfasis en que el controlador (y en algunos casos el procesador) deba "demostrar" este cumplimiento: el Reglamento utiliza el término no menos de 33 veces.

Esto contrasta con la Directiva de 1995, que en ninguna parte requiere explícitamente que un controlador o procesador demuestre el cumplimiento de cualquier cosa (salvo que una APD o un tribunal lo requiera). Más específicamente, los diversos esquemas de "notificación" o "registro" establecidos en virtud de la Directiva en al menos algunos países hicieron poco para demostrar dicho cumplimiento[237], mientras que en otros solo tuvieron éxito al ser muy detallados y presentados de tal manera que se estimularan. Los controladores deben aplicar todos los requisitos legales a cualquier operación de tratamiento de datos nuevos, con la agencia de protección de datos (APD) relevante alertando al controlador y sugiriendo modificaciones o dando consejos cuando sea necesario. En el contexto de las prácticas de tratamiento de datos que se expanden y evolucionan rápidamente, y en países (como los Estados miembros de la UE) en los que ya existe un conocimiento y una experiencia significativos con la aplicación de normas y principios de protección de datos, también en el contexto de la promoción de la "responsabilidad social" de las organizaciones, se solicitó un enfoque nuevo que enfatiza la responsabilidad principal y la responsabilidad de aquellos que procesan datos personales (ya sea como controlador o procesador). Eso es lo que representan el principio de responsabilidad y el deber de demostrar.

Como se analiza en la Sección 2.3, a continuación, el Reglamento exige el nombramiento de Delegados de Protección de Datos (DPD) para todos los controladores del sector público y muchos del sector privado como los principales medios institucionales para poner en práctica el principio de responsabilidad.

Como la estipulación del principio de responsabilidad en el artículo 5(2), citado anteriormente, aclara que el deber de demostrar el cumplimiento se aplica en primer lugar a los principios básicos que sustentan el Reglamento, establecidos en el art. 5(1), es decir, a la legalidad, la imparcialidad y la transparencia; especificación de propósito específico y explícito y limitación de propósito; minimización de datos (incluida la adecuación, relevancia y necesidad de los datos); exactitud (incluida la actualización); limitación al

---

[235] Esta Sección se basa, y en partes, repite o resume, el documento de Douwe Korff, Las implicaciones prácticas del nuevo Reglamento de protección de datos general de la UE para empresas de la UE y de fuera de la UE, agosto de 2016, documento presentado en CMS Cameron McKenna LLP, Londres, en febrero 2017, disponible en.
http://ssrn.com/abstract=3165515

[236] Luigi Carrozzi, presentación para la tercera sesión de formación "T4DATA", junio 2018, diapositiva "Inventario de activos y el principio de rendición de cuentas"

[237] Véase RGPD, considerando 89.

almacenamiento (retención); integridad, confidencialidad y seguridad. Por supuesto, también se aplica (en todo caso *a fortiori*) a la aplicación especialmente estricta de estos principios al tratamiento que involucra categorías especiales de datos (los llamados datos confidenciales - Art. 9) o que de otro modo puedan suponer un riesgo elevado para los derechos y libertades de las personas físicas (y que, por lo tanto, requieren una Evaluación de Impacto de Protección de Datos especial - Art. 35).

Más allá de esto, el Reglamento impone expresa o implícitamente el deber de demostrar el cumplimiento en muchos contextos más específicos, incluso en relación con:

- La obtención del consentimiento (cuando sea necesario) (ver Art. 7 (1));
- El rechazo de una solicitud de un titular de datos para acceder o rectificar datos (ver Arts. 11(2) y 12(5));
- Incumplimiento de las objeciones de los titulares de datos al tratamiento (véase el Art. 21(1));
- La provisión de "garantías suficientes" de competencia y la adopción de "medidas técnicas y organizativas apropiadas" para garantizar la seguridad del tratamiento de datos, por parte de procesadores y subprocesadores (véanse los artículos 28 y 32);
- La provisión de "salvaguardias apropiadas" para la transferencia de datos personales a terceros países sin una protección de datos adecuada (Art. 46);
- Etcétera.

Muy relacionados con este deber de demostrabilidad de cumplimiento están los deberes generales y específicos que impone el RGPD en términos de**:**

- **Crear un registro de operaciones de tratamiento de datos personales;**
- Realizar una **revisión geneal de dichas operaciones;**
- **Evaluar los riesgos** que entrañan dichas operaciones para los derechos y libertades de las personas;
- Realizar **evaluaciones exhaustivas del impacto de la protección de datos en relación con las operaciones que se considera que pueden dar lugar a un "alto riesgo";**
- Utilizar la **protección de datos por diseño y por defecto** en lo que respecta a todas las operaciones de tratamiento de datos personales;
- Requisitos de **notificación de violaciones de datos.**

En la Parte Tres se analizarán todos estos aspectos, y en particular el papel de los DPD en relación con los mismos. Por este motivo, bastará con hacer breves menciones y referencias a esa parte en este apartado.

Por lo tanto, en primer lugar, el Reglamento impone un **requisito general crucial para mantener registros detallados de todas las operaciones de tratamiento de datos personales del controlador**, estableciendo los detalles específicos de cada una de las operaciones (Art. 30); estos registros deben conservarse en **un registro de operaciones de tratamiento de datos personales** y deben demostrar que, y cómo, se cumplen tanto los deberes generales anteriores como los más específicos (*cf.* considerando 82). Véase el análisis de la Función 1 en la Parte Tres de este manual.

En segundo lugar, el Reglamento requiere a los responsables que, con la ayuda de sus DPD, **revisen sus operaciones** y, cuando sea necesario, las modifiquen para que cumplan el Reglamento, y registrar la revisión y cualquier medida correctiva adoptada en el mencionado registro. Véase análisis de la Función 2 en la Parte Tres de este manual.

En tercer lugar, el Reglamento impone a los controladores el deber general de "tener en cuenta" los riesgos planteados por la operación de tratamiento propuesta por el controlador, junto con el deber de implementar "medidas técnicas y organizativas adecuadas" para contrarrestar esos riesgos y un deber. "Para demostrar que el tratamiento se realiza de conformidad con este Reglamento", es decir, el Reglamento requiere que esos riesgos se hayan evaluado y que las medidas tomadas a la luz de esa evaluación eran apropiadas para esos riesgos (Art. 24 (1)); *cf.* también Art. 32). Estas cuestiones también deberán registrarse adecuadamente. Véase el análisis de la Función 3 en la Parte Tres de este manual.

En cuarto lugar, si el requisito general de una evaluación de riesgos (señalado anteriormente) muestra que existe

la probabilidad de que exista un alto riesgo para los derechos y libertades de las personas físicas, el controlador debe, antes del tratamiento, realizar **una evaluación del impacto de la protección de datos** (EIPD) de operaciones de tratamiento de datos personales previstas en la protección, y documentar esta evaluación. El **documento EIPD** debe contener: una descripción sistemática de las operaciones de tratamiento previstas y los propósitos del tratamiento; una evaluación de la necesidad y proporcionalidad de las operaciones de tratamiento y de los datos en relación con esos fines; una evaluación de los riesgos para los derechos y libertades de los sujetos de datos planteados por el tratamiento; y una descripción de las medidas previstas para abordar esos riesgos, que incluyen *"salvaguardas, medidas de seguridad y un mecanismo para garantizar la protección de datos personales y para **demostrar** el cumplimiento de este Reglamento teniendo en cuenta los derechos e intereses legítimos de los interesados y otras personas interesadas* "(Art. 35). Véase el análisis de la Función 4 en la Parte Tres de este manual.

En quinto lugar, el Reglamento impone a los controladores el deber general de utilizar "**Protección de Datos por diseño y por defecto**", tanto en la configuración como en la ejecución de todas las operaciones de tratamiento del controlador (Art. 25), y el controlador debe poder demostrar que se ha realizado. A este respecto, el Reglamento menciona que las certificaciones (sellos de protección de datos) se pueden utilizar como un "elemento" para demostrar el cumplimiento (Art. 25(3), que se analiza más adelante). Véase el análisis de la Función 9 en la Parte Tres de este manual.

En sexto lugar, los controladores deben **documentar todos los detalles** de todas las infracciones de datos (violaciones de seguridad de datos) y las medidas correctivas tomadas, y notificar a la autoridad de supervisión pertinente (competente) de esos detalles dentro de las 72 horas (Art. 33). Los titulares de datos afectados por la violación también deben ser informados, pero solo si "la violación de la seguridad de los datos puede resultar en un alto riesgo para [sus] derechos y libertades", y con menos detalles específicos (Art. 34). Véase el análisis de la Función 6 en la Parte Tres de este manual.

El Reglamento también contiene algunos deberes de grabación más específicos, entre los que se incluye la estipulación de que si dos o más controladores determinan conjuntamente los propósitos y los medios de tratamiento, son controladores conjuntos. Como tales, deben "de manera transparente determinar sus respectivas responsabilidades para el cumplimiento de las obligaciones en virtud del presente Reglamento" en forma de "**un acuerdo entre ellos**"; y esta "disposición" "deberá reflejar debidamente las funciones y relaciones respectivas de los controladores conjuntos con respecto a los interesados". En la práctica, dado que las autoridades de supervisión pueden pedir a los controladores que demuestren el cumplimiento de estos deberes, el acuerdo tendrá que ser **por escrito o en un formato electrónico similarmente fiable** (Art. 26);

Del mismo modo, las diferentes disposiciones recogidas en el Reglamento que requieren a los responsables, responsables conjuntos, encargados y subencargados que especifiquen cuáles son los acuerdos entre ellos o en relación con las transferencias de datos in **contratos o instrumentos con una vinculación legal similar** también precisan documentación.

2.4.2 Medios para demostrar el cumplimiento

El deber general de mantener **registros e inscripciones** detallados, y los deberes de mantenimiento de registros más específicos impuestos en relación con los controladores conjuntos, las violaciones de datos y las EIPDs, mencionados anteriormente, constituyen los principales medios generales para demostrar el cumplimiento, previstos en el Reglamento.

Esos registros deben reflejar una cultura y un enfoque generales que promueven la protección de datos, reflejados en **prácticas** tales como:

- elaborar y adoptar formalmente políticas internas de protección de datos (y tomar medidas asociadas, como la capacitación);
- incorporando protección de datos por diseño y protección de datos por principios predeterminados en todas las operaciones de tratamiento de datos, productos y servicios del controlador, en cada paso, desde su concepción hasta su operación real;
- minimizar el uso y la retención de datos personales, y más específicamente el uso de datos aún

identificables (mediante el uso de seudonimización o anonimización de datos previamente identificables siempre que sea posible);

- garantizando la máxima transparencia sobre las operaciones del controlador para los titulares de datos y el público en general, en formato de papel, como declaraciones de privacidad / protección de datos claras y mucho más diferenciadas en los sitios web (por ejemplo, claramente distintivo, directamente en la página de qué datos personales se recopilan, entre los campos / propósitos y datos obligatorios y opcionales, y permitiendo que los usuarios del sitio web realicen una elección legítima mucho mayor, haciendo clic en un recuadro) y estableciendo medios efectivos y eficientes para tratar las solicitudes de datos de los interesados para información general o específica; y
- garantizar que el controlador mismo pueda continuar supervisando las operaciones de manera efectiva, en particular en lo que respecta a la seguridad (mediante registros de acceso y alteración, etc.) y puede mejorar la seguridad siempre que sea necesario (por ejemplo, emitiendo "parches").

(Cons. Considerando 78)

En la Parte 3, analizaremos todos estos asuntos más a fondo y con mayor detalle, con ejemplos específicos y orientación práctica sobre cómo realizar las tareas anteriores.

Pero además, el considerando anterior (77) enumera varios **medios especiales** para demostrar el cumplimiento, es decir:

- que se actúa de acuerdo con un código de conducta aprobado;
- que se actúa de acuerdo con las certificaciones de protección de datos aprobadas;
- que se actúa de acuerdo con las directrices proporcionadas por el Consejo Europeo de Protección de Datos (EDPB); y, por supuesto,
- que se actúa de acuerdo con las indicaciones dadas por el Delegado de Protección de Datos.

A estos se pueden añadir, en particular en relación con las transferencias transfronterizas y el intercambio de datos personales:

- Reglas Corporativas Vinculantes (Binding Corporate Rules - BCRs);
- Acuerdos administrativos ("acuerdos") entre autoridades y organismos públicos; y
- Contratos de transferencia de datos estándar o aprobados individualmente.

En relación con las violaciones de datos, la notificación (y los detalles establecidos en la notificación) también puede considerarse como un medio especial para demostrar el cumplimiento de los requisitos pertinentes.
Sin embargo, cabe destacar que en relación con todos ellos, si bien pueden constituir "elementos" en un esfuerzo global para demostrar el cumplimiento, y "medios especiales" para hacerlo, no constituyen necesariamente una prueba legal del cumplimiento.

2.4.3 Valor probatorio de los diversos medios para demostrar el cumplimiento

En la mayoría de los casos, la adhesión a cualquiera de los medios de cumplimiento anteriores "es un elemento para demostrar el cumplimiento", es decir, crean una presunción de cumplimiento, pero esa presunción es refutable. Si una autoridad de protección de datos investigara un asunto más a fondo, podría encontrar que, independientemente de la adhesión formal a tales directrices, códigos, certificaciones, acuerdos, contratos o normas, en el caso específico, el Reglamento no se cumplió (aunque se consideró válido). El esfuerzo de cumplimiento con la fe, por supuesto, tendría un impacto significativo en el nivel de cualquier sanción, si es que se impusiera alguna (véase el artículo 83).

2.5 El Delegado de Protección de Datos (DPD)

2.5.1Antecedentes

El concepto de responsables de la protección de datos nombrados por los responsables del sector público y privado procede de la legislación alemana sobre protección de datos, que los ha exigido durante mucho tiempo.[238] Incluso en países que bajo la Directiva de protección de datos de 1995 no han exigido el nombramiento de DPD por ley (como Austria, que en otros aspectos sigue a menudo el ejemplo alemán), o sólo incluido como opción (como en Francia), la institución a menudo ha sido ampliamente adoptada. En varios países, existen asociaciones nacionales de DPD, y también hay una Confederación de Organizaciones Europeas de Protección de Datos, CEDPD, por sus siglas en inglés, que ha emitido "guías prácticas para organizaciones" para "elegir al mejor candidato" como DPD.[239] A nivel mundial, existe la Asociación Internacional de Profesionales de la Privacidad (IAPP),con sede en Estados Unidos, que entre otras cosas ofrece certificaciones de protección de datos para los "profesionales de la privacidad de la información"- (aunque, al igual que otros sistemas de certificación de RPD, éstos no constituyen certificaciones de cumplimiento basadas en GDPR: véase la sección 2.5.3, más adelante, bajo el epígrafe "Formación y certificación formales[de RPD]").

(Véase la lista de las asociaciones de DPD al final de esta subsección, con los links a sus respectivas páginas web).

La Directiva de protección de datos de 1995 aún no requería la designación de DPD por parte de los controladores sujetos a ella. Por el contrario, reconoció la existencia de DPD en la legislación y la práctica de los Estados miembros, al permitir a los Estados miembros eximir a los controladores de la obligación de notificar las operaciones de tratamiento a la agencia nacional de protección de datos (APD) pertinente, si la legislación del Estado miembro exigía que el controlador relevante designar un DPD "responsable en particular [] para garantizar de manera independiente la aplicación interna de las disposiciones nacionales adoptadas de conformidad con la presente Directiva [y] para mantener [un] registro de las operaciones de tratamiento realizadas por el controlador, que contengan [la misma información] como de otro modo tendría que ser notificado a la APD] "(Art. 18 (2)).

Sin embargo, el reglamento de la UE de 2001 que establece las normas de protección de datos para las instituciones de la UE, el Estado miembro (Reglamento (CE) 45/2001)[240], exige que cada institución u organismo de la UE designe al menos un DPD (Art. 24). Las normas sobre los DPD de las instituciones de la UE, consagradas en este reglamento, son muy similares a las del RGPD.

La llamada Directiva de Protección de Datos de Aplicación de la Ley (Directiva 2016/680),[241] adoptada al mismo tiempo que el RGPD, requiere que las "autoridades competentes" sujetas a ese instrumento también designen un DPD; y las Pautas GT29 sobre DPD (que, como se indica más adelante, contienen la guía principal para los DPD designados bajo el RGPD) enfatizan que "mientras estas guías se enfocan en los DPD bajo el RGPD, la guía también es relevante con respecto a los DPD bajo la Directiva 2016/680, con respecto a sus disposiciones similares".[242]

---

[238] Los términos alemanes son, respectivamente: *behördliche-* y *betriebliche Datenschutzbeauftragter* (DPD de la administración y de empresa) Para obtener un breve resumen de su función y funciones según la ley alemana, véase, por ejemplo: https://www.wbs-law.de/eng/practice-areas/internet-law/it-law/data-protection-officer/
Para una exposición más detallada en alemán, véase, p.e. Däubler/Klebe/Wedde/Weichert, *Kompaktkommentar zum BDSG* (Breve comentario sobre la Ley Federal Alemana de Protección de Datos), 3ª ed. (2010), comentarios sobre §4f BDSG, que incluye 85 notas al margen, pág. 187 – 213

[239] CEDPD, *Choosing the best candidate as your Data Protection Officer (DPD) – Practical guidelines for organisations*, (Elección del mejor candidato para su DPD – Guía práctica para las organizaciones), 30 de mayo, 2016, disponible en: http://businessdocbox.com/Human_Resources/77901620-Choosing-the-best-candidate-as-your-data- protection-officer-DPD-practical-guidelines-for-organisations.html

[240] Título completo: *Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data*, O.J. L 8 of 12.1.2001, p. 1 et seq., disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001R0045&from=EN

[241] Título completo: *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*, OJ L 119, 4.5.2016, p. 89ff., disponible en: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN

[242] Grupo de Trabajo Art. 29, Guidelines on Data Protection Officers ('DPOs'), (Guía sobre DPDs), adoptada originalmente el 13 de diciembre de 2016, última revisión, adoptada el 5 de abril, 2017 WP243 rev.01), p. 4, nota 2., disponible en:

Los DPD internos de la UE trabajan en estrecha colaboración con el Supervisor Europeo de Protección de Datos (SEPD) y han creado una Red de responsables de protección de datos de las instituciones y organismos de la UE. El SEPD creó un sitio web, el "Rincón del DPD" para apoyarlos. Tras un documento de posicionamiento de 2005 del SEPD,[243] en 2010, la Red emitió un conjunto de estándares delegados de protección de datos de las instituciones de la UE que trabajan bajo el Reglamento (CE) 45/2001.[244]

En 2012, el SEPD emitió un informe sobre el estado de los DPD, como parte de su monitoreo del cumplimiento por parte de las instituciones del Reglamento (CE) 45/2001.[245] Este informe confirma que la función del DPD está bien establecida dentro de las instituciones y órganos de la UE., y que en general cumplen con el Artículo 24 del Reglamento, pero también señalaron "algunas áreas de preocupación" que son objeto de un mayor seguimiento por parte del SEPD.[246] Estos documentos contienen una guía bastante extensa sobre asuntos relacionados con el nombramiento, el puesto y las tareas de los DPD.

Más recientemente, y más directamente relacionado con este Manual, el Grupo de Trabajo Artículo 29 proporcionó directrices sobre DPD en preparación para la plena aplicación del RGPD.[247] El Consejo Europeo de Protección de Datos (CEPD), que tomó el relevo del GT29 al entrar en vigor la plena aplicación del GDPR, respaldó formalmente estas directrices (así como los demás documentos orientativos sobre cuestiones derivadas del GDPR, adoptados por el GT29 antes de esa fecha).[248]

Como consecuencia, varias APD nacionales también han emitido guías sobre DPD, algunas incluso antes del RGPD, y han promovido servicios específicos para ellos.[249]

La presente Sección del Manual se basa en las directrices GT29 en particular, pero también se refiere a la otra orientación mencionada anteriormente, cuando sea apropiado, para enriquecer el pensamiento del lector.

El punto principal que se debe mencionar en esta introducción al DPD es que, términos del RGPD, es una institución crucial nueva que debe considerarse como un medio esencial para dar efecto práctico a la

---

http://ec.europa.eu/NUEVOsroom/Artículo29/item-detail.Cons.m?item_id=612048
En lo sucesivo, "WP29 Guidelines on DPDs"

[243] 153SEPD, Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001, disponible en:
https://SEPD.europa.eu/sites/edp/files/publication/05-11-28_DPD_paper_en.pdf

[244] https://SEPD.europa.eu/sites/edp/files/publication/10-10-14_DPD_standards_en.pdf

[245] SEPD, *Monitoring compliance of EU institutions and bodies with Artículo 24 of Regulation (EC) 45/2001 – Report on the Status of Data Protection Officers*, 17 de diciembre de 2012, disponible:
https://SEPD.europa.eu/sites/edp/files/publication/2012-12-17_DPD_status_web_en.pdf

[246] *Idem*, pág. 3.

[247] Véase nota 242, más arriba.

[248] EDPB, *Endorsement 1/2018*, refrendando, entre otras cosas, las *Directrices WP29 sobre DPD* (enunciadas como el 7º documento refrendado), adoptado el 25 de mayo de 2018, disponible en: https://edpb.europa.eu/sites/edpb/files/files/NUEVOs/endorsement_of_wp29_documents_en_0.pdf

[249] Véase p.e.:
Guide de Correspondant Informatique et Libertés (CIL) (Guide Pratique Correspondant), (Guía del responsable de Informática y de las Libertades (CIL) (Guía Práctica), publicada por CNIL, Agencia Francesa de Protección de Datos en 2011, disponible en:
https://www.cnil.fr/sites/default/files/typo/document/CNIL_Guide_correspondants.pdf
En **Italia**, la Agencia Nacional de Protección de Datos, el *Garante del Privacy*, ha publicado un documento con FAQS (Preguntas Frecuentes y Respuestas) sobre los DPDs, disponible en:
https://www.garanteprivacy.it/garante/doc.jsp?ID=8036793 (FAQs para DPD en el sector privado)
https://www.garanteprivacy.it/garante/doc.jsp?ID=7322110 (FAQs para DPD en el sector público)
En **Polonia**, la agencia nacional de protección de datos, la Urząd Ochrony Danych Osobowych (UODO) ofrece consejos y recomendaciones útiles acerca de la aplicación del RGPD en su página web, en una parte dedicada específicamente a los DPD: https://uodo.gov.pl/p/najwazniejsze-tematy/inspektor-ochrony-danych.
Antes de la entrada en vigor del RGPD, la agencia polaca mantenía la página web ABI para lo que se denominaba "Administradores de seguridad de la información", que contenía información útil para que futuros DPD se preparasen para realizar estas funciones, véase https://abi.giodo.gov.pl/. A través de este servicio, los futuros DPD podían plantear preguntas y sugerencias relativas a la aplicación y la interpretación de disposiciones legales relativas a la protección de datos personales.
En el **Reino Unido**, la Agencia Nacional de Protección de Datos, el ICO - Information Commissioner´s Office – ofrece en su página web unas guías que sobre todo reflejan (con referencias cruzadas) las Guías del WP29, Véase:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-GDPR/accountability-and- governance/data-protection-officers/

"responsabilidad" (deber de demostrar cumplimiento) principio discutido anteriormente: cuando un DPD ha sido designado y cumple debidamente sus tareas (como se analiza en la parte 3 de este manual), eso debería dar como resultado un cumplimiento mejor, más completo y serio con el RGPD que el que se logró a través de la supervisión principalmente externa Las autoridades de protección de datos en relación con la Directiva de protección de datos de 1995.Ahora, bajo el RGPD, los APD tienen un punto de contacto directo e informado dentro de la organización de todos los controladores relevantes y un aliado dentro de la organización del controlador. No es sorprendente que varias APD hayan hecho de ella una de sus prioridades, ahora que el RGPD ha entrado en vigor, para verificar si las organizaciones que tienen que designar un DPD (como se explica a continuación, en la subsección 2.3.2) lo han hecho así.[250]

[250] Por ejemplo, la APD de Suecia ha anunciado que va a revisar qué organizaciones en los sectores bancario, salud y seguros han nombrado un DPD. Véase
https://www.datainspektionen.se/nyheter/datainspektionen-inleder-forsta-granskningarna-enligt-GDPR/
La APD holandesa destaca de manera parecida en su plan para 2018-2019 que, en particular, en relación a las autoridades públicas, comprobará "el cumplimiento de la obligación de mantener un registro de las operaciones de procesado, el deber de nombrar un DPD y la manera en la que la organización posiciona al DPD y le permite cumplir sus tareas bajo el RGPD", Véase: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoEstado Miembro/files/toezichtkader_autoriteit_persoonsgegev ens_2018-2019.pdf (p. 7, bajo el título "Overheid" (autoridad pública) (traducción nuestra).

ASOCIACIONES INTERNACIONALES Y NACIONALES DE DELEGADOS DE PROTECCIÓN DE DATOS:

Asociaciones internacionales:

A nivel mundial:

International Association of Privacy Professionals (IAPP):
(Asociación Internacional de Profesionales de la Privacidad)
https://iapp.org/certify/cipp/

Europeas:

Network of Data Protection Officers of the EU Institutions and Bodies:
(Red de los Delegados de Protección de Datos de las Instituciones y Entes de la UE)
https://SEPD.europa.eu/data-protection/eu-institutions-DPD_en

Confederation of European Data Protection Organisations, CEDPD
(Confederación de Organizaciones Europeas de Protección de Datos, CEDPD)
http://www.ceDPD.eu/

Asociaciones nacionales:
(Las marcadas con un * son miembro de la CEDPD)

Francia:
Association Française des Correspondants à la Protection des Données à Caractère Personnel, AFCDP:*
https://www.afcdp.net/

Irlanda:
Association of Data Protection Officers, ADPD:*
https://www.DPD.ie/

Italia:
Associazone Data Protection Officer, ASSO DPD:*
http://www.assoDPD.it/en/home_en/

Países Bajos:
Nederlands Genootschap voor Functionarissen Gegevensbescherming, NGFG:*
https://www.ngfg.nl/

Polonia:
Stowarzyszenie Administratorów Bezpieczeństwa Informacji, SABI:*
http://www.sabi.org.pl/

Continúa en la siguiente página

.

España:
Asociación Profesional Española de Privacidad, APEP:*
http://www.apep.es/

Reino Unido:
National Association of Data Protection & Freedom of Information Officers, NADPD:
https://naDPD.co.uk/

Los miembros alemán y austríaco de la CEDPD, respectivamente Gesellschaft für Datenschutz und Datensicherheit e.V., DGG* (fundada en 1977) y Arge Daten* tienen un ámbito de Asociados más amplio que únicamente DPDs, pero son ambas miembros de la CEDPD:
https://www.gdd.de/ueber-uns
http://www.argedaten.at/php/cEstado Miembro_monitor.php?q=PUB-TEXT-ARGEDATEN&s=15904tpb

2.5.2 El deber de nombrar un Delegado de Protección de Datos para las autoridades públicas[251]

El nombramiento de un DPD es obligatorio para todas las autoridades u organismos públicos que procesan datos personales que están sujetos al RGPD (Art. 37 (1) (a)).[252] Aunque en principio lo deja en manos de los Estados miembros, el GT29 toma con razón un punto de vista más amplio de este requisito:[253]

> "Autoridad o ente público"
>
> El RGPD no define lo que constituye una "autoridad u organismo público". El GT29 considera que dicha noción debe determinarse en virtud de la legislación nacional. En consecuencia, las autoridades y los organismos públicos incluyen a las autoridades nacionales, regionales y locales, pero el concepto, según las leyes nacionales aplicables, generalmente también incluye una serie de otros organismos regulados por el derecho público.[254] En tales casos, la designación de un DPD es obligatoria.

Sin embargo, el deber de designar un DPD, de hecho, se extiende más allá de esta categoría puramente formal.

> Entidades del sector privado que llevan a cabo "tareas de interés público" o que "ejercen autoridad oficial"

El GT29 destaca, con referencia a la base legal especial para el tratamiento en el art. 6 (1) (e) del RGPD, que (independientemente de las limitaciones en el deber de designar un DPD para "puramente" entidades del sector privado)[255] un DPD también debe ser siempre designado por controladores del sector privado que realicen

---

[251] Aparte de las entidades privadas que llevan a cabo "tareas públicas" o "ejercer la autoridad pública, como se explica en el texto, el deber de designar un DPD para empresas "puramente" privadas (comerciales) no se trata en este Manual. Basta con señalar que, para tales entidades, el Reglamento en principio hace obligatorio el DPD solo en los siguientes casos:
-cuando las actividades principales del controlador o el procesador consisten en operaciones de tratamiento de datos que, por su naturaleza, su alcance y / o sus elementos, requieren un seguimiento regular y sistemático de los titulares de datos a gran escala; o
- cuando las actividades principales del controlador o el procesador consisten en el tratamiento a gran escala de categorías especiales de datos de conformidad con el Artículo 9 [es decir, de los llamados 'datos confidenciales'] y datos personales relacionados con condenas penales y delitos a los que se hace referencia en Artículo 10.
(Artículo 37(1) (b) and (c) RGPD)
Estas condiciones se analizan con cierto detalle en las Guías WP29 para DPD. Aquí, puede ser suficiente tener en cuenta que en la práctica a la mayoría de las empresas de cualquier tamaño les resultará útil designar a un DPD para cumplir con los requisitos de "responsabilidad" / "obligación de demostrar el cumplimiento", que se analizan en la sección 2.2.

[252] La única excepción a este respecto se refiere a los "tribunales que actúan en su capacidad judicial" (Art. 37 (1) (a) RGPD). Sin embargo, como destaca el WP29 en sus Guías sobre DPD (nota 242 anterior), esto no significa que no tengan que cumplir con el Reglamento, por el contrario: ellos también deben cumplirlo. Y con respecto al procesado por parte de los tribunales que no sean de su capacidad judicial, están sujetos al requisito de designar un DPD. Este manual no trata de los DPD de organismos que realizan procesos que están completamente fuera del alcance de la legislación de la UE, como las agencias de seguridad nacional.

[253] *WP29 Guidelines on DPDs*, (nota 242, véase más arriba) p. 6.

[254] Véase, p.e., la definición de "organismo del sector público" y "órgano regulado por el derecho público" en el Artículo 2(1) y (2) de la Directiva 2003/98 / CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, sobre la reutilización de información del sector público, DO L 345 de 31.12.2003, p. 90 et seq. [nota original]. El texto en inglés de esta directiva está disponible aquí:
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003L0098&from=EN

[255] Véase nota 251, más arriba.

"tareas ... en el interés público "o quién" ejerce la autoridad oficial ", incluso si no son formalmente "autoridades públicas" en los términos de las leyes nacionales, porque en tales actividades su función será similar a la función de las autoridades públicas:[256]

> Se puede llevar a cabo una tarea pública, y la autoridad pública puede ser ejercida no solo por autoridades u organismos públicos, sino también por otras personas físicas o jurídicas regidas por el derecho público o privado, en sectores tales como, según la reglamentación nacional de cada Estado miembro, Servicios de transporte público, suministro de agua y energía, infraestructura vial, radiodifusión de servicio público, vivienda pública u organismos disciplinarios para profesiones reguladas.
>
> En estos casos, los interesados pueden estar en una situación muy similar a cuando sus datos son tratados por una autoridad u organismo público. En particular, los datos pueden tratarse para fines similares y los individuos a menudo tienen poca o ninguna opción sobre cómo se tratarán sus datos y, por lo tanto, pueden requerir la protección adicional que puede aportar la designación de un DPD.
>
> **A pesar de que no existe obligación en tales casos, el GT29 recomienda, como buena práctica, que las organizaciones privadas que realizan tareas públicas o que ejercen una autoridad pública designen un DPD**. Tal actividad de DPD cubre todas las operaciones de tratamiento realizadas, incluidas aquellas que no están relacionadas con el desempeño de una tarea pública o el ejercicio de un deber oficial (por ejemplo, la administración de una base de datos de empleados).

A los ejemplos mencionados por el GT29 se podría agregar el funcionamiento de prisiones y otras instituciones o servicios estatales (como la deportación de inmigrantes detenidos ilegalmente en un país), por parte de entidades privadas. En todos estos casos, las entidades privadas actúan efectivamente como Miembro del Estado y, en todos los casos, las empresas en cuestión deben designar un DPD. Los Estados miembros pueden aclarar esto en su legislación nacional e imponer el deber de designar un DPD para controladores específicos o tipos de controladores distintos de las autoridades u organismos públicos formales (véase el artículo 37(4)).

EJEMPLO:
En **Italia,** la autoridad nacional de protección de datos, el *Garante* considera que todas las entidades que entran en el ámbito de aplicación de las Secciones 18 a 22 del Código de Protección de Datos de Italia deben considerarse obligadas a designar un DPD. Las secciones 18 a 22 del Código de DP establecen las reglas generales que se aplican al tratamiento realizado por entidades públicas, tales como organismos administrativos estatales, organismos públicos de búsqueda sin fines de lucro a nivel nacional, regional y local, regiones, autoridades locales, universidades, Cámaras de Comercio, agencias de salud, autoridades de supervisión independientes, etc.

El *Garante* también sostiene que siempre que una entidad privada desempeña funciones públicas, por ejemplo, basada en una licencia o concesión: se recomienda encarecidamente la designación de un DPD, aunque no sea obligatorio. Añade, con referencia a las Pautas GT29 sobre DPD, que, si un DPD se designa de manera voluntaria, se aplican los mismos requisitos y condiciones que en el caso de un DPD designado de forma obligatoria, en términos de Criterios para la designación, cargo y tareas de los DPD.

DPDs para procesadores

Como señala el GT29, el Artículo en el RGPD que impone la obligación de designar un DPD en ciertos casos (Art. 37), como se describe para el sector público anterior, se aplica tanto a los controladores como a los

[256] *WP29 Guidelines on DPDs* (nota 242, véase más arriba), p. 6. El uso del término "tarea pública" y "autoridad pública" por el WP29es simplemente un asunto lingüístico: en las directrices, estos términos se refieren a las "tareas de interés público" y al "ejercicio de la autoridad oficial" mencionados en el art. 6 (1) (e) del RGPD.

procesadores.[257] Añade:[258]

> Dependiendo de quién cumpla con los criterios de designación obligatoria, en algunos casos solo el controlador o solo el procesador, en otros casos tanto el controlador como su procesador deben designar un DPD (quien debe cooperar entre sí).
>
> Es importante destacar que incluso si el controlador cumple con los criterios para la designación obligatoria, no es necesario que su procesador designe un DPD. Esto puede, sin embargo, ser una buena práctica.

Para el sector público, donde todos los organismos relevantes deben, en cualquier caso, designar un DPD (como se expuso anteriormente), esto puede no parecer un problema importante. Sin embargo, en vista del último comentario del GT29, si una autoridad pública subcontratara alguna actividad de tratamiento a una entidad privada (por ejemplo, la contabilidad o la realización de encuestas) sería al menos recomendable elegir un procesador que en sí mismo también tiene un DPD, o para requerir un procesador que aún no tiene un DPD para designar uno.

En la medida en que las autoridades públicas que trabajan en conjunto también pueden actuar a veces como procesadores entre sí, eso también debe reflejarse en el registro escrito de sus acuerdos, anotado en el siguiente subtítulo y discutido en la Parte 3, subsección 3.1.

DPDs para grandes autoridades públicas o grupos de autoridades

Junto con la "transición digital", los datos personales se procesan cada vez más en entornos y arquitecturas técnicas muy complejos, en los que diferentes agentes trabajan en estrecha colaboración y han desempeñado funciones conjuntas o vinculadas en relación con diversas operaciones de tratamiento, incluso en relación con los ciudadanos. Este es también el caso en el sector público, que de hecho tiene sus propias complejidades en términos de la medida de la autonomía que pueden tener las diferentes agencias dentro de un marco constitucional o administrativo-legal más amplio. Como se explica más adelante en la Parte 3, Sección 3.1, una de las primeras tareas de cualquier DPD nuevo nombrado debe ser "determinar" el contexto para el tratamiento de datos personales que será responsable de supervisar y / o asesorar. Parte de este trabajo será aclarar, con respecto a estos contextos complejos qué estados precisos tienen las diferentes entidades que forman parte del complejo, y hacer y registrar los acuerdos adecuados.

A este respecto, debe señalarse que el RGPD estipula expresamente (como lo hizo la Directiva de protección de datos de 1995) que "cuando los propósitos y medios de... el tratamiento esté determinados por la legislación de la Unión o del Estado miembro" autoridades) “la legislación de la Unión o del Estado miembro puede establecer el controlador o los criterios específicos para su nominación” (art. 4 (7)). A menudo tendrá sentido, en tales casos, designar al DPD para todo el tratamiento cubierto por tal determinación en las oficinas de la entidad que se designa como el controlador del tratamiento; de hecho, la ley que determina el controlador puede aclarar eso.

Si la ley no lo determina, es posible que el asunto deba ser resuelto por el ministro de gobierno pertinente, un alto funcionario o entre las propias entidades públicas. Esto debería llevar a acuerdos claros para las responsabilidades y competencias respectivas de diferentes DPD en diferentes entidades que forman parte del complejo. Parte de esto implica la decisión sobre dónde designar un DPD o varios DPD. Los acuerdos también deben cubrir los enlaces y acuerdos entre diferentes DPD en entidades vinculadas operativamente.

Algunos organismos públicos muy grandes (o los ministros del gobierno o altos funcionarios de dichos organismos) pueden decidir nombrar varios DPD para cada una de sus partes constituyentes − siempre y cuando refleje la distribución real de competencias de toma de decisiones entre los departamentos o unidades independientes dentro de dichos organismos. O pueden decidir nombrar un DPD para todo el organismo, para trabajar con personas designadas en aquellas partes de la entidad de gran tamaño en su totalidad. En este último

---

[257] *WP29 Guidelines on DPDs* (nota 242, véase más arriba), Sección 2.2, DPD del procesador, en la pág. 9.
[258] Ídem. El WP29 ofrece algunos ejemplos, tomados del sector privado, que se centran en las limitaciones de la obligación de nombra un DPD para dicho sector; por ese motivo, no son especialmente útiles para el presente Manual.

caso, se desprende de los comentarios realizados por el GT29 en el contexto de la designación de DPD sobre la base de un contrato de servicio (que se analiza en la siguiente subpartida) que dichas personas designadas en departamentos o partes distintas de la gran organización deben, por un lado, cumplir con los requisitos de los DPD, en particular de no tener ningún conflicto de intereses, y por otro lado, debe recibir una protección similar a la del propio DPD, y no ser penalizado por el ejercicio de las funciones relacionadas con el DPD.[259]

A la inversa, el RGPD permite expresamente grupos de **cuerpos públicos más pequeños (formalmente distintos)** - como las autoridades locales (Fr: *comunas*) - para decidir (o recibir instrucciones) para designar conjuntamente un DPD:

> Cuando el controlador o el procesador son una autoridad u organismo público, se puede designar un único delegado de protección de datos para varias de dichas autoridades u organismos, teniendo en cuenta su estructura y tamaño organizativos. (Art. 37 (3))

Un DPD central o común de este tipo podría ser un funcionario de una de las autoridades, o podría decidirse contratar conjuntamente un DPD externo, sobre la base de un contrato de servicio (como se explica nuevamente en la siguiente subpartida). Si se designa un DPD central (interno o externo), las demás entidades (pequeñas) aún deben designar a una persona del personal responsable de la coordinación con el DPD central (conjunto), y en ese caso, se aplica lo mismo que se acaba de mencionar con respecto a las autoridades más grandes: las personas designadas deben cumplir los requisitos de un DPD, y recibir una protección similar a la del DPD propiamente dicha.

DPDs externos

Como ya se señaló en el subtítulo anterior, las autoridades públicas (y las empresas privadas) no tienen que crear un puesto interno para un DPD, y mucho menos uno a tiempo completo (aunque muchos organismos más grandes probablemente elijan hacerlo si No lo han hecho ya). Más bien:

> El delegado de protección de datos puede ser un miembro del personal del controlador o procesador, o cumplir las tareas sobre la base de un contrato de servicio (Art. 37 (6))

En Alemania, donde se origina la idea del DPD,[260] los despachos legales u otros expertos independientes ofrecen funciones de DPD de esta manera. Además, las "asociaciones y otros organismos que representan categorías de controladores o procesadores" pueden, al parecer, proporcionar funciones DPD a sus miembros y, a este respecto, actuar en nombre de todos ellos (véase el artículo 37(4)). Esto sería útil en particular para las pequeñas empresas. Una serie de Consultorías importantes y despachos legales también ofrecen soporte de DPD "sobre la base de un contrato de servicio", y también habrá algunas firmas más pequeñas, especialmente aquellas especializados en el trabajo de las TIC, que ofrecerán este servicio sobre tal base.

Sin embargo, dichos DPD externos no deben estar muy alejados de los organismos a los que prestan sus servicios; como se explica en la siguiente parte del Manual, los DPD deben tener un conocimiento completo e íntimo de esos cuerpos y sus operaciones de tratamiento. También deben ser accesibles de forma completa y fácil, tanto para el personal de los organismos en cuestión como para los interesados y las agencias de protección de datos (autoridades de supervisión). Sus datos de contacto deben figurar claramente en los sitios web de los organismos pertinentes y en los folletos pertinentes, etc.

La agencia francesa de protección de datos, la CNIL, considera que un DPD debe ser "preferiblemente" un miembro del personal de la organización del controlador, pero acepta que para las pequeñas y medianas empresas esto no siempre es posible.[261]

En el sector público, a menudo puede ser preferible tener una DPD del sector en particular, por ejemplo, como se discutió en el subtítulo anterior, una DPD central para un organismo público grande o una conjunta para un grupo de autoridades más pequeñas adjuntas para uno de ellos, en lugar de que una empresa del sector privado actúe como DPD externa, pero esto dependerá de la cultura y las prácticas del país en

---

[259] Cons. WP29 Guidelines on DPDs (nota 11, véase más arriba), Sección 2.4, último punto en la pág. 12
[260] Véase subsección 2.3.1, más arriba.
[261] CNIL, *Guide Pratique Correspondant* (nota 249, véase más arriba), p. 6

cuestión.

2.5.3 Cualificaciones, calidades y posición del DPD

Experiencia requerida

El Reglamento estipula que:

> El oficial de protección de datos se designará en función de las cualidades profesionales y, en particular, del **conocimiento experto de la legislación y las prácticas de protección de datos y de la capacidad para cumplir las tareas mencionadas** en el Artículo 39 [como se explica a continuación, en 2.3.4].
> (Art. 37(5), énfasis añadido)

En el primer punto - el conocimiento de los experto-, el documento de "estándares profesionales" de las APDs institucionales de la UE señala la necesidad de lo siguiente[262]

> (a) Experiencia en el ámbito de la legislación de la UE sobre privacidad y protección de datos, en particular el Artículo 16 del Tratado de Funcionamiento de la Unión Europea, el Artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, Reglamento (CE) 45/2001. y otros instrumentos legales de protección de datos relevantes, y experiencia en TI y seguridad de las TI; y
>
> (b) Una buena comprensión de la forma en que opera la institución [a la que se designa DPD] y sus actividades de tratamiento de datos personales, y la capacidad de interpretar las reglas de protección de datos relevantes en ese contexto.

El conocimiento técnico de los sistemas de TI debe ser especialmente enfatizado. Como dice la agencia **francesa** de protección de datos, la CNIL:[263]

> En relación con la informática, se requiere una buena comprensión de la terminología, las prácticas [de TI] y diferentes estados de tratamiento de datos. Un DPD debe conocer, por ejemplo, la administración y explotación de sistemas de datos, tipos de software, archivos y almacenamiento de sistemas de datos, así como sobre los requisitos de las políticas de confidencialidad y seguridad (cifrado de datos, firmas electrónicas, biometría,...). Este conocimiento debe permitir a [el DPD] monitorear el despliegue de proyectos de TI y proporcionar consejos útiles al controlador responsable del tratamiento.

El considerando 97 del RGPD también destaca que:

> El nivel necesario de conocimiento experto se debe determinar, en particular, de acuerdo con las operaciones de tratamiento de datos realizadas y la protección requerida para los datos personales tratados por el controlador o el procesador.

En otras palabras, la naturaleza del "conocimiento experto" y las "habilidades" requeridas pueden variar dependiendo de las actividades del controlador: un DPD para una autoridad fiscal requerirá una experiencia diferente a la que trabaja para una autoridad educativa o de bienestar. El SEPD se refiere a esto como la necesidad de "**proximidad**" (del DPD a la entidad a la que sirve):[264]

> El DPD tiene un papel central dentro de la institución / organismo: los DPD están [es decir, deberían estar] familiarizados con los problemas de la entidad para la que trabajan (idea de

---

[262] Red de Delegados de Protección de Datos de las Instituciones y los Organismos de la UE, *Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001* (véase nota 244, más arriba), pág. 3 – 4.
[263] CNIL, Guide Pratique Correspondant (véase nota 249, más arriba), p. 8 (traducción nuestra).
[264] SEPD, *Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001* (véase nota 243, más arriba), p. 5, énfasis añadido

> proximidad) y, dado su estado, tienen un papel crucial que desempeñar para dar consejos y ayudar a resolver problemas de protección de datos [lea: como específico del cuerpo en cuestión].

Como indican las Directrices del GT29 sobre DPD:[265]

> El DPD también debe tener una comprensión suficiente de las operaciones de procesado llevadas a cabo [en el sector y la organización relevantes], así como de la información del Sistema de Información y las necesidades de seguridad y protección de datos del controlador.
>
> En el caso de una autoridad u organismo público, el DPD también debe tener un conocimiento sólido de las normas y procedimientos administrativos [internos] de la organización.

A lo que se podría añadir: y de las leyes y reglas y procedimientos bajo los cuales opera el organismo público relevante (por ejemplo, la Ley de Impuestos, o la Ley de Educación, etc.), y el derecho y procedimiento administrativo en general.

Por otro lado, como se indica a continuación bajo los encabezados "*Conflictos de interés*" y "*Posición dentro de la organización*", designar a alguien del personal existente de un organismo público puede causar un problema, especialmente si la persona elegida es nombrada a tiempo parcial y retiene otras funciones dentro del cuerpo en cuestión.

El conocimiento experto de la legislación y las prácticas de protección de datos generalmente se puede demostrar mediante cursos de capacitación y fuera de línea, etc., realizados por la persona en cuestión, como los que se ofrecen en el programa "T4DATA" en el contexto del cual se escribió este Manual. Pero muchos otros cursos, de diferentes niveles y calidad, también se ofrecen ampliamente como se señala a continuación.

Formación formal y certificación

En el momento de redactar este Manual (diciembre de 2018) se estaban tomando medidas en un Estado miembro de la UE, España, hacia la creación de un sistema de certificación formal para DPD, pero aún no está operativo.[266] Además, este sistema de certificación para DPD (y otros en consideración) se basa en la ISO 17024; es decir, en un sistema de ceritificación para personas físicas y profesionales; por consiguiente, no cumplen los requisitos de la ISO 17065, que es el sistema al que se hace referencia en el concepto de certificación en virtud del RGPD (certificación de servicios, productos, posiblemente sistemas de gestión). Por lo tanto, las certificaciones reltivas a los DPD son diferentes de las "certificaciones" del artículo 42 del RD-PIB. Son encomiables, pero no son certificaciones que cumplan con los requisitos del RGPD.

En **Francia**, la APD (CNIL) emitió dos "référentiels" (en inglés: "specifications") relativas a certificaciones de DPD el 11 de octubre de 2018, que se publicaron en el Diario Oficial nacional. Una de ellas trata la certificación relativa a las competencias de los DPD, y la otra aborda la estipulación de las competencias de los DPD y la organización de acreditación autorizada para certificar DPD.[267]

En **Alemania**, se ofrecen varios cursos y seminarios para capacitar a personas, algunos de ellos conducen a algún tipo de certificación[268], pero a pesar de ser una institución establecida desde hace mucho tiempo en el país, no existe un plan oficialmente respaldado por ley. Varias de las asociaciones internacionales y nacionales de DPD, enumeradas anteriormente, también ofrecen capacitaciones especializadas - pero de

---

[265] *WP29 Guidelines on DPDs* (nota 242, véase más arriba), p. 11

[266] La Agencia Española de Protección de Dato (AEPD) de España has establecido un Esquema de Certificación de Delegados de Protección de Datos de la Agencia Española de Protección de Datos (Esquema AEPD-DPD) bajo el cual la Entidad Nacional de Acreditación – ENAC puede acreditar a Entidades de Certificación que a su vez estarán autorizadas a emitir una certificación relevante sobre la base de criterios desarrollados por la AEPD y un examen formal. Véase:
https://www.aepd.es/reglamento/cumplimiento/common/esquema-aepd-dpd.pdf (versión 1.3, 13 June 2018) Sin embargo, aún no se ha acreditado a dichos Organismos de Certificación y, por lo tanto, no se han emitido Certificaciones de DPD.
Véase también la breve discusión más general de los esquemas de certificación en 2.1, más arriba.

[267] Véase:
https://www.cnil.fr/fr/loutil-pia-mis-jour-pour-accompagner-lentree-en-application-du-rgpd

[268] Cons., p.e.: https://www.datenschutzexperten.de/grundlagenseminar-ausbildung-betrieblicher-datenschutzbeauftragter- nach-bdsg-mit-dekra.html

nuevo, sin fundamento legal.[269]

Muchos de estos cursos o seminarios de capacitación están dirigidos específicamente a proporcionar a los aprendices experiencia en el RGPD y orientación sobre las tareas asignadas a los DPD en el RGPD. Pero el RGPD (como las leyes alemanas y otras leyes nacionales) no contempla específicamente ningún criterio o esquema de certificación más detallado. Posiblemente, en el futuro, aparte de España, otros Estados miembros también proporcionarán dichos esquemas formales, oficialmente reconocidos, y/o el Consejo Europeo de Protección de Datos podría (probablemente de manera informal) respaldar algunos.[270] Pero hasta que esto suceda, los parámetros seguirán siendo bastante abiertos. Como dijo la agencia **italiana** de protección de datos, el Garante:[271]

> Como es el caso de todas las denominadas "profesiones no reguladas", se han desarrollado esquemas de propiedad para certificar, de manera voluntaria, las habilidades y competencias profesionales. Tales esquemas son gestionados por varios organismos de certificación. Las certificaciones de este tipo, que no están incluidas en el alcance del Artículo 42 del RGPD, se emiten a veces después de la asistencia a cursos de capacitación y / o verificación de aprendizaje.
>
> Si bien representa una herramienta valiosa que, de manera similar a otras certificaciones, puede proporcionar evidencia de que un profesional tiene al menos un conocimiento básico de las reglas aplicables, dichas certificaciones no equivalen, per se, a "calificaciones" que permitan el desempeño de tareas relacionadas con DPD y no puede reemplazar la obligación de los organismos administrativos públicos de evaluar los requisitos que un DPD debe cumplir con vistas a las tareas y deberes establecidos en el Artículo 39 del RGPD.

Como lo expresa la Confederación de Organizaciones Europeas de Protección de Datos (CEDPD):[272]

> Los candidatos probablemente le mostrarán una gran cantidad de certificados y diplomas que han obtenido a lo largo de los años para mostrar su calificación. ¿Pero cómo saber cuáles son valiosos y cuáles no? Lo primero que debe verificar es las credenciales de la parte que otorga la capacitación y la certificación. Si se trata de una organización pan-UE o nacional reconocida y acreditada (en algunos países incluso las autoridades de protección de datos lo certifican), puede sentirse más cómodo. Además, consulte la agenda de los cursos de formación. Un evento de un día o certificaciones obtenidas principalmente como resultado de un pago y un examen muy simple no tendrán a nadie capacitado para un DPD fiable.

Todos los diversos documentos de orientación también hacen hincapié en la necesidad de las organizaciones de garantizar que su DPD pueda continuar manteniendo y mejorando su experiencia, también después de su nombramiento, asistiendo a cursos y seminarios relevantes. De hecho, esto también es requerido por el RGPD (vea las últimas palabras en el Art. 38 (2)). Como lo pone el GT29:[273]

> Los DPD deben tener la oportunidad de mantenerse al día con respecto a los desarrollos dentro de la protección de datos. El objetivo debe ser aumentar constantemente el nivel de experiencia de los DPD y se les debe alentar a participar en cursos de capacitación sobre protección de datos y otros para el estado de desarrollo profesional, como la

---

[269] El documento de la UE sobre los estándares para los DPD de las instituciones recomienda los esquemas de la Asociación Internacional de Profesionales de la Privacidad (IAPP). La IAPP ofrece una certificación específica para las regiones, incluyendo una para Europa que cubre el RGPD de manera específica. Véase: https://iapp.org/certify/cippe/
Red de Delegados de Protección de Datos de las Instituciones y los Organismos de la UE, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (véase nota 212, más arriba), p. 5. El documento institucional los DPD de la UE también menciona la gestión de la seguridad de TI y las certificaciones de auditoría, pero son más generales y no están específicamente dirigidas a la protección de datos

[270] La Guía WP29 Guidelines on DPDs (véase nota 209, más arriba), simplemente dice que "también es útil si las autoridades de supervisión promueven una capacitación adecuada y regular para los DPD" (p. 11).

[271] Garante del Privacy, *FAQs on DPDs* (véase nota 218, más arriba), Sección 3.

[272] CEDPD, *Choosing the best candidate as your Data Protection Officer (DPD) – Practical guidelines for organisations* (véase nota 239, más arriba), p. 2.

[273] WP29 Guidelines on DPDs (véase nota 209, más arriba), p. 14.

participación en foros de privacidad, talleres, etc.

La agencia **francesa** de protección de datos, la CNIL, proporciona una "**extranet**" especial útil para los DPD registrados, a la que solo tienen acceso un nombre de usuario y una contraseña, que les proporciona textos legales (leyes, decretos, etc.) y capacitación e información, incluidos información sobre los informes o la guía de NUEVO emitidos por la CNIL, y sobre otros desarrollos legales y prácticos, y les permite intercambiar opiniones y mantener discusiones.[274]

Experiencia

Las Directrices GT29 sobre DPD no abordan la cuestión de qué (la duración de) la experiencia debe tener un DPD. Sin embargo, la Red de DPD institucionales de la UE recomienda que dichos DPD tengan la siguiente experiencia / madurez:[275]

> al menos 3 años de experiencia relevante [ver más abajo] para servir como DPD en un cuerpo donde la protección de datos no está relacionada con el negocio principal [ídem] (y, por lo tanto, las actividades de procesado de datos personales son principalmente administrativas); y
>
> al menos 7 años de experiencia relevante para desempeñarse como DPD en una institución de la UE o en aquellos organismos de la UE donde la protección de datos está relacionada con la actividad principal o que tienen un volumen importante de operaciones de tratamiento de datos personales.

Añaden en una nota de pie de página:

> La experiencia relevante incluye la experiencia en la implementación de los requisitos de protección de datos y la experiencia dentro de la institución / organización designada, lo que resulta en el conocimiento de cómo funciona. A falta de los años de experiencia especificados, la institución / organismo designado debe estar preparado para que el DPD tenga más tiempo disponible para la capacitación y para el trabajo en tareas de protección de datos.

Sobre la cuestión de si el procesado de datos personales "está relacionado con el negocio principal" de la organización en cuestión, la guía GT29 sobre el significado de la frase similar en el RGPD ("actividades principales del controlador o procesador") es relevante:[276]

> Las "actividades principales" pueden considerarse como las operaciones clave necesarias para lograr los objetivos del controlador o del procesador.

La frase "experiencia relevante" no debe leerse como experiencia específica como DPD, podría ser experiencia en la redacción e implementación de políticas en la organización relevante (o una organización similar), o en áreas relevantes como TI, desarrollo de productos, basta con tener en cuenta que la publicación no debe asignarse a una persona relativamente joven e inexperta, o una persona que no esté familiarizada con la organización particular (tipo de) en cuestión.

Características y cualidades personales

El SEPD, los DPD institucionales de la UE y el CEDPD señalan acertadamente que un DPD debe tener cualidades personales especiales. El o ella se encuentra en una posición delicada: deben estar dispuestos a decir "no" a sus jefes en casos excepcionales, pero más a menudo son capaces de ayudar a encontrar una solución a los problemas que sea aceptable para la organización y que cumpla con la ley. (y en todo caso, mejora de la privacidad). Como lo indican las Directrices GT29:[277]

---

[274] CNIL, Guide Pratique Correspondant (véase nota 249, más arriba), Sección 4.
[275] Red de Delegados de Protección de Datos de las Instituciones y los Organismos de la UE, *Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001* (véase nota 244, más arriba), p. 4.
[276] *WP29 Guidelines on DPDs* (véase nota 242, más arriba), p. 6.
[277] *WP29 Guidelines on DPDs* (véase nota 242, más arriba), p. 11.

> Las cualidades personales deben incluir, por ejemplo, integridad y alta ética profesional; la principal preocupación del DPD debería ser permitir el cumplimiento del RGPD. El DPD desempeña un papel clave en el fomento de una cultura de protección de datos dentro de la organización y ayuda a implementar elementos esenciales del RGPD.

Los DPD institucionales de la UE subrayan la necesidad de las siguientes habilidades "personales" e "interpersonales".[278]

> Habilidades personales: integridad, iniciativa, organización, perseverancia, discreción, capacidad para hacer valer en circunstancias difíciles, interés en la protección de datos y motivación para ser un DPD.
>
> Habilidades interpersonales: comunicación, negociación, resolución de conflictos, capacidad para construir relaciones de trabajo.

En otra parte, indican:[279]

> El desempeño adecuado de las tareas de la DPD a menudo requiere que la DPD adopte una actitud firme e insistente también con los controladores que tienen una alta posición en la organización, lo que puede percibirse, en el mejor de los casos, como burocratización o, en el peor, desagradable "problema". Por lo tanto, el DPD debe ser capaz de soportar las presiones y dificultades que acompañan a esta importante posición.

El CEDPD añade:[280]

> El DPD tiene que enfrentarse a varios desafíos y con diferentes intereses en juego. Es por eso por lo que el DPD también debe mostrar fuertes habilidades de comunicación combinadas con una diplomacia refinada. Un DPD no es (y no debe ser) un "activista de privacidad": con el apoyo de los otros líderes de la organización, debe desempeñar un papel de habilitador de negocios responsable y ayudar a la organización a incluir la privacidad en el negocio. - Decisiones de procesos, no solo para detectar y prevenir riesgos sino también para crear valor. Además, el RGPD requiere que su línea de informes se encuentre en el nivel más alto de la administración y que su independencia esté asegurada. Esto requiere "seriedad" y habilidades de liderazgo también.

Independencia

Ya hemos reseñado que "[el] delegado de protección de datos puede ser un miembro del personal del controlador o procesador, o cumplir las tareas sobre la base de un contrato de servicio" (Art. 37 (6)). Sin embargo, en ninguno de los casos se trata de una posición de empleado o contratista ordinario. En particular, el Reglamento subraya que:

> Dichos oficiales de protección de datos, sean o no empleados del responsable, deben estar en condiciones de realizar sus tareas y tareas de manera **independiente**. (Considerando 97)

Más específicamente, el Reglamento estipula:

> El controlador y el procesador se asegurarán de que el **delegado de protección de datos no reciba ninguna instrucción con respecto al ejercicio de esas tareas. Él o ella no serán**

---

[278] Red de Delegados de Protección de Datos de las Instituciones y los Organismos de la UE, *Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001* (véase nota 244, más arriba), p. 4.

[279] Ídem, p. 6. La Red prepara recomendaciones para aliviar estas presiones en el contexto de este debate. La Red realiza recomendaciones para aliviar estas presiones en el contexto de su debate sobre la posición a otorgar al DPD en la organización, tal y como se analiza bajo el título "Posición del DPD dentro de la organización", más abajo.

[280] CEDPD, Elección del mejor candidato para su Delegado de Protección de Datos – Guía práctica para la organización (véase nota 239, más arriba), p. 3 (con edición y cambios ligeros)

> **despedidos ni penalizados por el controlador o el procesador por realizar sus tareas**. El delegado de protección de datos deberá **reportar directamente al nivel de administración más alto del controlador** o del procesador.
>
> (Artículo 38(3))

El GT29 lo aclara de la siguiente manera:[281]

> [Las estipulaciones anteriores] significan [] que, al cumplir con sus tareas bajo el Artículo 39, los DPD no deben recibir instrucciones sobre cómo tratar un asunto, por ejemplo, qué resultados deben lograrse, cómo investigar una queja o si deben y consultar a la autoridad de supervisión. Además, no se les debe dar instrucciones para tener una cierta visión de un tema relacionado con la ley de protección de datos, por ejemplo, una interpretación particular de la ley.
>
> Sin embargo, la autonomía de los DPD no significa que tengan poderes de decisión que se extiendan más allá de sus tareas de conformidad con el Artículo 39.
>
> El controlador o procesador sigue siendo responsable del cumplimiento de la ley de protección de datos y debe poder demostrar el cumplimiento. Si el controlador o procesador toma decisiones que son incompatibles con el RGPD y el consejo del DPD, se le debe dar al DPD la posibilidad de hacer patente su posición disidente más allá de sus tareas según el Artículo 39.

Como se señala más adelante en la Parte 3, el consejo del DPD, y cualquier acción tomada en contra de dicho consejo, debe registrarse, y cualquier omisión del consejo puede realizarse contra el controlador o el procesador en cualquier investigación posterior por parte de la autoridad de protección de datos correspondiente. (Como se señaló anteriormente, a la inversa, el hecho de que un controlador o procesador actuó de acuerdo con cualquier consejo o guía emitida por su DPD puede constituir un "elemento" para demostrar el cumplimiento con el RGPD (Considerando 77).[282]

El GT29 también aclara el alcance de la estipulación de que los DPD "no deben ser descartados ni penalizados por el controlador o el procesador por realizar [sus] tareas":[283]

> Este requisito también fortalece la autonomía de los DPD y ayuda a garantizar que actúen de manera independiente y disfruten de suficiente protección al realizar sus tareas de protección de datos.
>
> Las sanciones solo están prohibidas por el RGPD si se imponen como resultado de que el DPD desempeñe sus funciones como DPD. Por ejemplo, un DPD puede considerar que un tratamiento particular puede resultar en un alto riesgo y aconsejar al controlador o al procesador que realice una evaluación de impacto de protección de datos, pero el controlador o el procesador no están de acuerdo con la evaluación del DPD. En tal situación, el DPD no puede ser despedido por proporcionar este consejo.
>
> Las sanciones pueden adoptar diversas formas y pueden ser directas o indirectas. Podrían consistir, por ejemplo, en ausencia o retraso de promoción; prevención de la promoción profesional; Negación de beneficios que otros empleados reciben. No es necesario que estas sanciones se lleven a cabo, una simple amenaza es suficiente siempre que se utilicen para penalizar al DPD por motivos relacionados con sus actividades de DPD.
>
> Como una regla de gestión normal y como sería el caso para cualquier otro empleado o contratista, y sujeto a, el contrato nacional aplicable o la legislación laboral y penal, un DPD

[281] *WP29 Guidelines on DPDs* (véase nota 242, más arriba), Sección 3.3, pp. 14 – 15.
[282] Véase Sección 2.2.2, véase más arriba.
[283] *WP29 Guidelines on DPDs* (véase nota 242, más arriba), Sección 3.4, p. 15.

> aún podría ser despedido legítimamente por razones distintas a la ejecución de sus tareas como DPD (por ejemplo, en caso de robo, acoso físico, psicológico o sexual o falta grave de conducta similar).
>
> En este contexto, se debe tener en cuenta que el RGPD no especifica cómo y cuándo un DPD puede ser despedido o reemplazado por otra persona. Sin embargo, cuanto más estable sea el contrato de un DPD y existan más garantías contra el despido improcedente, más probable será que puedan actuar de manera independiente. Por lo tanto, el GT29 agradecería los esfuerzos de las organizaciones en este sentido.

Como mínimo, cualquier contrato de trabajo ofrecido a un DPD debe incluir cláusulas que repitan las estipulaciones sobre independencia en el RGPD, o referencias cruzadas a esas. Por supuesto, los tribunales o tribunales que juzguen en casos de despido deben tener plenamente en cuenta las disposiciones del RGPD. Cuando sea necesario, puede ser útil modificar las leyes laborales a tal efecto. Los Estados miembros también podrían apuntalar la independencia de los DPD en otras leyes nacionales: se pueden encontrar ejemplos de salvaguardas contra el despido de cierto personal en las leyes que proporcionan protecciones especiales para, por ejemplo, dirigentes sindicales, y / o que requieren la aprobación de los consejos de trabajadores para nombramientos y despido de determinados puestos.

NB: Los DPD institucionales de la UE discuten los temas de independencia y conflictos de interés (el próximo número tratado en este Manual) principalmente en términos de contrato, duración del nombramiento y otras salvaguardas, como se discute más adelante, bajo el título "Posición del DPD dentro de la organización", a continuación. CEDPD simplemente señala que la organización que designa al DPD debe "considerar... cómo garantizar la independencia del DPD".[284]

Conflictos de intereses

Como señala el GT29:[285]

> El Artículo 38(6) permite a los DPD "cumplir con otras tareas y deberes". Sin embargo, se requiere que la organización se asegure de que "cualquiera de esas tareas y deberes no den lugar a un conflicto de intereses".
> La ausencia de conflicto de intereses está estrechamente relacionada con el requisito de actuar de manera independiente. Aunque a los DPD se les permite tener otras funciones, solo se les pueden encomendar otras tareas y deberes siempre que no den lugar a conflictos de intereses. Esto implica, en particular, que el DPD no puede ocupar un puesto dentro de la organización que lo lleve a determinar los propósitos y los medios del tratamiento de datos personales. Debido a la estructura organizativa específica de cada organización, esto debe considerarse caso por caso.
> Como regla general, los puestos en conflicto pueden incluir cargos de alta gerencia (como director ejecutivo, jefe de operaciones, jefe de finanzas, director médico, jefe de departamento de marketing, jefe de recursos humanos o jefe de departamentos de TI), pero también otros roles inferiores en la estructura organizativa si tales posiciones o roles conducen a la determinación de propósitos y medios de tratamiento.
> Dependiendo de las actividades, el tamaño y la estructura de la organización, puede ser una buena práctica para los controladores o procesadores:
> - Identificar las posiciones que serían incompatibles con la función de DPD
> - Elaborar normas internas al efecto para evitar conflictos de intereses.
> - Incluir una explicación más general sobre conflictos de intereses.
> - Declarar que su DPD no tiene conflicto de intereses con respecto a su función como DPD, como una forma de concienciar sobre este requisito.
> - incluir salvaguardas en las reglas internas de la organización y garantizar que el aviso de

[284] CEDPD, Elección del mejor candidato para su Delegado de Protección de Datos – Guía práctica para la organización (véase nota 239, más arriba), p. 3.
[285] *WP29 Guidelines on DPDs* (véase nota 242, más arriba), Sección 3.5, pp. 15 – 16. El tercer párrafo ("Como regla de oro...") aparece como una nota en el documento, en lugar de en el texto principal, como se hace aquí.

> vacante para el puesto de DPD o el contrato de servicio sea lo suficientemente preciso y detallado para evitar un conflicto de intereses. En este contexto, también se debe tener en cuenta que los conflictos de intereses pueden tomar varios de los Estados miembros dependiendo de si el DPD se contrata interna o externamente.

Los DPD institucionales de la UE añaden:[286]

> [El] DPD no debe tener conflictos de interés entre los deberes de DPD y cualquier otro deber oficial, en particular en relación con la aplicación de las disposiciones del Reglamento (Art. 24.3). Un conflicto de intereses está presente cuando las demás tareas que se le solicitan a un DPD pueden tener intereses directamente adversos, a los de la protección de datos personales dentro de su institución. Si es necesario, el DPD debe plantear este asunto ante su autoridad de nombramiento.

Abordan el tema con más detalle en términos de contrato, duración del nombramiento y otras garantías, como se indica en el siguiente encabezado. El CEDPD nuevamente simplemente señala que, si la cita del DPD no es un trabajo de tiempo completo, la organización que lo designe debe "considerar... cómo tratar [con] el conflicto de intereses".[287]

Posición del DPD dentro de la organización

La posición jerárquica y contractual del DPD dentro de una organización es crucial para garantizar la efectividad, independencia y evitar conflictos de intereses del DPD.

Por un lado, como se señaló anteriormente, el DPD debe estar "próximo" a la organización a la que presta servicio (véase más arriba, bajo el título "Experiencia requerida"). Además, como indica el CEDPD:[288]

> Para que un DPD sea efectivo, [él o ella] debe estar en el terreno, no solo a disposición de varios interesados dentro de su organización, sino que también busca oportunidades para interactuar con diferentes departamentos de manera proactiva.

Esto puede ser problemático en casos de DPD externos que actúan bajo un contrato de servicio: por definición, no formarán parte del organismo al que asisten. En el sector privado, puede haber, y en algunos países, como Alemania, sin duda hay, DPD externos con amplia experiencia en el sector privado o subsector en el que trabajan. En el sector público, esto puede ser más difícil (como se sugiere en la Sección 2.3.2, más arriba, bajo los encabezados "*DPD para grandes autoridades públicas o grupos de autoridades*" y "*DPD externos*").

Pero siempre existe una tensión entre, por un lado, la necesaria "proximidad" del DPD a su organización y, por otro lado, la necesidad de evitar conflictos de intereses y garantizar la independencia real del DPD en la práctica.

Como ya se señaló, en la opinión del GT29, esto significa que un DPD no puede participar en la determinación de los propósitos y los medios del tratamiento de datos personales, y no puede ocupar un cargo de alta gerencia como jefe ejecutivo o jefe de un departamento principal.[289]

---

[286] Red de Delegados de Protección de Datos de las Instituciones y los Organismos de la UE (CEDPO), *Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001* (véase nota 244, más arriba), p. 15.

[287] CEDPD, Elección del mejor candidato para su Delegado de Protección de Datos – Guía práctica para la organización (véase nota 239, más arriba), p. 3.

[288] Ídem, p. 2.

[289] Véase más arriba, bajo el encabezado *"Conflictos de interés",* en particular el tercer párrafo de la cita de la Guía WP29 sobre DPD. Por el contrario, la autoridad italiana de protección de datos, el *Garante*, en sus preguntas frecuentes sobre DPD, dice que:
… El Artículo 38 (3) dispone que el DPD 'deberá informar directamente al más alto nivel de gestión del controlador o procesador.' Este requisito de informe directo puede garantizar, en particular, que la alta dirección esté informada de las directrices y recomendaciones proporcionadas por el DPD, actuar en su capacidad de asesoramiento y / o sensibilización con respecto al controlador o procesador de datos
En consecuencia, si se designa un DPD interno, sería preferible, en principio, que se seleccione un jefe de departamento o un miembro principal del personal siempre que sea posible en función de la estructura organizativa y teniendo en cuenta la complejidad de las actividades de tratamiento. De esa manera, el DPD designado estará en condiciones de cumplir con sus tareas de forma totalmente autónoma e independiente, así como mediante el enlace directo con los niveles superiores de administración.

El problema se aborda con mucho más detalle en los DPD institucionales de la UE. Aunque, por supuesto, sus puntos de vista deben verse a la luz de su contexto específico, todavía es útil señalarlos. Habiendo notado varias disposiciones en el reglamento que las cubre (Reglamento (EC) 45/2001)[290] que están diseñadas para garantizar su independencia, continúan de la siguiente manera:[291]

> En la práctica, sin embargo, puede ser difícil para el DPD ejercer sus funciones con total independencia. No hace falta decir que la situación individual y la personalidad del DPD desempeñarán un papel, pero en general se puede suponer que ciertos elementos pueden tender a debilitar la posición de un DPD:
>
> - Un DPD a tiempo parcial enfrenta un conflicto permanente entre la asignación de tiempo y esfuerzos a sus tareas DPD frente a otras tareas. Con respecto al desarrollo de la carrera y la revisión del desempeño, la gerencia puede dar mayor importancia a las actividades que no son DPD. Esto crea presión en el DPD para concentrar sus esfuerzos en las tareas que no son DPD. Un DPD a tiempo parcial también está en peligro de encontrar conflictos de interés.
> - El DPD con un contrato limitado probablemente estaría en una posición más débil para realizar sus tareas de DPD vigorosamente que uno con un contrato permanente (oficial o agente temporal con contrato de duración indefinida). Esto se debe a que él / ella puede estar preocupado por cómo sus acciones podrían influir negativamente en el reporte de su contrato. Un DPD que es muy joven y tiene una experiencia laboral limitada puede tener dificultades para enfrentarse a los controladores y puede estar más centrado en su propio desarrollo profesional que en el desempeño vigoroso de los deberes del DPD.
> - Un DPD que informa y es revisado por un superior directo en la jerarquía (director o jefe de unidad) puede sentirse presionado para cooperar y llevarse bien con la administración y otros colegas, ya que el desempeño vigoroso de los deberes del DPD puede tener un efecto negativo. Impacto en la carrera. ... Para aliviar esta presión, el DPD debe informar y ser revisado por el jefe administrativo de la institución u organismo. Esto es particularmente importante para los DPD a tiempo parcial, que deben informar directamente y ser revisados por la autoridad de nombramiento para sus deberes de DPD, y para / por el superior normal en la jerarquía para otros deberes.
> - Un DPD que debe solicitar personal y recursos (recursos de TI, presupuesto para viajes de negocios y capacitación) de su superior directo puede enfrentar dificultades si este último no está totalmente comprometido con el cumplimiento de la protección de datos. Esto se puede evitar si el DPD tiene su propia responsabilidad presupuestaria, y al tener cualquier solicitud de recursos adicionales sujeto a la aprobación de la autoridad que le nombra.

Las mejores prácticas para ayudar a asegurar la independencia del DPD son:

> - La institución u organismo debe establecer el puesto de DPD dentro de la organización como asesor, jefe de unidad o director y, en cualquier caso, el puesto de DPD debe ser oficialmente reconocido como nivel de gestión, en el organigrama oficial de la institución / organismo;
> - La institución u organismo debe designar al DPD para el mayor plazo posible, a la luz del contrato del DPD. Por lo tanto, un contrato de cinco años debería ser la norma, a menos que no sea posible en virtud de las roturas de circuito;
> - El DPD debe tener un contrato permanente / indeterminado con la institución u organismo [y] debe tener suficiente experiencia (...);
> - El DPD debe poder dedicar su tiempo por completo a sus funciones de DPD, especialmente para instituciones y organismos grandes, y para los más pequeños en la fase inicial de establecer un régimen de protección de datos. Debe proporcionarse el

---

(Garante, FAQs on DPDs [véase nota 249, más arriba], Sección 2.)
Quizás la mejor manera de conciliar los puntos de vista del WP29 y el Garante a este respecto, sería sugerir que el DPD debería ser nombrado a nivel de jefe de departamento o gerente senior, pero sin ser realmente responsable de las operaciones de tratamiento de datos.

[290] Véase nota 148, véase más arriba.

[291] Red de Delegados de Protección de Datos de las Instituciones y los Organismos de la UE, *Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001* (nota 244, véase más arriba), pp. 6 – 7.

apoyo adecuado en términos de recursos e infraestructura. Los deberes no DPD de un DPD a tiempo parcial no deben presentar un conflicto de intereses, ni siquiera la apariencia de un conflicto, con los deberes del DPD;

- Los DPD en organizaciones donde las actividades de tratamiento de datos son el negocio central de la organización normalmente requerirán varios miembros del personal. Dicha capacidad del personal debe ser asegurada;
- Deben establecerse reglas dentro de la organización que garanticen la obligación de todos los miembros del personal de cooperar con el DPD sin tener que esperar una orden o permiso de su superior;
- El DPD debe informar al jefe de la institución u organismo, quien debe ser responsable de la revisión del desempeño del DPD de sus funciones, según lo establecido por el Reglamento. La persona responsable de la revisión de desempeño del DPD debe ser sensible a la necesidad de que el DPD tome posiciones sólidas que otros en la organización no puedan apreciar. El DPD no debe sufrir ningún perjuicio por el desempeño de sus funciones. La autoridad nominadora debe garantizar que durante el mandato del DPD, él / ella tenga al menos un progreso "normal" de carrera. Al revisar el desempeño del DPD, el evaluador no debe reprender al DPD por tomar posiciones impopulares ni considerar los requisitos de protección de datos como una carga administrativa. Para un DPD a tiempo parcial, el desempeño en los deberes del DPD debe tener la misma ponderación que el desempeño en los deberes que no son del DPD...;
- El DPD debe tener su propia línea presupuestaria, establecida de acuerdo con las normas y procedimientos relevantes de la institución / entidad respectiva; sus solicitudes de recursos adicionales deben estar sujetas a la aprobación del jefe administrativo. Otros arreglos son aceptables si le brindan al DPD los recursos que necesita para realizar su misión de manera independiente...;
- El DPD debe tener poder de firma para la correspondencia relacionada con la protección de datos.

Las autoridades públicas de los Estados miembros, y las autoridades de protección de datos, si se les pide que asesoren sobre el tema, deben tener en cuenta lo anterior al decidir cómo, dónde y con arreglo a qué acuerdos formales o contratos para designar a los DPD, o al asesorar sobre esos asuntos. Las APD pueden sentir que es apropiado emitir una guía detallada al respecto, en las líneas anteriores.

Recursos e instalaciones

El RGPD estipula que:

> El controlador y el procesador apoyarán al oficial de protección de datos en la realización de las tareas a las que se hace referencia en el Artículo 39 [como se indica en la Sección 2.3.4, debajo de ese encabezado], proporcionando los **recursos necesarios para llevar a cabo esas tareas** y el acceso a los datos personales y el procesado de operaciones, y para mantener su conocimiento experto.
>
> (Artículo 38 (2))

En ese sentido, el GT29 recomienda lo siguiente en particular:[292]

> • Apoyo activo de la función del DPD por parte de la alta gerencia (como a nivel de la junta directiva).
> • Tiempo suficiente para que los DPD cumplan con sus obligaciones. Esto es particularmente importante cuando el DPD se designa a tiempo parcial o cuando el empleado lleva a cabo la protección de datos además de otras tareas. De lo contrario, las prioridades en conflicto podrían dar lugar a que se descuiden los deberes del DPD. Tener tiempo suficiente para dedicarse a las tareas de DPD es primordial. Es una buena práctica establecer un porcentaje de tiempo para la función DPD donde no se realiza a tiempo

[292] *WP29 Guidelines on DPDs* (nota 13, véase más arriba), Sección 3.2, pp. 13 – 14

completo. También es una buena práctica determinar el tiempo necesario para llevar a cabo la función, el nivel apropiado de prioridad para los deberes del DPD y para que el DPD (o la organización) elabore un plan de trabajo.
• Apoyo adecuado en términos de recursos financieros, infraestructura (locales, instalaciones, equipos) y personal, según corresponda.
• Comunicación oficial de la designación del DPD a todo el personal para asegurar que su existencia y función sea conocida dentro de la organización.
• Acceso necesario a otros servicios, como Recursos Humanos, legal, TI, seguridad, etc., para que los DPD puedan recibir apoyo, aportaciones e información esenciales de esos otros servicios.
• Formación continúa. [Ver arriba, bajo el título "Formación formal y certificaciones"]
• Dado el tamaño y la estructura de la organización, puede ser necesario configurar un equipo de DPD (un DPD y su personal). En tales casos, la estructura interna del equipo y las tareas y responsabilidades de cada uno de sus miembros deben estar claramente definidas. De manera similar, cuando la función del DPD es ejercida por un proveedor de servicios externo, un equipo de personas que trabajan para esa entidad puede llevar a cabo efectivamente las tareas de un DPD como equipo, bajo la responsabilidad de un contacto principal designado para el cliente.

En general, cuanto más complejas y sensibles sean las operaciones de tratamiento, más recursos se le deben dar al DPD. La función de protección de datos debe ser eficaz y contar con recursos suficientes en relación con el tratamiento de datos que se lleva a cabo.

Como ya se señaló, los DPD institucionales de la UE consideran que "un DPD que debe solicitar personal y recursos (recursos de TI, presupuesto para viajes de negocios y capacitación) de su superior directo podría enfrentar dificultades si este último no está totalmente comprometido con el logro del cumplimiento de la protección de datos". Por lo tanto, recomiendan que se le otorgue a la DPD su propia responsabilidad presupuestaria, con cualquier solicitud de recursos adicionales sujeta a la aprobación de la autoridad nominadora (en lugar de a un superior directo).[293]

La CEDPD señala:

> [En] organizaciones complejas, deberá pensar si el DPD será asistido o no por otras personas internamente que complementarán sus habilidades, de forma permanente (el equipo del DPD) o según sea necesario, según sea el caso, un consejero externo.

En las autoridades públicas,la creación de un equipo sería realmente aconsejable. En los organismos públicos pequeños, esto podría consistir simplemente en que el personal existente se reúna regularmente con el DPD para discutir asuntos relevantes y preparar políticas. En los más grandes, a algunos se les puede asignar más formalmente funciones de apoyo de DPD a tiempo parcial. En algunos, puede ser necesario nombrar a tiempo completo para apoyar el DPD. Como todos los documentos de orientación dejan claro, las decisiones sobre estos asuntos deben tomarse a la luz de (i) la complejidad o sensibilidad de las operaciones de tratamiento de datos personales y (ii) el tamaño y los recursos de la entidad en cuestión. Pero al final, es un requisito legal del RGPD que los recursos asignados al DPD (y al equipo) sean adecuados para las tareas en cuestión.

Poderes del DPD

Aparte de los recursos, y una posición suficientemente fuerte, protegida y de alto nivel dentro de la organización, el DPD también necesita tener el poder para llevar a cabo su tarea. El Artículo 38 (2) (citado en el encabezado anterior) aclara que, para ese fin, la entidad que designe al DPD debe garantizar que él o ella tendrá "acceso" a los datos personales y las operaciones de tratamiento. Esto debe leerse de la misma manera que la disposición correspondiente en el reglamento que cubre los DPD institucionales de la UE. El artículo 24(6) del Reglamento (CE) 45/2001, es leído por esos DPD de la siguiente manera:[294]

---

[293] Véase véase más arriba, bajo el título "Posición del DPD dentro de la organización"

[294] Red de Delegados de Protección de Datos de las Instituciones y los Organismos de la UE, *Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001* (nota 244, véase más arriba), pp. 12. Nótese que, a diferencia del art. 38 (2) RGPD, artículo 24(6) del Reglamento (CE) 45/2001, de hecho, no menciona expresamente el acceso a los datos

> El Reglamento exige que los controladores ayuden a la DPD a cumplir con sus obligaciones y que proporcionen información en respuesta a las preguntas, y establece que la DPD tendrá acceso en todo momento a los datos que constituyen el objeto de las operaciones de tratamiento y a todas las oficinas. Tratamiento de instalaciones y soportes de datos.
>
> Si bien el DPD no tiene poder de ejecución respecto de los controladores, él / ella está facultado para monitorear el cumplimiento mediante la recopilación de todos los datos relevantes, que la institución / cuerpo nominador y sus controladores están obligados a poner a disposición.

Otros comentarios de los DPD institucionales de la UE en relación con el deber del DPD de garantizar el cumplimiento de las normas de protección de datos también son relevantes.[295]

> Se pueden desarrollar herramientas de TI para ayudar al DPD a realizar un monitoreo regular. También se pueden hacer arreglos administrativos, como asegurar que el DPD reciba una copia de todos los problemas de protección de datos que surjan, y que se consulte al DPD sobre los documentos que plantean problemas de protección de datos. El seguimiento cuidadoso y regular del cumplimiento y el informe de los resultados puede crear una fuerte presión sobre los controladores para garantizar que sus operaciones de tratamiento sean compatibles. El monitoreo y los informes regulares son, por lo tanto, las herramientas más sólidas del DPD para garantizar el cumplimiento. Para este fin, una encuesta / informe anual emitido a la gerencia... es una buena práctica.

Surgen problemas especiales cuando un controlador o procesador se niega a seguir los consejos de su DPD. En palabras del GT29:[296]

> Si el controlador o procesador toma decisiones que son incompatibles con el RGPD y el consejo del DPD, se le debe dar al DPD la posibilidad de dejar clara su opinión disidente al más alto nivel de gestión y a los que toman las decisiones. A este respecto, el Artículo 38 (3) dispone que la DPD "informará directamente al nivel de gestión más alto del controlador o del procesador". Dicha información directa garantiza que la alta gerencia (por ejemplo, la junta directiva) esté al tanto del consejo y las recomendaciones del DPD como parte de la misión del DPD de informar y asesorar al controlador o al procesador. Otro ejemplo de información directa es la redacción de un informe anual de las actividades del DPD proporcionadas al más alto nivel de gestión.

Aunque no existe un deber específico establecido en el RGPD para que el DPD informe el incumplimiento de la ley a las autoridades, el RGPD estipula que es una de las tareas del DPD es

> actuar como punto de contacto para la autoridad de supervisión en asuntos relacionados con el procesado, ... y consultar, cuando corresponda, con respecto a cualquier otro asunto (Art. 39 (1) (e), énfasis añadido)

En los casos en que un DPD siente que su empleador está actuando en violación de la ley, el DPD ciertamente tiene el poder (y, de hecho, argumentaríamos, el deber) de plantear el problema ante el APD nacional, para resolver el asunto. Esto ilustra la delicadeza de la posición.

Al mismo tiempo, como el GT29 enfatiza correctamente:[297]

---

personales y las operaciones de procesado de datos personales. Por lo tanto, en este último contexto, léase la estipulación más general sobre la provisión de los recursos necesarios. Esto está presumiblemente influido por la disposición más específica y fuerte sobre el acceso a dicha información (dentro de las instituciones de la UE) al SEPD.

[295] *Idem.*

[296] *WP29 Guidelines on DPDs* (nota 242, véase más arriba), p. 15. El mismo enfoque es adoptado por la Red de DPDs institucionales de la UE, Véase de nuevo *Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001* (nota 13, más arriba), pp. 12 (Véase el párrafo siguiente al citado en el texto, véase más arriba).

[297] *W29P Guidelines on DPDs,* (nota 242, más arriba) p. 15, con referencia al principio de "responsabilidad" en el Art. 5(2) RGPD.

> Sin embargo, la autonomía de los DPD no significa que tengan poderes de decisión que se extiendan más allá de sus tareas de conformidad con el Artículo 39.
>
> El controlador o procesador sigue siendo responsable del cumplimiento de la ley de protección de datos y debe poder demostrar el cumplimiento.

Formalidades

Todos los requisitos anteriores, etc., del DPD deben estar claramente reflejados en el documento legal por el cual él o ella son designados. Como autoridad de protección de datos italiana, Garante del Privacy, lo coloca en sus preguntas frecuentes sobre DPD:[298]

> El Artículo 37 (1) del RGPD establece que un controlador de datos o un procesador de datos designarán un DPD. En consecuencia, la existencia de un instrumento que designe el DPD es una parte integral de cualquier acuerdo para cumplir con la obligación relevante.
>
> Si el candidato a DPD es miembro del personal, se deberá producir un instrumento ad hoc que lo designe como DPD. A la inversa, si se selecciona una entidad externa, la designación formal de esa entidad como DPD será una parte integral del acuerdo de servicio ad-hoc que se redactará de conformidad con el Artículo 37 del RGPD (...).
>
> Independientemente de la naturaleza y el tipo de instrumento legal, este último debe especificar de manera inequívoca quién será el DPD al mencionar su nombre, las tareas comprometidas (que también pueden ir más allá de las previstas en el Artículo 39 del RGPD) y los deberes relacionados para el soporte, se espera que el DPD proporcione al controlador de datos / procesador de datos de conformidad con el marco legal y normativo aplicable.
>
> Si se comprometen tareas adicionales al DPD además de las mencionadas inicialmente en el instrumento de designación, este último o el contrato de servicio tendrá que ser enmendado y / o complementado en consecuencia.
>
> El instrumento de designación y / o el acuerdo de servicio también deben especificar, de manera concisa, los motivos por los cuales el organismo o autoridad pública ha designado a la persona física determinada como DPD para que cumpla con los requisitos del Artículo 37 (5) del RGPD se puede establecer; con ese fin, se puede hacer referencia al resultado del procedimiento de selección interno o externo. La especificación de los criterios aplicados antes de designar a un determinado candidato no solo es una indicación de transparencia y buena administración, sino también un elemento que debe tenerse en cuenta al evaluar el cumplimiento del principio de "responsabilidad".
>
> Una vez designado el DPD, el controlador de datos o el procesador deben incluir los datos de contacto del DPD en la información proporcionada a los interesados y también publicar esos datos en los sitios web relevantes; la comunicación de los datos a Garante también se requiere en virtud del Artículo 37 (7). En cuanto a la publicación en el sitio web, puede ser apropiado publicar los datos de contacto del DPD en la sección de "transparencia" o "apertura" del sitio, así como en la página de "privacidad", cuando esté disponible.
>
> Como se aclara en las Directrices [GT29], el nombre del DPD no tiene que publicarse de conformidad con el Artículo 37 (7); sin embargo, esto podría ser una buena práctica en el sector público. A la inversa, los datos de contacto deben proporcionarse a Garante para facilitar las interacciones(...)Por otro lado, los detalles de contacto de DPD deben comunicarse a los interesados en caso de una violación de seguridad (ver Artículo 33 (3)

[298] Garante, FAQs on DPDs (véase nota 249, más arriba), Sección 1. El Garante ha adjuntado un modelo de nombramiento [Nombramiento del DPD appointment] a las FAQs para mayor comodidad. También se adjunta un `Formulario para comunicar los datos del DPD al Garante´

b).

2.5.4 Funciones y Obligaciones del DPD (Resumen)

En relación con las DPD institucionales de la UE, el SEPD ha distinguido las siguientes siete funciones de DPD:[299]

- Función de información y sensibilización;
- Función de asesoramiento;
- Función organizacional;
- Función cooperativa;
- Monitorización de la función de cumplimiento;
- Gestión de consultas o quejas. y
- Función de cumplimiento.

Los DPD nombrados bajo el RGPD desempeñan funciones en gran medida similares. Se correlacionan con un rango de tareas más específicas, indicadas en el amplio artículo en términos amplios en el Artículo 39 del RGPD de la siguiente manera:

Artículo 39

Funciones y Obligaciones del DPD

1. El delegado de protección de datos tendrá al menos las siguientes funciones:

(a) informar y asesorar al controlador o al procesador y a los empleados que llevan a cabo el tratamiento de sus obligaciones de conformidad con el presente Reglamento y otras disposiciones de protección de datos de la Unión o los Estados miembros;

(b) controlar el cumplimiento del presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del controlador o procesador en relación con la protección de datos personales, incluida la asignación de responsabilidades, la sensibilización y la formación del personal involucrado en las operaciones de tratamiento, y las auditorías relacionadas;

(c) proporcionar asesoramiento cuando sea requerido con respecto a la evaluación de impacto de protección de datos y monitorear su desempeño de conformidad con el Artículo 35;

(d) cooperar con la autoridad de control;

(e) actuar como punto de contacto para la autoridad de supervisión en asuntos relacionados con el tratamiento, incluida la consulta previa mencionada en el Artículo 36, y consultar, cuando corresponda, con respecto a cualquier otro asunto.

2. El oficial de protección de datos deberá, en el desempeño de sus tareas, tener debidamente en cuenta el riesgo asociado con las operaciones de procesado, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del mismo.

En la práctica, los DPD también se encargarán de forma natural de determinadas tareas que se han encomendado formalmente a su responsable, puesto que la mayor parte de los responsables (salvo que cuenten con experiencia relevante y consolidada fuera del alcance del puesto de DPD, por ejemplo en el área legal o de cumplimiento) solicitarán la ayuda de su DPD para llevar a cabo dichas funciones. De hecho, por decirlo de una forma suave: en muchos casos, cuando los responsables se enfrentan a sus nuevas y difíciles funciones en virtud del RGPD (en particular las funciones de demostración de cumplimiento/ responsabilidad corporativa) delegarán en su DPD una gran parte del trabajo aunque, como indica claramente el RGPD en diferentes casos, el responsable tendrá responsabilidad plena ante la ley por cualquier fallo en ese sentido, y no el DPD.

[299] SEPD, *Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001* (véase nota 243, más arriba), pp. 6 – 7.

Concretamente, tal y como el Artículo 5 (2) del RGPD:

> El controlador será responsable de, y podrá demostrar el cumplimiento de, [los diversos requisitos del RGPD]

En otras palabras, esa responsabilidad no descansa sobre los hombros del DPD, como también se desprende del Artículo 39, citado anteriormente, que enfatiza las tareas de asesoramiento y apoyo del DPD.

Sin embargo, el DPD sigue siendo crucial en ese sentido, ya que debe, a través de sus consejos, hacer posible que la alta dirección y el personal disminuya las obligaciones relevantes. A la inversa, los gerentes superiores e inferiores tienen el deber de consultar al DPD si surgen problemas de cumplimiento del RGPD.

El SEPD ha proporcionado una matriz útil, denominada RACI ("Responsable, Aprueba, Consultado, Informado") a este respecto, aplicable en particular en relación con el mantenimiento de registros / el registro de operaciones de tratamiento de datos personales:[300]

	Responsable	Aprueba	Consultado	Informado
Alta dirección		X		
Propietario del negocio	X			
DPD			X	
Departamento TI			X	
Procesadores, cuando sean relevantes			X	

Añadió la siguiente aclaración de términos.:[301]

> '**Responsable**' significa tener la obligación de actuar y tomar decisiones para lograr los resultados requeridos; "**Aprueba**" significa ser responsable de las acciones, decisiones y desempeño; "**Consultado**" significa que se le pida que contribuya y proporcione comentarios; "**Informado**" significa mantenerse informado de las decisiones tomadas y del proceso.

El SEPD utiliza el término **"propietario de la empresa**" para la persona responsable, en la práctica, en términos cotidianos, para la actividad de tratamiento relevante: el "propietario" del proceso. Como se explica más adelante a continuación, bajo el encabezado *"Tarea preliminar",* formará parte de las primeras tareas del DPD para definir estas asignaciones internas de responsabilidades.

---

[300] SEPD, *Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments*, (Responsabilidad sobre el terreno Parte I: Registros, registros y cuándo realizar evaluaciones de impacto de protección de datos, febrero de 2018, p. 4 disponible en: https://SEPD.europa.eu/sites/edp/files/publication/18-02-06_accountability_on_the_ground_part_1_en_0.pdf
Se podría agregar a la columna de la izquierda, "titulares de datos" y "Autoridad de protección de datos", con una "X" para ellos en la última columna ("Informado"), pero los deberes relevantes son de hecho más complejos de lo que podría indicarse de esta manera: los titulares de los datos deben ser informados de ciertos asuntos en muchos casos (ya sea por el controlador motu proprio o bajo solicitud), pero no siempre de todo, y la APD no solo debe ser informada sino que debe ser consultada en algunos casos. En cualquier caso, la matriz tiene como objetivo aclarar los asuntos dentro de la organización del controlador, en lugar de en relación con entidades externas.

[301] Ídem, nota 7 (las negritas son nuestras)

De acuerdo con lo anterior, en la descripción general de las tareas de los DPD, a continuación, esas tareas a menudo se describirán como "ayudando al controlador a garantizar" varios asuntos, o como "asesorando al controlador" (o al "propietario de la empresa" / miembro del personal responsable) sobre cómo lograr ciertos fines, en lugar de "garantizar" esos asuntos o dictar cómo deben abordarse. En la práctica, especialmente en las organizaciones pequeñas, puede ser que el DPD lleve consigo gran parte de estas cargas, pero formalmente seguirá siendo responsabilidad del controlador (e internamente, del "propietario del negocio" / miembro del personal responsable).

De lo anterior, y teniendo en consideración esta salvedad de no responsabilidad del DPD, **deducimos quince tareas del DPD, o que en la práctica implicarán al DPD** (*más una tarea preliminar*), que se pueden agrupar en los siete encabezados de función identificados por el SEPD, tal como se indica al principio de la parte final de este manual, Parte Tres.

Estas funciones y tareas, a su vez, están ligadas y fuertemente vinculadas al "**principio de responsabilidad**" y la "demostración de deberes de cumplimiento" asociadas impuestas al controlador, discutidas anteriormente, en la Sección 2.4 de este manual, más arriba.

En la siguiente parte de este manual (Parte Tres), proporcionamos orientación sobre cómo deben realizar esas tareas el responsable y el DPD. Sin embargo, primero es importante reiterar que, aunque el DPD tendrá una gran influencia y aportes en relación con las tareas anteriores, no tiene ninguna responsabilidad personal formal para cumplir con el RGPD.

- o – O – o –

PARTE TRES

Guía práctica sobre las funciones del DPD o en las que, en la práctica, estará involucrado el DPD («Las funciones del DPD»)

El presente apartado del manual ofrece una guía práctica sobre **las funciones del DPD, o en las que, en la práctica, estará involucrado el DPD**, que ya se enumeraron en el apartado 2.5.4 anterior y aparecen, de nuevo, a continuación. A efectos de brevedad, nos referiremos a ellas, en cada momento, como «Las funciones del DPD». Tal y como se indica en ese apartado, las quince funciones surgen de la lista de funciones enumeradas en el artículo 39 del RGPD, que se agrupan en **las siete funciones del DPD**, que identifica el SEPD. En los diferentes apartados en que se aborda este asunto, ofrecemos **ejemplos** que los ilustran, relativos a prácticas reales.

Funciones del DPD:

Función preliminar:

Delimitar el alcance del entorno del responsable

Funciones organizativas:

Función 1: Crear un registro de operaciones de tratamiento de datos personales

Función 2: Revisar las operaciones de tratamiento de datos personales:

Función 3: Evaluar los riesgos que implican las operaciones de tratamiento de datos personales

Función 4: Gestionar operaciones que puedan dar lugar a un «alto riesgo»: llevar a cabo una Evaluación de Impacto de Protección de Datos (EIPD)

Supervisión de las funciones de cumplimiento normativo:

Función 5: Repetición de las Funciones 1 – 3 (y 4) de forma continua

Función 6: Gestionar violaciones de la seguridad de datos personales

Función 7: Función de investigación (incluyendo el tratamiento de denuncias internas)

Funciones consultivas:

Función 8: Función consultiva - general

Función 9: Respaldar y fomentar la «Protección de datos por diseño y defecto»

Función 10: Asesorar sobre y supervisar el cumplimiento normativo de las políticas de protección de datos, de los contratos de corresponsables del tratamiento, responsable-responsable y responsable-encargado, Normas corporativas vinculantes y cláusulas de transferencia de datos

Función 11: Participación en códigos de conducta y certificaciones

Cooperación con y consulta a la APD:

Función 12: Cooperación con la APD

Gestión de peticiones sobre protección de datos personales:

Función 13: Gestión de peticiones sobre protección de datos personales

Información y sensibilización:

Función 14: Funciones de información y sensibilización

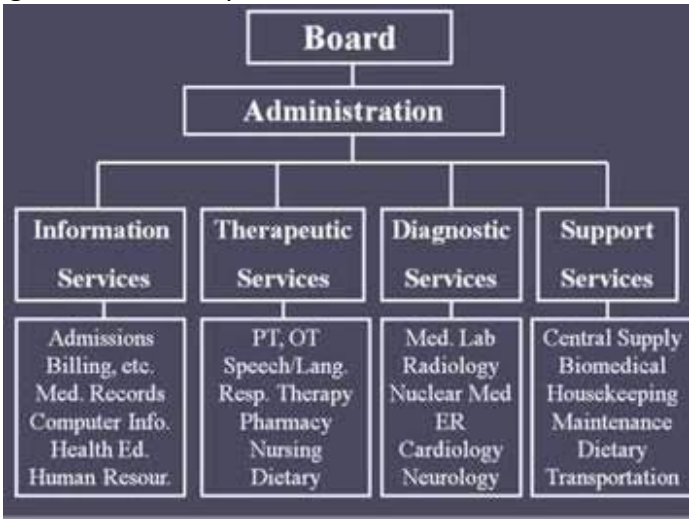
Función 15: Planificación y revisión de las actividades del RPD

Función preliminar:

Función preliminar del DPD: definir el alcance del entorno del responsable y preparar un mapa de las actividades de tratamiento de la organización en términos generales

Un DPD solo podrá llevar a cabo funciones relativas a su empleados si conoce completamente (i) la distribución **interna** y la asignación de funciones y responsabilidades relativas a (o que podrían implicar) un tratamiento de datos personales; (ii) los enlaces y acuerdos **externos** de dicha organización con otras organizaciones; y (iii) el/los marco(s) **legal(es)** de aquellos.
Antes de realizar sus otras funciones principales – salvo preparar el inventario inicial (registro) de las operaciones de tratamiento de datos personales, que se enumeran en primer lugar en el siguiente apartado (Función 1) que pueda realizarse en paralelo – el DPD deberá mapear dichos enlaces internos y externos y líneas de responsabilidad en relación con todas las operaciones de tratamiento de datos personales, y ponerlos en el contexto amplio de su función y objetivos en la organización, y familiarizarse con las normas correspondientes de forma rigurosa.
Para aclarar las estructuras y funciones **internas**, el DPD deberá, en primer lugar, obtener y estudiar el **organigrama** de su organización, que le proporcione la dirección.

EJEMPLO Organigrama de un hospital



Fuente: *Principles of Health Science*, https://www.youtube.com/watch?v=FpQEwbAV3Qw

No obstante, los organigramas identificarán, por regla general, tan solo las unidades y departamentos relevantes en términos generales: «Recursos humanos», «finanzas y contabilidad», «jurídico», «gestión de clientes», etc., (y muchos organismos públicos adoptan la terminología de entidades privadas, por ejemplo, al referirse a los solicitantes de ayudas sociales como «clientes» de la oficina de ayudas sociales). Se trata de un punto de partida útil, pero poco más que eso. El DPD deberá aclarar en más detalle, en conversaciones pormenorizadas con la alta dirección, incluyendo al/a los responsable(s) de TIC y jurídico de la

organización y, cuando corresponda, a las oficinas regionales o nacionales, de qué son exactamente responsables las distintas unidades y departamentos, incluyendo, en particular, el objetivo por el que cada unidad y departamento necesita y realiza tratamiento de datos personales; bajo qué arquitectura de tecnologías internas y externas se realiza; y si implica servicios o medios tecnológicos externos (incluyendo computación en la nube). Es aquí donde la definición preliminar del alcance se solapa con la ejecución del inventario de operaciones de tratamiento de datos personales de la Función 1 – pero en la fase preliminar, tan solo es necesario identificar en términos generales las operaciones de tratamiento de datos personales, con referencia al objeto de cada una de dichas operaciones, y las tecnologías empleadas. Además, el DPD deberá, en esta fase previa, formar también una idea inicial de cuáles son las **funciones** y **responsabilidades** que tiene cada unidad o departamento con respecto a cada operación de datos personales – por ejemplo deberá, identificar quién es el «**propietario del negocio**» de cada operación (utilizando la terminología del SEPD).

EJEMPLOS:[302]

La Agencia **española** de protección de datos, la AEPD, enumera los siguientes **ejemplos de registros de datos personales (requeridos por ley) que mantienen las autoridades locales:**

- Padrón municipal de habitantes
- Gestión de tributos locales
- Registro de receptores de subvenciones (por ejemplo, subvención para vivienda o prestación por incapacidad)
- Registro de clientes de servicios sociales (por ejemplo, bienestar infantil)
- Registros de imposición de multas (por ejemplo, multas de aparcamiento)
- Registro de licencias y permisos (por ejemplo, para abrir un bar)
- Registro de unidades y agentes de policía local
- Registro de personas dadas de alta en las oficinas de empleo de la administración local;
- Registro de niños en el sistema educativo local
- Registro de personas a las que se expiden documentos oficiales (por ejemplo, nacimientos, matrimonios, fallecimientos)
- Registro de personas enterradas en cementerios locales
- Registro de usuarios de bibliotecas que gestionan las autoridades locales
- Registro de personas que han firmado para recibir notificaciones sobre eventos culturales

Y, por supuesto, también:

- Contabilidad
- Recursos humanos
- Etcétera

La agencia de protección de datos ofrece los siguientes **ejemplos de leyes o reglamentos que respaldan el tratamiento de datos personales en relación con algunos de los registros de datos personales que mantienen las autoridades locales españolas**, que constan más arriba:[303]

Registro:	Ley/normativas de base:

[302] Basado en: *Protección de Datos y Administración Local* (Data Protection and Local Administration) guía sectorial publicada por la Agencia Española de Protección de Datos, AEPD, 2017, p. 8 (nuestra traducción y edición), que se encuentra disponible en: https://www.aepd.es/media/guias/guia-proteccion-datos-administracion-local.pdf

[303] AEPD, Guías sectoriales sobre Protección de datos y Administración Local (pie de página anterior), p. 11.

• Padrón municipal	Ley sobre padrones municipales locales
• Registro de personas obligadas al pago de impuestos locales	Ley de *Haciendas locales*
• Datos de recursos humanos	Normas que cubren esta actividad

En algunas circunstancias, podrían existir otras bases jurídicas para el tratamiento, por ejemplo:

Registro:	Otras bases jurídicas:
• Registro de personas que se apuntan a eventos culturales	Normativa local y de consentimiento
• Registro de usuarios de las bibliotecas de las autoridades locales	Normativa de contratos y local

Además, es importante que, en esta fase, el DPD (con ayuda del personal de TIC y de seguridad) se familiaricen en profundidad con los **sistemas técnicos TIC, -arquitectura y -políticas de su organización**: los ordenadores (o, si se siguen usando, los sistemas de entrada manual de datos) empleados y si incluyen dispositivos portátiles o móviles (o «dispositivos propios o personales del personal correspondiente, para lo que debe contarse [o implantarse] una política de «Trae tu propio dispositivo [BYOD, por sus siglas en inglés]; si se utilizan ordenadores personales o dispositivos en línea o exclusivamente en modo sin conexión, en la ubicación o también fuera de ella; qué software de seguridad y de cifrado se utiliza, y si está totalmente actualizado; cuáles son los enlaces e instalaciones externos (incluyendo el uso de servidores en la nube, especialmente si se encuentran fuera de la UE/EEE, por ejemplo, en EE.UU., en cuyo caso deben verificarse los acuerdos o contratos relevantes sobre transferencia de datos; si parte del tratamiento es efectuada por encargados (en cuyo caso, deberán revisarse los contratos con ellos); [304]cuáles son las medidas físicas de seguridad (puertas, habitaciones, red, y contraseñas de ordenador, etc.); si existen políticas y formación en materia de seguridad, etc. En esta fase preliminar, no es necesario abordar y resolver todos esos asuntos, pero al menos, deberán ser **mencionados, localizados y registrados**.

Posteriormente, el DPD deberá tratar de aclarar todos los enlaces **externos** que su organización tenga con otras organizaciones. Habitualmente, son de **dos tipos**: (a) las organizaciones (hermana/madre/hija) con las que la organización del DPD tenga vínculos formales, dentro de lo que, a menudo, será (en el sector público) un **marco jerárquico**. Una

---

[304] La Agencia Española de Protección de Datos, AEPD, como contribución a este manual, ofrece los siguientes **ejemplos** de operaciones de tratamiento que, a menudo, subcontratan las autoridades locales (es decir, en los cuales, en términos de protección de datos, un encargado realiza el tratamiento):

• Preparación de nóminas del personal [*continúa al dorso*]
• Destrucción de documentos o medios
• Control de cámaras de videovigilancia
• Gestión tributaria
• Mantenimiento de equipos informáticos
• Tratamiento de datos del Padrón municipal de habitantes:
• Tratamiento de datos de impuestos municipales:
• Tratamiento de datos de recursos humanos: aplicable a normas de servicios públicos.
• Suscripción por medio de un servicio ofrecido por un Ayuntamiento en su página web para recibir comunicaciones relativas a actividades culturales.
• Registro en un banco de trabajo.

(La AEDP también tiene en cuenta la computación en la nube, tal y como consta en el texto).

autoridad local puede estar, a nivel formal, bajo la inmediata jurisdicción de una entidad regional, que, a su vez, esté controlada o supervisada por una entidad estatal provincial o federal, que a su más alto nivel encaje en una agencia a nivel nacional, en un ministerio nacional. No obstante, existen diferencias significativas en los acuerdos de un país a otro, o incluso dentro de un mismo país, incluyendo en lo relativo a la relativa autonomía con la que cuentan los distintos organismos, también en relación con el establecimiento y la gestión de sus operaciones de tratamiento de datos personales – por esto exactamente el DPD deberá familiarizarse con los acuerdos particulares de su organización particular.

El marco para todos los organismos públicos correspondientes pertenecientes a una determinada jerarquía quedarán definidos ampliamente en **legislación formal**, en varios niveles: constitución, ley, instrumentos normativos (legislación secundaria, vinculante), órdenes e instrucciones ministeriales, así como posibles **acuerdos administrativos**, acuerdos,[305] directrices y declaraciones políticas que no sean vinculantes o que no estén respaldadas por una norma, etc. El tratamiento de datos personales por parte de la organización del DPD podrá estar, asimismo, cubierto por un **código de conducta**, del que existen varios tipos. De nuevo, el DPD deberá comprender, de forma tan completa y detallada como sea posible, las normas y acuerdos y códigos – y los procesos mediante los que se adoptan, aplican, revisan y modifican – en la medida de lo posible, de nuevo, si fuera necesario con la ayuda del/de los asesor(es) jurídico(s) de su organización (o asistiendo a cursos sobre los asuntos necesarios si no tuviera pleno conocimiento de dichos asuntos cuando aceptó su cargo).

Asimismo, habrá otros DPD en las otras organizaciones pertenecientes a la jerarquía correspondiente – y será crucial para nuestro DPD estar plenamente comprometidos con ellos, en una **red de DPD.** Si todavía no existe dicha red, el DPD deberá trabajar para lograr su creación. Todos los DPD deberán establecer **relaciones óptimas y cercanas con la autoridad de protección de datos (APD)**, incluyendo a los miembros directivos dentro de la APD con responsabilidades específicas en relación con las autoridades públicas/ el tipo de autoridad pública a la que pertenece la organización del DPD.

Los acuerdos que alcance la autoridad francesa de protección de datos, el CNIL, para establecer una red nacional de DPD, con una «extranet» propia, es un buen ejemplo de una APD que respalda dicha creación de redes e interacciones.[306]

Existen, además, enlaces a **organizaciones externas que quedan fuera de la jerarquía de la organización del DPD.** Estos pueden incluir a otras **autoridades públicas en una jerarquía distinta** – por ejemplo, podrían existir enlaces entre establecimientos educativos e instituciones de prestaciones sociales, o la policía, o entre autoridades educativas en un país y organizaciones similares en otro. De nuevo, habrá (o debería haber) **leyes** que cubran dichos enlaces con esas entidades u otros **acuerdos y contratos formales y vinculantes** (como acuerdos y contratos de reparto de datos entre instituciones educativas y organizaciones de protección). El DPD deberá, de nuevo, obtener los datos completos de dichos acuerdos, cuando estos impliquen, o puedan implicar, el tratamiento de datos personales-y deberá revisarlos para comprobar si reflejan, confirman e implantan adecuadamente los requisitos del

---

[305] Dichos acuerdos podrán incluir acuerdos entre organismos públicos en virtud de los cuales un organismo público procese datos personales en nombre de otro organismo público, es decir, actúa como encargado para el último organismo. Este debate debe plantearse en el texto de los contratos responsable-responsable, responsable-encargado y transferencia de datos.

[306] Ver el apartado 2.3.3, bajo el encabezado «*Certificados y educación formal*», anteriores, así como la nota al pie 456, a continuación.

RGPD y de cualquier ley y norma de protección de datos, y de una ley más general de derechos humanos.[307] Es posible que el DPD no pueda poner en cuestión una ley o acuerdo legal deficiente como tal, pero podría, y debería, notificar a su empleador, y probablemente a la APD correspondiente, de su opinión de que dicha ley es deficiente.

En ocasiones, la relación entre y la cooperación entre entidades formalmente distintas, se basa en **acuerdos privados e informales**. No obstante, esto es problemático desde el punto de vista de la protección de datos.

Tal y como indica el Grupo de trabajo del Artículo 29 en su opinión sobre los conceptos de responsable y encargado:[308]

> [Hay] una tendencia creciente hacia la diferenciación organizativa en la mayor parte de sectores relevantes. En el sector privado, la distribución de riesgos financieros o de otro tipo ha llevado a la continua diversificación corporativa actual, que solo se ve mejorada por fusiones y adquisiciones. En el sector público, se produce una diferenciación similar en el contexto de la descentralización o separación de los departamentos de política y agencias ejecutivas. En ambos sectores, existe un énfasis creciente en el desarrollo de cadenas de suministro o cadena de servicios en todas las organizaciones, y sobre el uso de la subcontratación o externalización de servicios, para beneficiarse de la especialización y posibles economías de escala. Como resultado de ello, existe un crecimiento en varios servicios, ofrecido por los proveedores de servicios que no siempre se consideran responsables o culpables. Con motivo de las elecciones organizativas de las compañías (y sus contratistas o subcontratistas), podrán ubicarse las correspondientes bases de datos en uno o más países, dentro o fuera de la Unión Europea.

Esto conlleva dificultades en relación con la división de responsabilidades y la atribución de la función de control. Tal y como indica el Grupo de Trabajo, las entidades involucradas deben proporcionar «aclaraciones suficientes» respecto de dicha división de responsabilidades y una atribución eficaz de (varias formas y niveles de) función de control; en la práctica, esto implica que las entidades involucradas deben ***analizar*** dichos asuntos, ***acordar*** dichas divisiones y atribuciones y ***registrar*** todo ello como **acuerdo formal** que pueda proporcionarse (y, de solicitarse, deba proporcionarse) a la o las APD y (quizás de forma simplificada) a los interesados y al público general.

Como parte de la Función de definición del alcance preliminar, el DPD deberá, de nuevo, **comprobar** si dichos acuerdos formales ya están implantados y, en ese caso, si (a) reflejan realmente las divisiones prácticas y atribuciones de responsabilidades y (b) cumplen totalmente con los requisitos del RGPD. Si dicho acuerdo no está en vigor, el DPD deberá **aconsejar** que se redacte uno de urgencia (y deberá participar en las conversaciones, acuerdo y registro). Si únicamente hubiera acuerdos informales en vigor, el DPD deberá **aconsejar** que sean reemplazados por otros formales.

Además, cuando los enlaces y acuerdos con otras entidades alcancen o incluyan acuerdos responsable - responsable o responsable - encargado, deberán ir respaldados por los

---

307 Ver la sentencia del Tribunal Europeo de Derechos Humanos en el caso *Copland c. Reino Unido, de* 3 de abril de 2007, en la que el Tribunal sostuvo que una disposición de redacción imprecisa de una ley que concedía a una autoridad pública una competencia amplia en un ámbito determinado (en el caso concreto, la oferta de enseñanza superior y continua) no constituía una «ley» en el sentido del Convenio Europeo de Derechos Humanos:
http://hudoc.echr.coe.int/eng?i=001-79996 (ver, en particular, el párrafo 47.)

308 Grupo de trabajo del Artículo 29, Opinión 1/2010 sobre los conceptos de «responsable» y «encargado» (WP169, adoptado el 16 de febrero de 2010), p. 6, disponible en:
http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

correspondientes contratos **responsable – responsable o responsable – encargado**; y si los enlaces y acuerdos con otras entidades implican transferencias de datos personales a países de fuera de la UE/EEE (denominados «terceros países»), las transferencias deberán estar basadas en sus correspondientes **cláusulas sobre transferencia de datos** (ya sean cláusulas estándar aprobadas por la o las APD correspondiente o por el CEPD, o cláusulas *ad hoc* que se ajusten al RGPD).
Si existen dichos contratos o cláusulas, el DPD deberá **revisarlas** para ver si cumplen con el RGPD, y si no existen dichos contratos o cláusulas, pero debería haberlas, el DPD **aconsejará** que se formalicen urgentemente.
Esas funciones del DPD en relación con acuerdos formales, contratos responsable - responsable y responsable - encargado y cláusulas de transferencia de datos (y en otros aspectos relacionados) se analizan en detalle en 3.x siguiente. Aquí, será suficiente con indicar que el DPD deberá **identificar** dichos asuntos en la función de definición de alcance preliminar, que se abordará posteriormente.
Por último, la organización del DPD tendrá **enlaces con proveedores (del sector público y privado) externos de bienes o servicios**, que comprenderán tratamiento externo de datos, contabilidad y gestión de páginas web o aprovisionamiento de menús de la cafetería, mantenimiento y reparaciones, apoyo médico y de bienestar del personal, etc., etc. El trabajo realizado a este respecto sobre **contratos** (ya sean contratos civiles habituales o contratos especiales público-privados). Esos contratos constituirán, igualmente, una base (y deberán abordar de forma específica) toda operación tratamiento de datos personales que realicen las partes en relación con dichos contratos: desde la recogida de los datos personales relevantes, reparto y uso de dichos datos, hasta su destrucción o borrado finales. Si la otra entidad fuera la auténtica responsable, dichos contratos (o, al menos, los elementos relevantes sobre protección de datos de dichos contratos) constituirán, en términos de protección de datos, **contratos de tratamiento de datos personales responsable-responsable.** Si la otra entidad actúa meramente como encargada para la organización del DPD, el contrato será del tipo **responsable-encargado**. Y si en virtud del contrato, los datos personales se transfieren a una ubicación fuera de la EU/EEE, (normalmente, a un servidor «en la nube» que mantenga el contratista), dichos contratos constituirán **contratos de transferencia de datos personales**.
En el ejercicio preliminar de definición del alcance, el DPD **identificará** si existen dichos contratos y, entonces, poco después del ejercicio de definición del alcance, los **revisará**, y si, en términos del RGPD estuvieran incompletos o fueran deficientes, **aconsejará** que se formalicen o revisen.

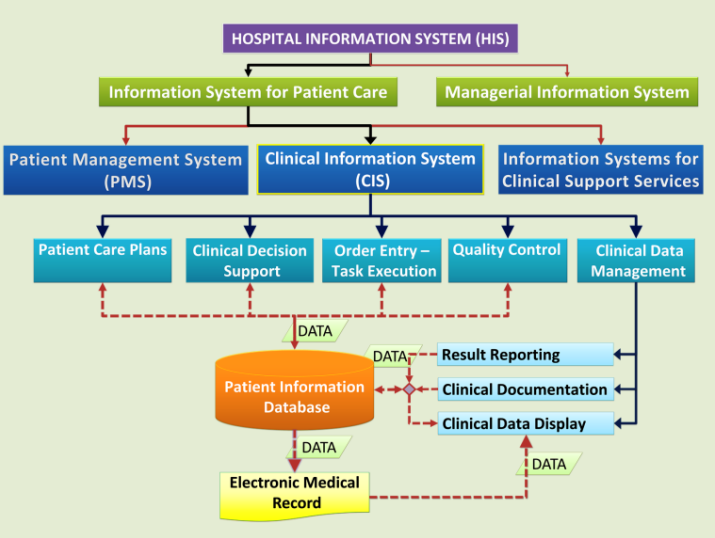
Creación de mapas sobre las actividades de tratamiento de la organización en términos generales

Cuando el DPD ha realizado la definición del alcance general de su organización (como consta más arriba), podrá realizar el mapa de las actividades de tratamiento de datos personales en términos generales, como paso crucial hacia la creación de un registro de tallado de todas esas actividades y de todas las operaciones de tratamiento de datos personales que se realizó en la Función 1 (según se comenta a continuación). Esto debería resultar en una tabla como la que se proporciona al dorso, creada por Dr. Abdollah Salleh, que indica los «*Componentes funcionales de un sistema clínico de información»* empleados en la primera formación T4DATA, en una presentación de la agencia italiana de protección de datos, la *Garante del Privacy*).[309]

[309] Luigi Carrozzi, presentación a la primera sesión de formación "T4DATA" de junio de 2018, diapositivas sobre «Guía práctica para DPD – Registro de operaciones de tratamiento de datos».

EJEMPLO

Mapa de las actividades de tratamiento de datos personales de una organización [aquí: de un hospital]



Fuente: Dr Abdollah Salleh, https://drdollah.com/hospital-information-system-his/

Es preciso tener en cuenta que el mapa superior está más estrechamente vinculado con las operaciones de tratamiento de datos personales que el organigrama de un hospital, que se mostró anteriormente.

Funciones de organización:

FUNCIÓN 1: Crear un registro de operaciones de tratamiento de datos personales

Con arreglo a una exención limitada que se comenta más abajo en dicho encabezado, el artículo 30 del RGPD dispone que cada responsable «llevará un **registro** de las actividades de tratamiento efectuadas bajo su responsabilidad», indicando varios detalles de cada operación, como el nombre del responsable (y, puede añadirse, del «propietario del negocio») de la operación, el objeto(s) de la operación, las categorías de los interesados, datos personales y receptores, etc. Dicha obligación de llevar un registro de operaciones de tratamiento está estrechamente relacionada con el principio de responsabilidad corporativa mencionada en el punto 2.2. anterior, al facilitar una supervisión eficaz por parte de la autoridad de protección de datos relevante («autoridad de supervisión»), tal y como subraya el Considerando (82) del RGPD:[310]

> ***Para demostrar la conformidad*** con el presente Reglamento, el responsable o el encargado del tratamiento **debe mantener registros de las actividades de tratamiento** bajo su responsabilidad.
>
> Todos los responsables y encargados **están obligados a cooperar con la autoridad de control y a poner a su disposición, previa solicitud, dichos registros**, de modo que puedan servir para supervisar las operaciones de tratamiento.

En otras palabras, tal y como indica la autoridad italiana de protección de datos, *Garante*:[311]

> **[El registro es una] medida para demostrar el cumplimiento normativo del RGPD.**

La referencia a «operaciones de tratamiento que son competencia [del responsable]» sugiere que el registro (a menudo, mencionado igualmente como registro) deberá abarcar **todas** las operaciones de tratamiento, y esto se estipula expresamente en la versión alemana del RGPD.[312] Esto también tiene sentido porque, tal y como indica el *Garante*:[313]

> La imagen general de activos de información «datos personales» y la operación de tratamiento que proporciona el registro, **es el primer paso hacia la responsabilidad corporativa**, dado que permite la evaluación del riesgo sobre derechos y libertades de los individuos y para implantar medidas adecuadas técnicas y organizativas que garanticen un nivel de seguridad adecuado al riesgo.

No obstante, y del mismo modo que casi todos los demás requisitos del RGPD, se trata de un deber formal del responsable más que del DPD; en la práctica, será el DPD quien estará a cargo de este trabajo (en estrecha cooperación con el personal relevante del responsable), o quien, en última instancia, participará directamente y lo supervisará. Tal y como indica el Grupo de trabajo del Artículo 29 (GP29):[314]

> En la práctica, los DPD crean, a menudo, inventarios y llevan un registro de operaciones de tratamiento basadas en la información que les proporcionen los diferentes departamentos de su organización responsables del tratamiento de datos personales.

---

310 Luigi Carrozzi, presentación en la primera sesión de formación "T4DATA", junio de 2018, de diapositivas sobre "Orientaciones prácticas para RPD - El registro de las operaciones de tratamiento de datos

311 *Idem*.

312 «*Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis **aller Verarbeitungstätigkeiten**, die ihrer Zuständigkeit unterliegen.*» (Se ha añadido el subrayado).

313 Luigi Carrozzi (nota al pie 236, anterior (subrayado original).

314 Directrices sobre DPD del GT29, (nota al pie 242, anterior), apartado 4.4, *El papel del DPD en el mantenimiento de registros*, p. 18.

Esta práctica se ha establecido en muchas leyes vigentes y bajo las normas de protección de datos aplicables a las instituciones y entidades de la UE.[315]

El artículo 39(1) proporciona una lista de funciones que debe tener el DPD como mínimo. Por lo tanto, nada evita que el responsable o el encargado de asignar al DPD la función de mantener el registro de operaciones de tratamiento bajo la responsabilidad del responsable. Dicho registro debe considerarse como una de las herramientas que permiten al DPD llevar a cabo sus funciones de supervisión de cumplimiento normativo, de información y asesoramiento al responsable o al encargado.

En cualquier caso, el registro que el Artículo 30 obliga a llevar debe considerarse igualmente como una herramienta que permita al responsable y a la autoridad de supervisión, previa solicitud, contar con una visión general de todas las actividades de tratamiento de datos personales que lleva a cabo una organización. Es, así, un pre-requisito para el cumplimiento normativo y, como tal, una medida de responsabilidad corporativa eficaz.

Para un nuevo RPD, se requiere en primer lugar, la realización de un inventario de todas las operaciones de la organización que puedan implicar el tratamiento de datos personales y de los vínculos con otras organizaciones. Esto implica considerar qué datos son realmente necesarios, lo que no siempre es sencillo[316].

Es útil llevar a cabo, en paralelo con la definición del alcance general de la organización y de su contexto operativo, un ***inventario básico inicial***, en la función preliminar (Función 0) descrita más arriba. Con arreglo a dicha exención, que consta más abajo, esto deberá ir posteriormente seguido de un ***inventario completo***.

El ***inventario completo*** debe conducir a la creación del **registro** (la recogida de «**registros**») de todas las operaciones de datos personales del responsable que se mencionan en el Artículo 30 (tal y como se analiza posteriormente en este apartado, bajo el encabezado «Contenidos y estructura de las entradas del registro») – que, en adelante (y tras la revisión y valoración que se indica a continuación, en las Funciones 2 y 3) sean actualizadas por el DPD (o el DPD debería, al menos, asegurar que esté actualizada): ver el texto siguiente, bajo el encabezado «*Supervisión de cumplimiento normativo* (en curso), tras la Función 4.

Exención:

El Artículo 30(5) exime a las **empresas u organizaciones que empleen a menos de 250 personas, cuyo tratamiento de datos personales sea «ocasional»**[317], del deber de mantener un registro de sus operaciones de tratamiento de datos personales. No obstante, dicha exención no será de aplicación si:

- el tratamiento que lleva a cabo la empresa u organización «puede suponer un **riesgo para los derechos y libertades de los interesados**» (téngase en cuenta que no tiene por qué ser un «riesgo elevado», que desencadene la necesidad de llevar a cabo una evaluación de impacto de la protección de datos (Función 4): cualquier riesgo para los derechos y libertades de los interesados, por pequeño que sea, requeriría el registro (y la revisión) de las operaciones del responsable del tratamiento;

---

315 Artículo 24(1)(d) Reglamento (CE) 45/2001 [nota al pie original]

316 Véase WP29, Dictamen 4/2007 sobre el concepto de datos personales (WP136), adoptado el 20 de junio de 2007, disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

317 En nuestra opinión, la condición de que la pequeña organización deba continuar únicamente con el tratamiento de datos personales «de forma ocasional» se deriva de la estipulación (que se comenta en el texto) de que la exención no será de aplicación si el tratamiento que realice dicha pequeña organización «no es ocasional».

- El tratamiento **no es ocasional**; o
- El tratamiento incluye **datos sensibles o datos sobre condenas penales y delitos**.

En relación con el primero de ellos, en el contexto de las EIPD (necesarios cuando existe la posibilidad de un *«alto ries*go para los derechos y libertades de personas físicas»: ver Función 4, a continuación), el GT29 ha descrito el término «**riesgo**» como:[318]

> Escenario que describa un evento y sus consecuencias [negativas], estimadas en términos de gravedad y probabilidad

Y se explica que:[319]

> la referencia a «**los derechos y libertades**» de los interesados tiene que ver, principalmente, con los derechos a protección de datos y privacidad, pero puede involucrar, igualmente, otros derechos fundamentales, como libertad de expresión, de pensamiento, de movimiento, prohibición de discriminación, derecho a la libertad, conciencia y religión.

En abril de 2018, el GT29 publicó un "Documento de posición" sobre el artículo 30(5) del RGPD[320]. En este sentido, subrayó que:

> la redacción del artículo 30, apartado 5, es clara al establecer que los tres tipos de tratamiento a los que no se aplica la excepción son alternativos ("o") y que la existencia de cualquiera de ellos por sí solo obliga a llevar un registro de las actividades de tratamiento.
>
> Por consiguiente, aunque estén dotados de menos de 250 empleados, los responsables o encargados del tratamiento que se encuentren en situación de efectuar un tratamiento que pueda suponer un riesgo (no sólo un riesgo elevado) para los derechos de los interesados, o de tratar datos personales de forma no ocasional, o de tratar categorías especiales de datos con arreglo al artículo 9, apartado 1, o datos relativos a condenas penales con arreglo al artículo 10, están obligados a llevar un registro de las actividades de tratamiento[321]. No obstante, dichas organizaciones sólo tendrán que llevar registros de las actividades de tratamiento de los tipos de tratamiento mencionados en el artículo 30, apartado 5. Por ejemplo, es probable que una organización pequeña procese regularmente los datos relativos a sus empleados. En consecuencia, este tratamiento no puede considerarse "ocasional" y, por lo tanto, debe incluirse en el registro de las actividades de tratamiento. No obstante, no es necesario incluir en el registro de las actividades de tratamiento otras actividades de tratamiento que sean de hecho "ocasionales", siempre que sea improbable que supongan un riesgo para los derechos y libertades de los interesados y no impliquen categorías especiales de datos [los denominados "datos sensibles"] o datos personales relativos a condenas y delitos penales.

---

318 Directrices sobre la EIPD del GT29 (pie de página 351, siguiente), p. 6.

319 *Idem*, se ha añadido el subrayado.

320 WP29, Documento de posición sobre las excepciones a la obligación de mantener registros de las actividades de procesamiento de conformidad con el Artículo 30 (5) GDPR, 19 de abril de 2018, disponible en: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045
El documento de posición no fue aprobado expresamente por el Comité Europeo de Protección de Datos cuando aprobó una serie de "dictámenes" más formales del WP29 (EDPB, Endoso 1/2018, véase la nota 248, más arriba), pero todavía puede considerarse como una autoridad en la materia.

321 el WP29 considera que una actividad de tratamiento sólo puede considerarse "ocasional" si no se lleva a cabo con regularidad y se produce fuera del curso normal de las actividades del responsable del tratamiento o del transformador. Véase WP29 Directrices sobre el artículo 49 del Reglamento 2016/679 (WP262). [nota al pie de página original]

Ejemplo:

En Croacia, la ley exige que la información detallada sobre todos los funcionarios y empleados de los organismos públicos se cargue en un sistema central, el *Registro de Empleados del Sector Público*. Esto también será de aplicación a las entidades públicas más pequeñas, como las pequeñas comunidades locales que pueden emplear a muy pocas personas. El tratamiento de los datos sobre estos pocos empleados por parte de esa pequeña comunidad no es, por lo tanto, «ocasional» y no se beneficia de la exención de mantenimiento de registros.

En caso de duda, el responsable del tratamiento deberá solicitar el asesoramiento del DPD sobre estas cuestiones, y el DPD deberá inclinarse por aconsejar la creación de un registro completo en casos marginales, en lugar de arriesgarse a que se considere que la organización ha incumplido las obligaciones consagradas en el artículo 30, apartados 1 a 4.

Notas:

1. Sobre la pregunta de si el registro de operaciones de tratamiento de datos personales debe ser accesible a cualquiera (en línea o de otro modo), o no, ver Función 12, «*Información y sensibilizació*n».
2. La creación del registro, como tal, no implica aún una valoración del cumplimiento normativo de las operaciones registradas en el RGPD: esto se realiza en la Función 2 pero, desde luego, el registro deberá modificarse y actualizarse del modo y en el momento en que se realicen los cambios sobre las operaciones de tratamiento registradas: ver la entrada «*Supervisión del cumplimiento normativo*»: *Repetición de las Funciones 1 – 3 (y 4) de forma continua*», al final de la Función 4 (antes de la Función 5).

Contenido y estructura de las entradas del registro (registros):

El RGPD distingue entre los registros de responsables y encargados.

Contenido y estructura de las entradas del registro de responsables (registros)

En virtud del Artículo 30, apartado 1 del RGPD, el **registro** de operaciones de tratamiento de datos personales de un *responsable* consistirá en una colección de **registros** de cada una de dichas operaciones; y cada uno de dichos **registros deberá incluir toda la información indicada a continuación** (se han añadido las palabras entre corchetes y en cursiva):

a. el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;

b. los fines del tratamiento;

c. una descripción de las categorías de interesados y de las categorías de datos personales [*incluyendo si alguno de los datos entra en la lista de «categorías especiales de datos»/datos sensibles*];

d. las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;

e. en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;

f. cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;

g. cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.

Esta lista no incluye las bases jurídicas para el tratamiento de los datos correspondientes (artículo 6, en relación con datos no sensibles; artículo 9, en relación con datos sensibles), ni los instrumentos jurídicos utilizados para los contratos con los encargados del tratamiento o para la transferencia de datos, pero son cuestiones tan cruciales en relación con la determinación de la legalidad y la compatibilidad con los requisitos de la Directiva GDPR de cualquier operación de tratamiento que también deberían inscribirse en el registro, en relación con cada operación de tratamiento de datos personales (definida en función de la finalidad del tratamiento), con la validez de la base jurídica alegada y registrada que se comprobará en su momento.

MODELO DE FORMATO DE UN REGISTRO BÁSICO DE TRATAMIENTO DE DATOS PERSONALES DE UN RESPONSABLE[322]

Téngase en cuenta que debe crearse, para cada operación distinta, un registro individual

Parte 1 - Información sobre el responsable.

DATOS DE CONTACTO DEL **RESPONSABLE**:	Nombre, dirección, correo electrónico, teléfono
DATOS DE CONTACTO DEL **CORRESPONSABLE:***	Nombre, dirección, correo electrónico, teléfono
DATOS DE CONTACTO DEL **REPRESENTANTE**:*	Nombre, dirección, correo electrónico, teléfono
(*) *Si fuera de aplicación*	
DATOS DE CONTACTO DEL **DELEGADO DE PROTECCIÓN DE DATOS**:	Nombre, dirección, correo electrónico, teléfono

Parte 2 – Información básica sobre la operación de tratamiento de datos personales (OTDP)[323]

1.	Nombre de la OTDP[324]	
2.	Unidad responsable («propietario del	

[322] Ampliación del modelo de formulario presentado por Carrozzi (nota al pie de la página 236, más arriba) con modificaciones (por ejemplo, formato vertical en lugar de horizontal) y entradas sobre el nombre de la operación, las bases jurídicas para el tratamiento, las garantías adecuadas para la transferencia de datos y los detalles añadidos relativos a las tecnologías y la seguridad (en consonancia con las recomendaciones adicionales de Carrozzi).
NB: Al final de los comentarios de la presente función se adjunta un modelo de formato de un registro de tratamiento de datos personales más exhaustivo (15 páginas).

[323] La tabla modelo anterior tiene el mero objetivo de ilustrar el requisito de registro en términos más generales. El **modelo de registro detallado de tratamiento de datos personales** que se menciona en el pie de página previo y que se adjunta a esta Función solicita un dato adicional crucial, por ejemplo, para cada categoría de datos personales: el objeto, relevancia y fuente de los datos, etc...

[324] Desde un punto de vista legal-de protección de datos, cualquier tratamiento de datos personales es una operación que se define mejor sobre la base del objetivo al que sirve dicha operación (como consta en 2). No obstante, en muchas organizaciones, la personas que llevan a cabo las operaciones a menudo cuentan con un nombre interno/funcional específico para dicha operación, aunque ambas designaciones se solaparán a menudo y podrían ser idénticas.

negocio»)	
3. Objetivo de la OTDP	
4. Categorías de los interesados	
5. Categorías de los datos personales	
6. ¿Se incluyen datos sensibles?	
7. Base jurídica para el tratamiento:* * Ver art. 6 RGPD para datos no sensibles, art. 9 de datos sensibles	
8. ¿Se transfieren los datos a un 3º país o una organización internacional?	
9. En caso de transferencias mencionadas en el subpárrafo 2 del artículo 49(1) del RGPD: ¿qué garantías adecuadas se ofrecen?	
10. Plazos para el borrado	
11. Detalles de sistemas, aplicaciones y procesos (papel/archivos electrónicos; paquete de escritorio/aplicación gestionada centralmente/servicio en la nube/red local; transmisiones de datos, etc.) y medidas técnicas y organizativas (de seguridad) relacionadas.	
12. ¿Implica el procesamiento el uso de (un) procesador(es)? En caso afirmativo, facilítense todos los detalles y una copia del contrato o contratos correspondientes.	

Contenido y estructura de las entradas del registro de encargados (registros)[325]

En virtud del Artículo 30, apartado 2 del RGPD, el **registro** de operaciones de tratamiento de datos personales de un *encargados* consistirá en una colección de **registros** de cada una de dichas operaciones; y cada uno de dichos **registros deberá incluir toda la información indicada a continuación**:

a. el nombre y los datos de contacto del encargado del tratamiento o encargados del tratamiento y de cada responsable del tratamiento en cuyo nombre actúa el encargado del tratamiento y, en su caso, del responsable del tratamiento o de su representante y del responsable de la protección de datos;

b. las categorías de tratamientos efectuados por cuenta de cada responsable del tratamiento;

c. en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;

d. cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.

A continuación, ofrecemos una vez más un formato de muestra del tipo de registro que un procesador debe mantener para cumplir con estos requisitos.

MODELO DE FORMATO DE UN REGISTRO BÁSICO DE TRATAMIENTO DE DATOS PERSONALES DE UN RESPONSABLE[326]

Hay que indicar que debe crearse un registro individual por cada operación distinta de tratamiento de datos personales para cada responsable

Parte 1 - Información sobre el encargado y cualquier sub-encargado(s)

DATOS DE CONTACTO DEL **ENCARGADO:** Nombre, dirección, correo electrónico, teléfono
DATOS DE CONTACTO DEL **DELEGADO DE PROTECCIÓN DE DATOS**: Nombre, dirección, correo electrónico, teléfono
DATOS DE CONTACTO DEL **SUBENCARGADO:*** Nombre, dirección,

[325] Es cada vez más difícil distinguir completamente encargados de responsables. A menudo, las entidades que ofrecían servicios de encargados (que actuaban del modo que indicaba el responsable, quien determinaba los medios y los objetivos) han adoptado muchas otras responsabilidades y pueden pasar a ser «corresponsables». Es el caso, especialmente, en relación con proveedores de servicios en la nube, algunos de los cuales ofrecen ahora incluso «Inteligencia Artificial y aprendizaje automático (IA/AA(por medio de Aprendizaje automático mediante servicio (MLaaS)», ver: http://www.techmarketview.com/research/archive/2018/04/30/machine-learning-as-a-service-market-overview-technology-prospects
Tal y como se discute en la *Función preliminar*, los acuerdos entre entidades involucradas en acuerdos complejos deben registrarse clara y adecuadamente. Los modelos que registran las operaciones de tratamiento deberán revisarse y modificarse para que se ajusten a dichos acuerdos entre entidades (acordadas y registradas). Las entidades que sean encargados más que directos deberán usar el formulario detallado mencionado en el siguiente pie de página.

[326] De nuevo, se amplía a partir del modelo presentado por Carozzi (pie de página 236 anterior), con sus correcciones.

correo electrónico, teléfono
DATOS DE CONTACTO DEL **DELEGADO DE PROTECCIÓN DE DATOS**: Nombre, dirección, correo electrónico, teléfono
DATOS DE CONTACTO DEL **SUBENCARGADO:*** Nombre, dirección, correo electrónico, teléfono
DATOS DE CONTACTO DEL **DELEGADO DE PROTECCIÓN DE DATOS**: Nombre, dirección, correo electrónico, teléfono

* *Si fuera de aplicación*

Parte 2 - Información sobre el responsable de la OTDP en cuestión

DATOS DE CONTACTO DEL **RESPONSABLE**: Nombre, dirección, correo electrónico, teléfono
DATOS DE CONTACTO DEL **CORRESPONSABLE:*** Nombre, dirección, correo electrónico, teléfono
DATOS DE CONTACTO DEL **REPRESENTANTE**:* Nombre, dirección, correo electrónico, teléfono
(*) *Si fuera de aplicación*
DATOS DE CONTACTO DEL **DELEGADO DE PROTECCIÓN DE DATOS**: Nombre, dirección, correo electrónico, teléfono

NB: La relación entre el responsable y el encargado, y entre el encargado y cualquier sub-encargado, deberá basarse en un contrato escrito que cumpla lo dispuesto en el artículo 28 del RGPD. Los encargados deben mantener copias de los contratos relevantes con el formulario rellenado.

Parte 3 – Datos de la operación de tratamiento de datos personales (OTDP)

1. La categoría (tipo de) de tratamiento que se lleve a cabo para el encargado en relación con la OTDP general, incluyendo:	
- categorías de los interesados;	
- Categorías de datos personales; y	
- Si se incluyen datos sensibles.	
2. ¿Se transfieren los datos a un 3º país o una organización internacional?	
3. En caso de transferencias mencionadas en el subpárrafo 2 del artículo	

	49(1) del RGPD: ¿qué garantías adecuadas se ofrecen?	
4.	Detalles de sistemas, aplicaciones y procesos utilizados (tipo de archivos electrónicos; paquete de escritorio/aplicación gestionada centralmente/servicio en la nube/red local; transmisiones de datos, etc.) y medidas técnicas y organizativas (de seguridad) relacionadas.	
5.	¿Implica el procesamiento el uso de sub-procesador(es)? En caso afirmativo, facilítense todos los detalles y una copia del contrato o contratos correspondientes.	

Contenido y estructura del registro:

El DPD deberá construir el **registro** a partir de los **datos** que reciba en cada operación de tratamiento de datos personales. Normalmente, se clasifican por **organización**, y dentro de dicha categoría, por **propietario del negocio**. Con cada registro individual, el DPD deberá conservar toda la documentación pertinente (como se indica en los modelos de formularios anteriores).

El DPD deberá anotar en el registro cuándo se recibió cada dato, cuándo se revisó la operación de tratamiento pertinente (como se hace en la Función 2, descrita a continuación), con el resultado de dicha revisión y las medidas correctoras adoptadas, e indicar cuándo debe realizarse la operación para la siguiente revisión periódica (por ejemplo, anual).

- o – O – o –

Adjunto: Modelo de formato de un registro detallado de tratamiento de datos personales[327]

[327] También la APD polaca, Urząd Ochrony Danych Osobowych (UODO) ofrece un registro más detallado de datos personales en su página web, en: https://uodo.gov.pl/pl/123/214 (seguir el primer enlace al final de la página.)

Adjunto:

MODELO DE FORMATO DE UN REGISTRO DETALLADO DE TRATAMIENTO DE DATOS PERSONALES

Utilizar un modelo individual para cada operación de tratamiento de datos personales distinta

NB: Si cree que debe elaborar o aclarar un asunto, añada un número en el campo correspondiente y adjunte una página con esas elaboraciones o aclaraciones, con referencia a ese número.

I. GENERAL: * indica un campo obligatorio (si fuera de aplicación)

Responsable: (Principal entidad responsable)* (Nombre, lugar del establecimiento y dirección, número de registro, etc.)	
Entidades vinculadas (Cualquier entidad con la que el responsable esté vinculado en relación con esta operación, por ejemplo, empresas matrices o filiales u organismos públicos vinculados; encargados que participen en esta operación).	
Unidad de negocio: («Propietario del negocio»)* (Por ejemplo, RRHH, Contabilidad, I+D, Ventas, Atención al cliente)	
Persona de contacto en la unidad:	
OBJETO PRINCIPAL DE LA OPERACIÓN DE TRATAMIENTO DE DATOS PERSONALES:* ***Especificar del modo más preciso posible***	
¿Se utilizan o divulgan los datos personales para cualquier otro propósito o propósitos (secundarios)? *Por favor, especifique con la mayor precisión posible y añada un enlace o referencia al registro asociado.*	
¿Se realiza esta operación para todas las entidades vinculadas por igual? ¿O de forma separada o distinta para entidades distintas?* ***Especifique.*** ***Si las operaciones varían para cada entidad, utilice un formulario distinto para cada una.***	
Aproximadamente, ¿a cuántos individuos (interesados) afecta esta operación (si se conoce)?*	[*Añadir número o «desconocido»*]

Fecha de envío de este formulario al DPD:*	
Formulario y operación de tratamiento revisado por el DPD:	[*Sí/No y fecha que debe introducir el DPD*]
Fecha de entrega de revisión/actualización de este formulario:	[*Debe especificarlo el DPD*]

II. DETALLES DE LA OPERACIÓN DE TRATAMIENTO DE DATOS PERSONALES:

II.1 Datos y sus fuentes [NB: Todos los campos son obligatorios, si fuera de aplicación,

Salvo que se indique lo contrario]

1. ¿Qué datos personales o categorías de datos personales se recogen y utilizan para esta operación?	*Marcar √ según proceda:*	**¿Cuándo, cómo y de quién se obtienen los datos?** **Por ejemplo:** (interesado=DS) - DWP, tras emplear a la persona - DS, tras registro en una investigación
- Nombre y apellido(s)		
- Fecha de nacimiento		
- Domicilio		
- Número de teléfono del trabajo		
- Número de teléfono personal		
- Dirección de correo electrónico del trabajo		
- Dirección de correo electrónico personal		
Añadir datos adicionales, más abajo, si corresponde:* ** Ver también más abajo, en 2, datos sensibles*		
Añadir más columnas si fuera necesario		
2. Los datos que recoge y registra para la operación, ¿incluyen o revelan de forma indirecta alguna de las categorías especiales de datos personales que siguen («datos sensibles»)?	*Marque √ si los datos se recogen y utilizan expresamente para la operación;* *Marque √ y añada («indirecto») si el dato se revela de forma indirecta (explicar en nota si fuera necesario)*	**¿Cuándo, cómo y de quién se obtienen los datos?** **Por ejemplo:** (interesado=DS) - DWP, tras emplear a la persona - DS, tras registro en una investigación

- Raza u origen étnico		
- Opiniones políticas o afiliaciones		
- Creencias religiosas o filosóficas		
- Pertenencia a un sindicato		
- Datos genéticos		
- Datos biométricos		
- Datos relativos a la salud de la persona		
- Datos relativos a la orientación sexual o a la vida sexual de la persona		
- Información sobre condenas penales o delitos		
- Identificador nacional* * P. ej., Número NI, número fiscal		
- Datos sobre deudas/calificación crediticia		
- Datos sobre menores		
3. Si esto no se conoce o no se determina: ¿Cuánto tiempo se retienen los datos (especiales y de otro tipo)? ¿Qué sucede en ese caso?* * Indicar periodo o evento, por ej. «7 años» o «Hasta 5 años tras la finalización de su contrato de trabajo». Explicar, asimismo, qué ocurre con los datos; por ejemplo, borrado/destrucción o anonimización. **NB: Si hubiera periodos de retención distintos para datos distintos, indíquelo.**		

II.2 Comunicaciones de datos

4. ¿A qué terceros se comunican los datos arriba mencionados? ¿Y con qué objetivo? **NB: Esto es igualmente de aplicación a los datos que se hagan accesibles, especialmente de forma directa, en línea Comunicaciones re que impliquen transferencias a terceros países, ver más abajo, en II.5**	**Tercero receptor y lugar y país de establecimiento:**	**Objeto(s) de la comunicación(es):**
TODOS LOS DATOS QUE		

CONSTAN EN II.1		
***O:* Los datos siguientes:** (Copiar datos de 1 y 2, arriba)		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
Añadir más columnas si fuera necesario		

II.3 Base jurídica del tratamiento

5. **¿Sobre qué base jurídica se realiza el tratamiento de datos?** **NB: <u>Si existen diferentes bases jurídicas para datos distintos o para diferentes fines (primarios, secundarios o nuevos, no relacionados), indíquelo (en caso necesario, copiando y pegando las listas de datos de arriba a abajo, desplazando las diferentes bases jurídicas a la segunda columna).</u>**	*Marque la base jurídica correspondiente y ofrezca aclaraciones en la siguiente columna, según sea necesario.*	**Aclaración:**
- El interesado aceptó el tratamiento. **NB: Ver, también, PPs 6 - 9 más abajo.**		
- El tratamiento es necesario para el contrato entre tu organización y el interesado (O para tomar medidas a petición del interesado antes de celebrar un contrato, por ejemplo, obtener referencias)		
- El tratamiento es necesario para el		

cumplimiento de una obligación legal a la que su organización está sujeta * P. ej.: empleo o legislación fiscal - *especifique la ley en cuestión*		
- El tratamiento es necesario para proteger los intereses vitales de los interesados o de otras personas		
- El tratamiento es necesario para llevar a cabo una Función que se realiza en interés público * * *Especificar la fuente de la función (normalmente, una ley)*		
- El tratamiento se lleva a cabo en ejercicio de autoridad oficial * *Especificar la fuente de la función (normalmente, una ley)*		
- El tratamiento es necesario para un interés legítimo de su organización (o de otra entidad), y no es superado por los intereses de las personas interesadas Por ejemplo, marketing con sus propios clientes, o prevención del fraude - indique en detalle.		
CONSENTIMIENTO - explique con más detalle:		
6. **Si el tratamiento de datos se realiza sobre la base del consentimiento de los interesados, ¿cómo y cuándo se obtiene ese consentimiento?** **NB: Si el consentimiento se proporciona en formato papel o electrónico, proporcione una copia del texto/enlace correspondiente**		
7. ¿Qué prueba mantiene de que se ha dado el consentimiento? Por ejemplo, ¿se mantienen copias en formato papel, o registros del		

consentimiento electrónico?	
8. ¿Cuánto tiempo se mantiene dicha prueba?	
9. Si, en el contexto de un contrato, su organización solicita más datos de lo que sea necesario para el contrato, ¿se le comunica a la parte interesada que no debe proporcionar datos adicionales? **NB: Indique «N.A.» o, si fuera de aplicación, proporcione una copia del texto/enlace correspondiente**	

II.4 Informar a las partes interesadas [NB: Esta información no es obligatoria, pero Es útil para valorar y revisar las políticas internas de protección de datos]

10. **¿Se informa a las partes interesadas de lo siguiente? Y, en caso afirmativo, ¿cuándo y cómo?**	*Indicar sí/no (o «N.A.»)* **NB: Si corresponde, puede decir «es obvio en este contexto» o «La parte interesada ya tenía esta información»**	Explicar cuándo y cómo se hace esto **Entregue copias de cualquier aviso o enlace de información**
- ¿Su organización es responsable de la operación de tratamiento de datos personales?		
- Detalles de su organización (por ejemplo, nombre y número de registro)?		
- Si corresponde, datos de su representante en la UE		
- Datos de contacto del DPD		
- Fin principal del tratamiento		
- Cualquier otro fin para el que su organización quiera (o pueda querer) tratamiento de datos?		
- Si los datos no se obtuvieron directamente de las partes interesadas, la fuente o fuentes de los datos y si estos incluían fuentes accesibles al público (como registros		

públicos)		
- Los receptores o categorías de los receptores de los datos **NB: Ver P4 anterior**		
- Si los datos se transfieren (o se van a transferir) a un país de fuera de la UE/EEE (por ejemplo, a un servidor en la nube en EE.UU.) **NB: Esto es igualmente de aplicación a los datos que se hagan accesibles, (especialmente de forma directa, en línea) a entidades en países de fuera de la UE/EEE.**		
- Si los datos se transfieren de este modo, ¿qué garantías se han implantado, y cuándo pueden obtener las partes interesadas copias de las mismas? **NB: Se pueden proporcionar garantías en contratos de transferencia de datos o por medio de códigos de privacidad o sellos de privacidad.**		
- ¿Cuánto tiempo se mantendrán los datos?		
- ¿De sus derechos a solicitar acceso, rectificación o eliminación de sus datos; solicitar que se bloqueen sus datos o que se oponga a su tratamiento?		
- ¿De su derecho a presentar una reclamación ante la Autoridad de Protección de Datos correspondiente?		
11. Si se procesa la totalidad o parte de los datos sobre la base del consentimiento, ¿se informa a las partes interesadas de lo siguiente?		
- ¿Que pueden retirar su consentimiento en		

cualquier momento (y cómo lo hacen) (sin que ello afecte a la legalidad del tratamiento anterior)?		
12. Si la prestación de los datos es un requisito legal o contractual (o un requisito para formalizar un contrato), ¿se informa a las partes interesadas de lo siguiente?	*Indicar sí/no (o «N.A.»)* **NB: Si corresponde, puede decir «es obvio en este contexto» o «La parte interesada ya tenía esta información»**	Explicar cuándo y cómo se hace esto **Entregue copias de cualquier aviso o enlace de información**
- Si deben proporcionar los datos, y cuáles son las consecuencias si no los proporcionan.		
13. **Si se procesa la totalidad o parte de los datos sobre la base del criterio del «interés legítimo», ¿se informa a las partes interesadas de cuál es su interés legítimo en cuestión?**		Proporcione un breve resumen de los criterios aplicados en la prueba de ajuste llevada a cabo con respecto a los derechos y libertades fundamentales de las partes interesadas, en relación con el Artículo 6(1)f del RGPD.
14. **Si las partes interesadas quedan sujetas a toma de decisiones o perfilado automatizado, ¿se les informa de lo siguiente?**		Proporcione un breve resumen de la lógica empleada en el proceso de toma de decisiones o perfilado automatizados.
- ¿Que se llevará a cabo dicha toma de decisiones o perfilado?		
- En términos generales (pero significativos), ¿qué «lógica» interviene?		
- ¿Cuál es la importancia de la toma de decisiones o perfilado automático y las consecuencias deseadas de la toma de decisiones o perfilado?		

II.5 Flujo de datos transfronterizo [NB: No es obligatoria la entrada en el campo 17, pero de nuevo, es útil para la evaluación interna]

15. **¿Se transfiere alguno de los datos personales a un tercer país [por ejemplo, externo a la UE/EEE] (o un sector de un tercero país, o a una organización internacional que cuente con un nivel «adecuado» de protección, en virtud del art. 45 del RGPD?**	*Indicar sí/no y el/los país/es en cuestión.* *Si solo se transfieren algunos de los datos, pero no todos, especifique por cada categoría de datos.*	*Explique el objetivo de la transferencia, por ejemplo: como parte de las operaciones propias de su organización (por ejemplo, usando software en la nube), o como parte de una comunicación de los datos a un tercero (especifique la parte o las partes)*
TODOS LOS DATOS QUE CONSTAN EN II.1		
***O:* Los datos siguientes:** (Copiar datos de 1 y 2, arriba)		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
Añadir más columnas si fuera necesario		

16. **¿Se transfiere alguno de los datos a un tercer país [por ejemplo, externo a la UE/EEE], o a una organización internacional que no cuente con un nivel «adecuado» de protección, en virtud del art. 45 del RGPD?**	*Indicar sí/no y el/los país/es en cuestión.* *Si solo se transfieren algunos de los datos, pero no todos, especifique por cada categoría de datos.*	*Explique el objetivo de la transferencia, por ejemplo: como parte de las operaciones propias de su organización (por ejemplo, usando software en la nube), o como parte de una comunicación de los datos a un tercero (especifique la parte o las partes)*	*¿Qué dispositivo de seguridad o derogación forma la base de la transferencia? Indique un número, según la lista en la ***Nota** siguiente, y ofrezca una copia de cualquier documento*

			relevante
NB: *Si se transfieren los datos para distintos objetivos a los distintos receptores en distintos países, conteste a las preguntas por separado por cada contexto de transferencia.*			
TODOS LOS DATOS QUE CONSTAN EN II.1			
***O:* Los datos siguientes:** (Copiar datos de 1 y 2, arriba)			
-			
-			
-			
-			
-			
-			
-			
Añadir más columnas si fuera necesario			

*** NOTA:** Según el RGPD, las transferencias a países que no se considera que proporcionen una protección "adecuada" sólo pueden tener lugar si existen "garantías apropiadas", como se indica en la columna de la izquierda, más abajo, o si se aplica una excepción, como se indica en la columna de la derecha.

Garantías según lo dispuesto en el art. 46 del RGPD:	Excepciones según lo previsto en el artículo 49 del RGPD, si no estuvieran disponibles las garantías previstas en el art. 46 (ver Normas sobre CEPD a este respecto: se imponen aplicaciones e interpretación restrictivas):
1. Instrumento internacional entre entidades públicas; 2. Normas corporativas vinculantes (NCV); 3. Cláusulas estándar aprobadas sobre transferencia de datos; 4. Código de conducta; 5. Certificación; 6. Cláusulas ad hoc aprobadas	7. Consentimiento; 8. Contrato entre responsable y parte interesada 9. Contrato entre responsable y tercero 10. Necesario por motivos importantes de interés público 11. Necesario para reclamaciones legales; 12. Necesario para proteger intereses vitales de partes interesadas u otros; 13. La transferencia se realiza desde un registro accesible al público

17. **¿Existen normas que regulen cualquier sentencia de un órgano jurisdiccional y cualquier decisión de una autoridad administrativa de un tercer país que pueda notificarse al responsable del tratamiento o a cualquier otro encargado del tratamiento y que obliguen al responsable del tratamiento o al encargado del tratamiento a transmitir o divulgar datos personales?**	*Indicar sí/no y, en caso afirmativo, proporcionar copia de la normativa.*

(ver art. 48 RGPD)	

III. SEGURIDAD Y CONFIDENCIALIDAD

NB: Si las respuestas a las preguntas siguientes difieren entre los distintos datos, conteste por separado para cada grupo de datos distinto.	*Proporcione detalles:*
¿Los datos personales que constan en II.1 se mantienen en formato papel o electrónico? Si se mantienen en papel, ¿	
¿Dónde (físicamente) se almacenan los datos? (¿Su oficina? ¿En servidores del responsable principal? ¿En servidores de una organización vinculada? ¿En servidores de un tercero (por ejemplo, un proveedor de servicios en la nube)?	
¿Qué medidas existen para proteger contra el acceso no autorizado al/los lugar(es) físico(s) en el/los que se almacenan o a los que se puede acceder? ¿Existe una política de seguridad de datos que lo regule? *(En caso afirmativo, sírvase proporcionar una copia.)*	
¿Qué hardware se utiliza en el tratamiento de los datos? ¿Quién es responsable de la gestión y seguridad de este hardware?	
¿Están (cualquiera de) los datos almacenados en medios o dispositivos extraíbles? ¿Cuáles son esos medios/dispositivos? ¿Quién los tiene?	
¿Puede alguna de las personas con acceso a los datos utilizar dispositivos personales para acceder o procesar los datos? En caso afirmativo, ¿existe una política de BYOD sobre este asunto? *Proporcione una copia de la política.*	
¿Están todas las personas autorizadas a acceder a los datos personales sujetas a un deber de confidencialidad (ya sea en virtud de un conjunto de normas legales o profesionales o de un contrato)? *Sírvase*	

proporcionar detalles o copias de las normas o cláusulas contractuales pertinentes.	
¿Qué software/aplicaciones se utilizan en el tratamiento de los datos? (P.ej., paquete MS Office de escritorio, aplicación gestionada centralmente, servicio en la nube, etc.)	
- ¿Se gestiona este software de forma local o central? ¿En caso de que sea central, ¿quién es la entidad central? Si no es usted, ¿existe un acuerdo formal entre dicha entidad y su organización en relación con el uso del software? *Proporcione una copia de este acuerdo.*	
- ¿El software utiliza una «nube»? En su caso, ¿quién es el Proveedor de servicios en la nube, y donde su residencia legal? ¿Y dónde está la ubicación física de dicho(s) servidor(es) en la nube? Los datos en la nube ¿están totalmente codificados? ¿Cómo? (Por ejemplo, qué tecnología de encriptación se utilizó) *Proporcione una copia del contrato sobre el que se realiza el tratamiento.*	
- ¿Quién es el responsable (es decir, quién tiene poderes «admin») en relación con este software? (¿Usted? ¿Otra persona en su organización? ¿Alguien en una entidad central con quien usted tenga relación? ¿Otra persona?)	
Los datos se transmiten en algún momento/circunstancias de forma electrónica a otro medio, sistema o dispositivo?	
Si se transmiten por medios electrónicos, ¿se hace - por internet? En ese caso, ¿los datos están encriptados? ¿Cómo? (Por ejemplo, qué tecnología de encriptación se utilizó) - ¿por medio de FTP? ¿Cómo se asegura? - ¿por medio de VPN? ¿Cómo se asegura?	

- otros – *especifique*	

- o – O – o -

FUNCIÓN 2: Revisar las operaciones de tratamiento de datos personales

Para el DPD, después de haber creado el registro de la operación de tratamiento de datos personales de su organización (Función 1), el siguiente paso es llevar a cabo una revisión en profundidad de todas las operaciones de tratamiento de datos personales registradas, para comprobar si cumplen los requisitos del RGPD en todos los aspectos pertinentes, incluidos los relativos a:

- objeto-especificación y límites;
- validez de cualquier consentimiento (y existencia de la prueba documental de que se ha dado el consentimiento) o la aplicabilidad de cualquier otra base jurídica del tratamiento;
- datos personales procesados y su relevancia y necesidad, en relación con el objetivo(s) especificado(s));
- calidad de los datos (exactitud, actualización, etc., de los datos, así como minimización y seudonominizacion de los datos);
- Información ofrecida a la parte interesada de la moción propia del responsable (ya sea cuando se recogen datos de la parte interesada o de otro modo, o bajo petición - también en relación con datos recogidos de visitantes de sitios web);
- el periodo de tiempo durante el que se retienen datos en forma identificable y cualquier información relativa a la desidentificación;
- seguridad de datos técnicos, organizativos y físicos (incluyendo limitación de acceso físico y limitación de acceso técnico [nombre de usuario, contraseñas, políticas de PIN, etc.], encriptación, etc.);
- Transferencias transfronterizas (y compromisos legales y otros de tipo contractual para realizarlas)
- Etcétera

En vista de los resultados sobre lo anterior, el DPD deberá poder **valorar**:

- Si puede decirse que ***la totalidad*** de la operación de tratamiento cumple con el principio fundamental de legalidad y equidad.

(Esta evaluación del cumplimiento del RGPD es independiente y distinta de la evaluación de riesgos, que se describe más abajo como Función 3).

Los registros de las operaciones de tratamiento de datos personales creados en la Función 1 (en particular, si se crearon en su formato más detallado)[328] deberán conformar la base de la revisión, puesto que implicarán que el DPD pregunte y responde preguntas relevantes incluyendo, específicamente:

- ¿Queda suficientemente claro qué entidad es **responsable** de la operación de tratamiento de datos personales, y si hay involucradas otras entidades, cuál es su estado respectivo (p. ej., ***corresponsable, encargado***, o ***tercero*** responsable individual)? Si no fuera evidente, ¿existen **acuerdos formales** vigentes que aclaren dichos asuntos (ver función 1, arriba)?

[328] Según se indica en el formulario de muestra de un registro detallado de tratamiento de datos personales adjunto a la Función 1.

- ¿Queda lo suficientemente claro qué unidad de negocio es la «**propietaria del negocio**» respecto de la operación de tratamiento de datos personales (es decir, que tiene la responsabilidad diaria *de facto* sobre el tratamiento)? ¿Consta esto en un **documento formal** (por ejemplo, instrucciones específicas del responsable a la unidad)?

- ¿Quedan suficientemente claros los términos del **objetivo**, u **objetivos**, de la operación de tratamiento de datos personales? ¿Dónde (es decir, en qué parte del **documento**)? Si los datos personales que se utilizan en la operación de tratamiento se usan para más de un objetivo, ¿cuál es el ***objetivo principal*** y cuál es o son el/los ***objetivo(s) secundario(s)***? Esos objetivos secundarios, ¿son ***compatibles*** con el objetivo primario, o son objetivos independientes?

  NB: Al evaluar la compatibilidad de cualquier tratamiento para un objetivo secundario con el objetivo primario, el DPD deberá tomar en cuenta los asuntos que constan en el artículo 6, apartado 4 del RGPD.

  ¿Se justifican completamente y de forma legítima todos los objetivos para los que se realiza tratamiento de datos personales?

- ¿Son los datos personales tratados **adecuados**, **pertinentes** y **necesarios** para el objetivo principal? ¿Cómo se garantiza que son y siguen siendo **exactos** y **actualizados** para este fin, y qué medidas se toman para garantizarlo y para ***rectificar*** o ***actualizar*** o ***borrar*** información inexacta o desactualizada?

  ¿Las medidas adoptadas son adecuadas y suficientes? ¿Sería posible lograr el mismo objetivo con un menor riesgo para la privacidad y otros derechos de las personas afectadas?

- ¿Qué datos personales se utilizan o divulgan con *fines secundarios* o con fines nuevos y no relacionados (normalmente, a un tercero)? ¿Son los datos personales tratados **adecuados**, **pertinentes** y **necesarios** para esos fines secundarios o nuevos y no relacionados? (Si se revelan irreflexivamente todos los datos recogidos para un fin [primario] para un fin o fines secundarios o para uno nuevo, no relacionado, ellos, o algunos de ellos, podrían ser excesivos para tal fin secundario o no relacionado o para dichos fines secundarios o no relacionados. ¿Se ha tenido esto en cuenta?)

  NB: Ver formulario de tratamiento de datos personales en II.2.

  ¿Están completamente justificados, de forma legítima, todos los fines secundarios para los que se realiza tratamiento de datos personales?

- ¿Cómo se garantiza que los datos que se utilizan o revelan con fines secundarios o nuevos, no relacionados entre sí, sean **exactos** y estén **actualizados** para esos fines secundarios o nuevos en el momento de la primera utilización o divulgación para esos fines, y qué medidas se toman para garantizar que *sigan siendo* **exactos** y **actualizados** después de esa primera utilización o divulgación, y que se **rectifiquen** o **actualicen** o **eliminen** a medida que y en el momento en el cual pasen a ser inexactos o a estar desactualizados? ¿Las medidas relevantes son adecuadas y suficientes?

  NB: Si los datos se utilizan o divulgan para más de un propósito secundario o nuevo, estas preguntas deben responderse por separado para cada uno de los usos o divulgaciones secundarias o nuevas.

- **¿Cuándo, cómo, de quién y de qué forma** se obtiene **cada tipo** de datos personales? P. ej.: partes interesadas, departamento gubernamental, (antiguo) empleado, etc.; por ejemplo, en papel, por transferencia electrónica, etc.

  NB: Esta pregunta debe contestarse para datos no sensibles y sensibles, y si se obtienen datos distintos de fuentes distintas, deberá indicarse. Ver formulario de tratamiento de datos personales en II.1 y II.2.
  ¿Son adecuadas estas fuentes? ¿Sería mejor solicitar algunos datos que se obtienen de terceros de las partes interesadas?
- ¿Durante cuánto tiempo se retienen los datos (sensibles y no sensibles)? ¿Qué ocurre al final de ese periodo? Por ejemplo: ***supresión, destrucción, anonimización de los datos*** -o ***seudonimización***–, pero debe tenerse en cuenta que esto último significa que los datos siguen conservándose en forma identificable).[329] Si los datos se retienen de forma anónima o seudónima, ¿***por qué*** se hace esto? (Ejemplo: ¿por motivos de investigación o históricos?) En ese caso, deberá evaluarse por separado la compatibilidad con el RGPT del tratamiento a estos efectos).

  NB: * Indicar periodo de retención como tiempo específico, o como evento, por ej. «7 años» o «Hasta 5 años tras la finalización de su contrato de trabajo». Tener en cuenta que existen **normas formales** sobre los métodos recomendados de eliminación/destrucción de datos para las distintas categorías de datos y portadores de datos.[330] El DPD deberá comprobar si se cumplen (especialmente en lo relativo a información sensible, ya sea en el sentido legal de protección de datos, o en un sentido más amplio, social o político.
  ¿Son los periodos de retención de los datos los adecuados? ¿O demasiado largos? ¿Los medios de borrado/destrucción de datos cumplen con las normas nacionales e internacionales? Si se retienen datos más allá de los periodos normales de retención en

---

329 Es necesario indicar que en virtud del RGPD (en virtud de la Directiva de 1995 sobre Protección de Datos), los datos personales tan solo se considerarán anónimos si no nadie puede vincularlos a un individuo específico -es decir, no solo el responsable.(pero también, por ejemplo, por parte de colegas o parientes o amigos que podrían encontrar los datos si se publican en forma supuestamente desidentificada en Internet o en papel desechado). A este respecto, los DPD deben ser conscientes de que cada vez más datos que pueden parecer «no personales» o que se considere que se han «convertido en anónimos», pueden vincularse o volverse a vincular más fácilmente a personas concretas. En particular, los datos de conjuntos de datos «Big Data» supuestamente «anónimos» son, a menudo, de forma inesperada y preocupante, identificables posteriormente, especialmente si se enlazan o «emparejan» diferentes conjuntos de datos. Además, incluso si se utilizan conjuntos de datos verdaderamente no personales para crear «perfiles» (ya sean de consumidores típicos de un producto en particular, o de pacientes típicos, o de delincuentes o terroristas típicos), y dichos perfiles se aplican a conjuntos de datos para identificar a las personas que se ajustan al perfil, dicho tratamiento también puede afectar muy gravemente a esas personas, a las que se les puede negar un seguro, o un empleo, o el acceso a un vuelo o incluso a un país (o algo peor) sobre la base de algoritmos que, en la práctica, no pueden discutirse. Ver: Douwe Korff y Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards, informe para el Comité consultivo del Consejo de Europa sobre protección de datos, junio de 2015, Consejo de Europa, documento T-PD(2015)11, sección I.iii, *The dangers inherent in data mining and profiling*, disponible en: https://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2015)11_PNR%20draft%20report%20Douwe%20Korff%20&%20Marie%20Georges_15%2006%202015.pdf

330 Ver, por ejemplo:

- DIN German Institute for Standardization, Office machines - Destruction of data carriers, DIN 66399, octubre de 2012.
- NIST Special Publication 800-88 Revisión 1, Guidelines for Media Sanitization, diciembre 2014, en http://dx.doi.org/10.6028/NIST.SP.800-88r1
- US National Security Agency/Central Security Service, Media Destruction Guidance, enhttps://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml

forma anónima o seudónima: (i) ¿es apropiado a la vista del objetivo de la retención ampliada? ¿Podrían los datos conservados en forma seudonimizada mantenerse de forma totalmente anónima y continuar siendo suficientes para el propósito especial? ¿Qué tan cierto es cualquier afirmación de que los datos están «anonimizados»? (Es necesario tener en cuenta que la anonimización completa es cada vez más difícil de lograr, especialmente cuando se manejan grandes conjuntos de datos y, más especialmente, si se permite comparar los o vincular los conjuntos de datos a otros conjuntos de datos).

- ¿A qué **terceros** se **comunican** los datos arriba mencionados? ¿Y **con qué objetivo**? Los datos que se comunican son ***adecuados***, ***relevantes*** y ***necesarios*** a esos efectos, ***adecuados*** y ***actualizados*** y, en caso afirmativo, ¿cómo se asegura que sigan siéndolo?

  NB: Las respuestas a lo anterior pueden remitir, en parte, a las respuestas anteriores.
- ¿Sobre qué **base/s jurídica/s** se procesan los datos personales?

  NB:
  En el caso de datos no sensibles, la base jurídica deberá ser la especificada en el artículo 6 del RGPD, para datos sensibles, uno de los que se especifican en el artículo 6 del RGPD.
  Tenga en cuenta que la base del «interés legítimo» para el tratamiento (art. 6(1)(f)) no será de aplicación al tratamiento de cualquier dato – incluyendo datos no sensibles por parte de las autoridades públicas en la ejecución de sus funciones (art. 6(1), frase final) y no puede servir de base para ningún responsable, ya sea del sector público o privado, para procesar datos sensibles (ver art. 9).
  Además, si el tratamiento se basa en el artículo 6, apartado 1, letras c) o e) («tratamiento [que] sea necesario para cumplir una obligación legal aplicable al responsable», «el tratamiento [que] es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento»), deberá basarse en el Derecho de la Unión o de los Estados miembros de la UE (artículo 6, apartado 3). Si alguna de ellas constituye la base jurídica indicada, el DPD deberá comprobar si la ley en cuestión cumple los requisitos establecidos en el artículo 6, apartado 3, del RGPD.
  ¿La base jurídica que se reclama es adecuada para el tratamiento? ¿Se cumplen las condiciones necesarias para la aplicación de la base jurídica? (Por ejemplo, en relación con el consentimiento, del modo que se explica más adelante)?
  Tenga en cuenta que la base jurídica para el tratamiento con fines primarios puede ser diferente de la base jurídica para cualquier tratamiento (incluyendo el uso o la divulgación) de los datos con fines secundarios o nuevos y no relacionados, y la validez de la base jurídica alegada debe evaluarse por separado para cada uno de ellos.
- Si el tratamiento de datos se realiza sobre la base del **consentimiento** de los interesados:
  - ***cómo y cuándo*** se obtiene el consentimiento (por ejemplo, en formato papel o electrónico, por medio de una pregunta directa o solicitando a un individuo que seleccione una casilla)?[331]

[331] Tenga en cuenta que una declaración simple en una página web que diga lo siguiente: «Al continuar utilizando este sitio web, usted da su consentimiento para la recopilación y el uso de sus datos personales» ya no es suficiente como consentimiento válido en virtud del RGPD. No solo hay información insuficiente sobre el uso de los datos-lo que hace que el «consentimiento» no sea válido, pues no constituye un «consentimiento informado». Además, no está claro si continuar en el sitio web como tal puede constituir una «indicación inequívoca de los deseos de la parte interesada» con respecto a dicho consentimiento (ver definición de consentimiento en el artículo 4(11) del RGPD).

- ¿qué ***prueba*** se mantiene de que se ha dado el consentimiento (por ejemplo, copias en papel, registros)?
- ¿Cómo y cuánto tiempo se ***retiene*** esta prueba?
- Si, en el contexto de un contrato, su organización solicita más datos de lo que sea necesario para el contrato, ¿se le ***comunica a la parte interesada que no debe proporcionar datos adicionales***?

- ¿Se informa **a las partes interesadas** de todos los asuntos de los que debería informárseles (ver artículo 13 y 14 del RGPD, según consta en el formulario detallado de tratamiento de datos personales, en II.4), y, en ese caso, cuándo y cómo?

  ¿Se proporciona toda la información relevante? ¿Se hace esto en el mejor formato? ¿En el mejor momento? ¿Se distinguen claramente los campos obligatorios de los campos opcionales?
- ¿Se transfiere alguno de los datos a un **tercer país [por ejemplo, externo a la UE/EEE]**, o a una **organización internacional** que **no** cuente con un nivel «adecuado» de protección, en virtud del art. 45 del RGPD?

  ¿La decisión de adecuación relevante cubre, realmente, el tratamiento? ¿Sigue siendo válida? (Ver las conclusiones del TJEU de que la decisión sobre adecuación del «Puerto seguro» era inválida)
- ¿Se transfiere alguno de los datos a un tercer país [por ejemplo, externo a la UE/EEE], o a una **organización internacional** que **no** cuente con un nivel «adecuado» de protección, en virtud del art. 45 del RGPD? En ese caso, ¿qué dispositivo de seguridad o derogación forma la base de la transferencia?

  NB: En virtud del RGPD, las transferencias a países que no se considere que ofrecen una protección «adecuada» solo podrán tener lugar si se han implantado *bien* «**garantías adecuadas**», del modo indicado en el artículo 46 del RGPD, *o* si se aplica una **derogación**, según se indica en el artículo 48 del RGPD (ver sección II.5 en el formulario detallado de tratamiento de datos personales, pregunta 16).
  ¿Es/son correcta(s) la(s) garantía(s) o derogación(es) mencionada(s) ? ¿Cumple/n todos los requisitos que constan en el artículo correspondiente (art. 46 o 48)?
- ¿Existen normas que regulen cualquier sentencia de un órgano jurisdiccional y cualquier decisión de una autoridad administrativa de un tercer país que pueda notificarse al responsable del tratamiento o a cualquier otro encargado del tratamiento y que obliguen al responsable del tratamiento o al encargado del tratamiento a transmitir o divulgar datos personales?

  NB: En virtud del Artículo 48 del RGPD, cualquier sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país «únicamente podrá ser reconocida o ejecutable en cualquier modo si se basa en un acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el país tercero requirente y la Unión o un Estado miembro, sin perjuicio de otros motivos para la transferencia al amparo del presente capítulo». Se trata de una cuestión difícil de evaluar para los propietarios de empresas y para muchos controladores y procesadores, y debería existir orientación sobre cómo deben actuar los propietarios de empresas y los controladores y procesadores si se enfrentan a tal sentencia o decisión. Como mínimo, los transformadores y los propietarios de empresas deben remitir inmediatamente el asunto hasta el nivel de gestión más alto del responsable del tratamiento y del DPD.

Si existe una orientación pertinente, ¿es adecuada¿ (por ejemplo, si se adoptó antes de la plena aplicación del RGPD, puede que no mencionara la participación del DPD en el asunto, ya que puede que no hubiera un DPD cuando se elaboraron las directrices. Si todavía no se dispone de una orientación al respecto, debería redactarse con carácter de urgencia y consultarse al DPD sobre su contenido.

- ¿Qué medidas formales, organizativas, prácticas y técnicas existen para garantizar la seguridad y confidencialidad de los datos?

NB: En virtud de lo previsto en el artículo 23 del RGPD, el responsable y el encargado del tratamiento aplicarán «medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo» que suponga el tratamiento para los derechos y libertades de las personas jurídicas (incluyendo, en particular, a los interesados). El artículo enumera diversas medidas, como la seudonimización y el cifrado, las cláusulas de confidencialidad, las medidas técnicas para garantizar la integridad, la disponibilidad y la resistencia de los sistemas utilizados y las capacidades de restauración.

La cuestión se abordará más a fondo en la Función 3 (evaluación de riesgos). Sin embargo, en el contexto de la función 2 debería obtenerse ya una **visión general inicial** de las medidas adoptadas (o no), para dar una **indicación preliminar** de si las medidas adoptadas son «apropiadas» a la luz del «estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como el riesgo de que varíen las probabilidades y la gravedad de los derechos y libertades de las personas físicas» (como se indica en el artículo 23).

Muchas (aunque no todas) las medidas están cubiertas por normas reconocidas a nivel internacional, como las que se enumeran a continuación. Aun así, debe tenerse en cuenta que no siempre cubren todos los asuntos relevantes; por ejemplo, tienen a centrarse en la seguridad y no en la minimización de datos o en la limitación del objetivo.[332]

Incluso en ese caso, el DPD debe conocer las normas como esa, y comprobar si su APD o CEPD han emitido comentarios al respecto (de forma positiva o negativa, o con añadidos):[333]

- ISO/IEC 27001:2013 Código de prácticas para controles de información
- ISO/IEC 29100 - Tecnología de la información - Técnicas de seguridad - Marco de privacidad
- ISO/IEC 27018 - Código de prácticas para la protección de IIP en nubes públicas que actúan como procesadores de IIP
- ISO/IEC 29134 - Directrices para la evaluación del impacto en la privacidad (EIA)
- ISO/IEC 29151 - Código de práctica para la protección de la información de identificación personal
- JIS 15001:2006 - Requisitos del sistema de gestión de protección de datos personales
- BS 10012:2017 - Especificación de un sistema de gestión de la información personal

---

[332] Hace algunos años, las APD fueron conscientes de que un documento ISO sobre seguridad que abordaba códigos PIN no especificaba el número y la naturaleza de los caracteres que debían emplearse. Desde ese momento, las APD siguen una política de interaccionar lo más posible con grupos ISO cuyas actividades estén relacionadas con cualquier asunto de PD.

[333] Fuente: Alessandra de Marco, presentación de la primera sesión de formación «T4DATA», de junio de 2018, «*Normas vigentes (sobre seguridad y privacidad)*» y «*Normas (sobre privacidad) que aún no han concluido».*

Se están desarrollando nuevas normas:

- ISO 20889 - Técnicas de desidentificación de datos que mejoran la privacidad
- ISO 29184 - Avisos de privacidad en línea y consentimiento
- ISO 27552 Mejora de ISO/IEC 27001 para la gestión de la privacidad – Requisitos→ Nuevo título: Ampliación a ISO/IEC 27001 e ISO/IEC 27002 para la gestión de la información sobre privacidad - Requisitos y directrices.
- Práctica de referencia de UNI – Directrices sobre gestión de datos personales en entornos TIC en virtud del RGPD.

Si se utiliza una «nube» en el tratamiento, también se debe tener en cuenta si se han abordado los asuntos que figuran en las directrices «Trusted Cloud - Data Protection Profile for Cloud Services (TCDP)» publicadas en el marco del proyecto piloto «Data Protection Certification for Cloud Services», respaldado por el gobierno alemán (aunque hasta la fecha estas directrices todavía se refieren a la Ley Federal de Protección de Datos alemana anterior al RGPD, en lugar de al RGPD).[334]

En esta fase, el DPD debe comprobar si el responsable del tratamiento y/o los propietarios de las empresas son conscientes de las normas mencionadas y si tienen intención de aplicarlas y, en caso afirmativo, si existen certificaciones a tal efecto. La cuestión de si realmente se cumplen plenamente, o deberían cumplirse, puede abordarse más a fondo en la Función 3 (evaluación de riesgos).

Esta revisión es el primer ejemplo de la función de «(Seguimiento continuo del cumplimiento)» del DPD (que se menciona más adelante bajo dicho epígrafe después de la Función 4).

Si, en cualquier caso, el DPD considera que una operación de tratamiento de datos personales no cumple ninguno de los requisitos del RGPD, deberá informar de las deficiencias a la persona o personas internamente responsables pertinentes y proponer medidas correctoras (hasta, e incluso, la suspensión total de la operación en caso necesario). En caso de que no se siga este consejo, el DPD deberá remitir la cuestión a la alta dirección (véase más adelante, en «Funciones consultivas»).

Obsérvese que esta revisión general de las operaciones de tratamiento es una cuestión distinta de la situación de una violación de datos personales que se produce, como se ha comentado en relación con la Función 6 («Tratamiento de las violaciones de datos personales»): como se explica en la misma, dichas violaciones deben comunicarse inmediatamente a la más alta dirección.

El DPD deberá mantener registros completos de todas sus revisiones y evaluaciones, y de dicho asesoramiento.

- o – O – o -

---

334 Ver: https://tcdp.de/data/pdf/14_TCDP_v1.0_EN.pdf (ver, en particular la lista de normas que consta en las pp. 14 – 16). La versión disponible en el momento de su redacción (v.1.0) tiene fecha de septiembre de 2016, pero los autores esperan que – tras la creación de normas y procedimientos de certificación de auditoría basados en el RGPD – «*se convertirán las certificaciones de TCDP en certificaciones en virtud de lo previsto en el Reglamento General de Protección de Datos para servicios en la nube».* (p. 7). Ver, asimismo, el debate sobre factores de riesgo, etc., identificados por el Supervisor europeo de protección de datos en relación con servicios en la nube, debatidos en la Función 3 a continuación.

FUNCIÓN 3: Evaluar los riesgos que entrañan las operaciones de tratamiento de datos personales

Tal y como se indica en el artículo 2.2.1) anterior, el RGPD impone a los responsables un deber general de «[tener] en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los **riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas**, que plantee cada operación de tratamiento de datos personales, y «aplicar medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento» (Art. 24(1); ver también art. 25(1))).

El DPD, deberá también:

> En cumplimiento de sus funciones, tener en cuenta adecuadamente el riesgo asociado a las operaciones de tratamiento, teniendo en cuenta la naturaleza, alcance, contexto y objeto del tratamiento.
> (Art. 39(2))

Cumplir con esos requisitos requiere que se verifiquen los riesgos correspondientes. Esto deberá realizarse en relación con la ejecución del inventario de operaciones de tratamiento de datos personales y la creación del registro de dichas operaciones (Función 1) y, especialmente, con la revisión de dichas operaciones (Función 2).

El RGPD no requiere expresamente la participación del DPD en evaluaciones generales de riesgo: estipula dicha participación únicamente en relación con las Evaluaciones de impacto de protección de datos más detalladas (art. 35(2) - ver Función 4 más abajo). No obstante, en la práctica sería, cuando menos, muy recomendable implicar al DPD también en esas evaluaciones de riesgo más generales. De hecho, en la práctica, la evaluación dependerá a menudo de la opinión del DPD.

Debe tenerse en cuenta que los riesgos que es necesario evaluar no son solo riesgos de seguridad en un sentido reducido – es decir, la probabilidad e impacto de una **brecha de seguridad** [335] – sino los riesgos para los **derechos y libertades de las partes interesadas (y de otros individuos)** que pueda plantear la operación de tratamiento. Esto no solo incluye sus derechos generales a la privacidad y vida personal así como sus derechos específicos como partes interesadas, sino también, dependiendo del caso, sus derechos a la libertad de expresión, libertad de movimiento, no discriminación, libertad de poderes autoritarios y el derecho a permanecer en una sociedad democrática sin vigilancia indebida por sí mismos, o por otros países, y el derecho a una solución eficaz. El concepto es amplio.[336]

La evaluación general de riesgos también debería tener en cuenta los resultados de la Función 2. Por ejemplo, si resulta que, aunque una operación concreta de tratamiento fuera, como tal, legal (es decir, tuviera una base jurídica adecuada y tuviera un fin legítimo), pero se recogieran y almacenaran datos irrelevantes y excesivos para el objetivo correspondiente, contrario al principio de «minimización de datos», puede decirse que dicha operación supone un «riesgo» en sí misma, es decir, que se utilizarían erróneamente los datos irrelevantes e innecesarios. En tal caso, la medida adecuada para evitar dicho riesgo sería parar la recogida de los datos irrelevantes e innecesarios y borrar dichos datos que ya estuvieran almacenados. Otro

---

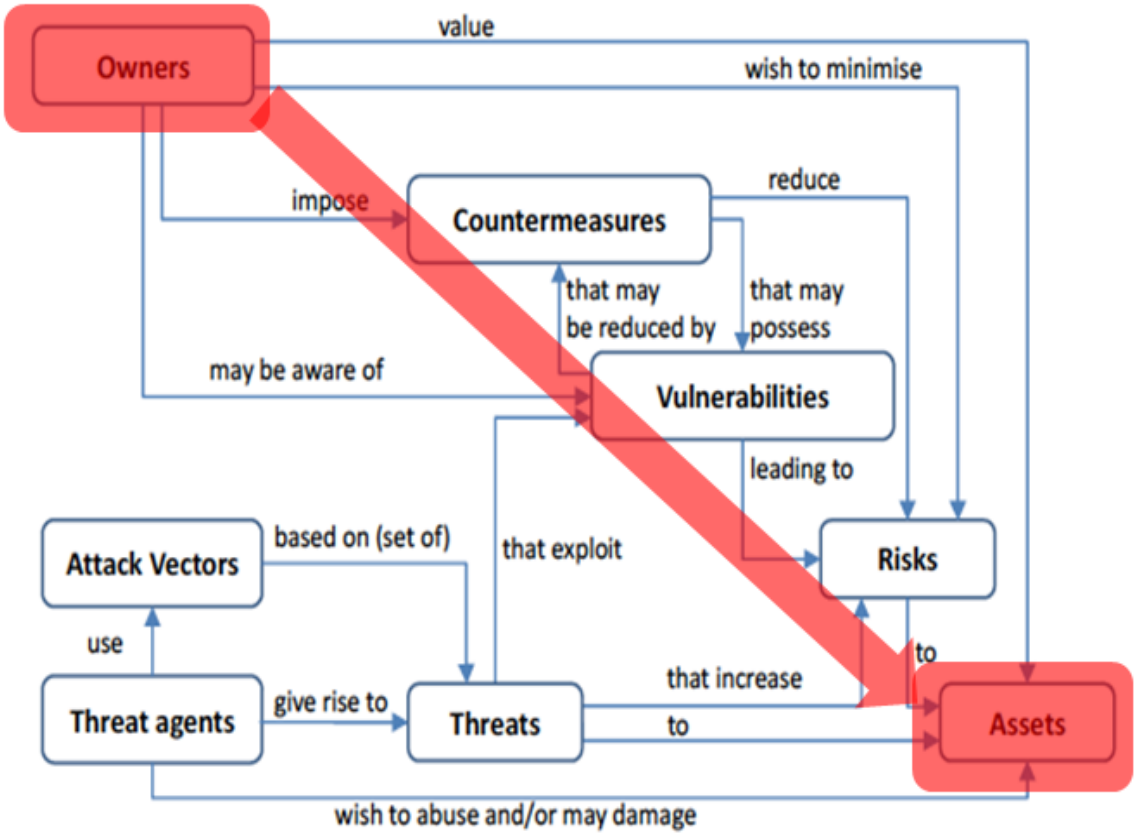
El RGPD define la «**violación de la seguridad de los datos personales**» como: «toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos». (Art. 4(12)). Ver Función 6, a continuación

[336] Ver los debates sobre el significado de «riesgo» y «riesgo alto» en, respectivamente, la Función 1 (en el epígrafe «*Exenciones*») y la Función 4.

ejemplo sería el uso de datos que pudieran identificarse en tratamiento estadístico que pueda llevarse a cabo por medios de datos seudoanonimizados o, incluso, totalmente anonimizados; en ese caso, la medida adecuada sería asegurar que los datos empleados se seudonimizarán adecuadamente (de forma seria) o que (preferiblemente) se anonimizarán por completo. Todo esto resalta que para la revisión general (Función 2) y la evaluación de riesgos (la presente Función 3), el responsable-en la práctica, el DPD- deberá analizar cuidadosamente **todos los aspectos de cada operación y función distinta de tratamiento de datos personales.** Tal y como sugiere la autoridad italiana de protección de datos, *Garante*, sería útil seguir el enfoque adoptado por ENISA (la Agencia Europea de Seguridad de las Redes y de la Información), que, a su vez, se basa en la norma ISO 27005, aceptada ampliamente: «*Las amenazas abusan de las vulnerabilidades de los activos para generar un daño a la organización*»; y debe considerarse, en términos más exhaustivos, que el **riesgo** está compuesto de los elementos siguientes:

Activo (Vulnerabilidades, controles), **Amenaza** (Perfil del agente de amenaza, Probabilidad) e **impacto**.

Los elementos del riesgo y sus relaciones pueden ilustrarse del siguiente modo:



Fuente: ENISA Threat Landscape Report 2016, Imagen 4: Los elementos de riesgo y sus relaciones, de conformidad con ISO 15408:2005, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016. Ver, además, su informe de 2017, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017.

Como también recalca el *Garante*, **una correcta evaluación de riesgos implica cuatro pasos**:[337]

[337] Giuseppe d'Acquisto, la presentación de la primera sesión formativa «T4DATA» sobre seguridad de datos, de junio de 2018, diapositiva sobre «*Evaluación de riesgos (enfoque en seguridad)*».

1. Definición de la operación de tratamiento y de su contexto.
2. Comprensión y evaluación del impacto.
3. Definición de posibles amenazas y evaluación de su probabilidad (probabilidad de que suceda una amenaza).
4. Evaluación de riesgos (combinación de la probabilidad y del impacto de que suceda una amenaza).

Lo primero (definir la operación de tratamiento y su contexto) se realizó en las Funciones 1 y 2 anteriores.

El segundo paso implica **definir distintos niveles de impacto** – que pueden razonablemente dejarse en cuatro niveles, del siguiente modo:[338]

NIVEL de impacto	**Descripción**
Bajo	Pueden encontrarse algunos inconvenientes menores, que superarán sin ningún problema (tiempo dedicado a reingresar información, molestias, irritaciones, etc.).
Medio	Los individuos podrían hacer frente a inconvenientes importantes, que podrán superar a pesar de algunas dificultades (costes adicionales, denegación de acceso a los servicios empresariales, miedo, falta de comprensión, estrés, malestar físico menor, etc.).
Alto	Los individuos pueden hacer frente a consecuencias significativas, que deben ser capaces de superar, aunque con serias dificultades (malversación de fondos, listas negras por parte de las instituciones financieras, daños a la propiedad, pérdida de empleo, citación, empeoramiento de la salud, etc.).
Muy alto	Individuos que pueden hacer frente a consecuencias significativas, o incluso irreversibles, que no pueden superar (incapacidad para trabajar, dolencias psicológicas o físicas de larga duración, fallecimiento, etc.).

Garante define **cuatro áreas principales de evaluación** en términos de **seguridad de datos**, que son:

A. Recursos de red y técnicos (equipo de hardware y software)
B. Procesos/procedimientos vinculados a la operación de tratamiento de datos
C. Distintas partes y personas involucradas en la operación de tratamiento
D. Sector negocios y escala del tratamiento

Por cada área de evaluación, plantea **cinco preguntas**, una respuesta positiva indica un riesgo,

338 *Idem*, diapositiva sobre «*Comprender y evaluar el impacto*»

del modo que se indica en la tabla al dorso.[339]

La persona que evalúe el riesgo de seguridad podrá, a partir de estas preguntas, calcular la **probabilidad de que suceda una amenaza**, según consta en las dos tablas en ese encabezado, tras la tabla, al dorso.

Esta puntuación podrá, posteriormente, combinarse con la puntuación de impacto para llegar a una **puntuación global de riesgos**, según consta en la tabla siguiente a las mismas.

LAS CUATRO ÁREAS PRINCIPALES DE EVALUACIÓN EN TÉRMINOS DE SEGURIDAD DE DATOS:

A. Red y recursos técnicos:	**B. Procesos y procedimientos**	**C. Partes y personas involucradas**	**D. Sector de negocio y escala**
1. ¿Hay alguna parte del tratamiento de datos personales que se lleve a cabo por internet?	**6.** ¿Los roles y responsabilidades con respecto a tratamiento de datos personales son vagos o no están claramente definidos?	**11.** ¿El tratamiento de datos personales es llevado a cabo por un número no definido de empleados?	**16.** ¿Considera que su sector de negocio es propenso a ciberataques?
2. ¿Es posible dar acceso a un sistema interno de tratamiento de datos personales por internet (por ejemplo, a algunos usuarios o grupos de interés)?	**7.** ¿El uso aceptable de la red, sistema y recursos físicos a nivel interno de la organización es ambiguo o está definido de forma poco clara?	**12.** ¿Alguna parte de la operación de tratamiento de datos la lleva a cabo un contratista/tercero (encargado de datos).	**17.** ¿Ha sufrido su organización algún ciberataque u otro tipo de brecha de seguridad en los dos últimos años?
3. ¿El sistema de tratamiento de datos personales está interconectado a otro sistema o servicio TIC externo o interno (de su organización)?	**8.** ¿Se permite que los empleados aporten y usen sus propias herramientas para conectarse al sistema de tratamiento de datos personales?	**13.** ¿Las obligaciones de las partes/personas involucradas en el tratamiento de datos personales son ambiguas o no son del todo claras?	**18.** ¿Ha recibido notificaciones o quejas con respecto a la seguridad del sistema TI (utilizado para el tratamiento de datos personales) durante el último año?
4. ¿Pueden los individuos no autorizados acceder fácilmente al entorno de tratamiento de datos?	**9.** ¿Se permite a los empleados transferir, almacenar o realizar otro tipo de tratamiento de datos personales	**14.** ¿El personal que participa en el tratamiento de datos personales no está familiarizado con asuntos de seguridad de la	**19.** ¿Una operación de tratamiento implica a un amplio volumen de individuos o datos personales?

339 *Idem*, las diapositivas sobre cada uno de los cuatro áreas principales de evaluación, con más explicaciones sobre por qué una respuesta positiva a la pregunta supone, en cada caso, un riesgo de seguridad.

	fuera de las instalaciones de la organización?	información?	
5. ¿Se diseña, implanta o mantiene el sistema de tratamiento de datos personales sin seguir las mejores prácticas relevantes?	**10.** ¿Pueden llevarse a cabo actividades de tratamiento de datos personales sin crear archivos de acceso?	**15.** ¿Las personas/partes involucradas en la operación de tratamiento de datos olvidan almacenar o destruir de forma segura datos personales?	**20.** ¿Existen mejores prácticas de seguridad específicas para su sector de negocio que no se hayan seguido adecuadamente?

PROBABILIDAD DE QUE OCURRA UNA AMENAZA (1):

Área de evaluación:	Nº de respuestas «sí»	Nivel	Puntuación
A. Red y recursos técnicos:	0 – 1	Bajo	**1**
	2 – 3	Medio	**2**
	4 – 5	Alto	**3**
B. Procesos y procedimientos	0 – 1	Bajo	**1**
	2 – 3	Medio	**2**
	4 – 5	Alto	**3**
C. Partes y personas involucradas	0 – 1	Bajo	**1**
	2 – 3	Medio	**2**
	4 – 5	Alto	**3**
D. Sector de negocio y escala	0 – 1	Bajo	**1**
	2 – 3	Medio	**2**
	4 – 5	Alto	**3**

Los puntos anteriores pueden introducirse en la siguiente tabla informativa:

PROBABILIDAD DE QUE OCURRA UNA AMENAZA (2):

SUMA global de puntuaciones:	NIVEL DE PROBABILIDAD de que ocurra una amenaza:
4 – 5	**Bajo**
6 – 8	**Medio**
9 – 12	**Alto**

Por último, estos resultados pueden combinarse con los resultados del «Nivel de Impacto» establecidos en el primer cuadro, arriba, para indicar el riesgo global, como se indica a continuación:

EVALUACIÓN GLOBAL DEL RIESGO:

		NIVEL DE IMPACTO		
		Bajo	**Medio**	**Alto/Muy alto**
PROBABILIDAD DE QUE OCURRA UNA AMENAZA	**Bajo**			
	Medio			
	Alto			

Leyenda:
[ ] *Riesgo bajo* [ ] *Riesgo medio* [ ] *Riesgo alto*

TENGA EN CUENTA, NO OBSTANTE, que el esquema anterior de evaluación de riesgos está principalmente relacionado con **riesgos de seguridad de datos.**
Existe, sin duda, una categoría principal de riesgos que debe evaluarse y abordarse, y no solo una vez, sino de forma continua, ya que los riesgos pueden evolucionar y mutar con el tiempo. Ver la nota titulada: *«Supervisión del cumplimiento normativo: Repetición de las Funciones 1 – 3 (y 4) de forma continua»* al final de la Función 4 (antes de la Función 5 que consta más abajo.
No obstante, el RGPD se refiere también, de forma general, a «**riesgo[s] para los derechos y libertades de personas físicas»** (ver artículos 34, 35 y 36). El primer artículo, artículo 34, acepta claramente que las brechas de seguridad, como tales, pueden resultar en dichos riesgos, e impone normas importantes sobre cómo abordarlos, según se indica en las Funciones 4 (EIPD), 5 (Función de investigación), 10 (Cooperación con la APD) y 12 (Función de información y sensibilización).
No obstante, debe indicarse que **«los riesgos para los derechos y libertades de personas físicas» no surgen solo de brechas de seguridad.** El mismo RGPD estipula en el artículo 35(1) que «altos riesgos» similares pueden surgir, en especial, de:

- evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;
- tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o

  o
- observación sistemática a gran escala de una zona de acceso público

En esos casos, *precisamente porque dichas operaciones de tratamiento suponen **altos riesgos inherentes** para los derechos y libertades individuales*, será necesaria una Evaluación de impacto de protección de datos (y, en algunos casos, deberá consultarse a la o las APD correspondiente(s)), como se indica en la siguiente función.
Más específicamente, la toma de decisiones automatizada basada en perfiles puede conllevar **decisiones injustas** (porque nadie es exactamente igual que otra persona, y ningún sistema puede saber, esperemos, todo sobre una persona) o decisiones no democráticas con **resultados discriminatorios pero incuestionables**;[340] el uso de datos sensibles también podría conllevar **discriminación** (ya sea intencionada o no);[341] el uso de datos sobre ventas aparentemente inocuos podría revelar información confidencial sobre salud o embarazo);[342] y la supervisión sistemática de personas en lugares públicos puede tener un **efecto**

---

340 Ver: Douwe Korff & Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards, informe preparado para el Comité Consultivo del Convenio de protección de individuos, con respecto al tratamiento automático de datos personales (T-DP) del Consejo de Europa, 2015, sección I.iii, *The dangers inherent in data mining and profiling*, disponible en: https://rm.coe.int/16806a601b

341 Por este motivo, en los instrumentos europeos de protección de datos se incluyeron normas especiales, especialmente restrictivas, sobre el tratamiento de datos personales: ver la «NB» en la Parte uno, sección 1.2.3, en la página 17 anterior.

342 Ver: *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*, Forbes, 16 de febrero de 2012, disponible en: https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#2ea04af16668

estremecedor sobre el ejercicio de derechos fundamentales, como el derecho a la libertad de expresión, de asociación y de protesta.[343] De hecho, los riesgos pueden combinarse, y después pasar a ser **complementarios**, como en el caso del uso de tecnología de reconocimiento facial en la supervisión policial de lugares públicos, con el objetivo de «identificar» a personas de mala conducta y predecir el mal comportamiento.[344]
Obsérvese que para que estos riesgos se materialicen no es necesario que se produzca una violación de los datos: los riesgos se derivan de las características intrínsecamente peligrosas de las propias operaciones de tratamiento, incluso si se realizan de conformidad con sus especificaciones y sin una violación de los datos tal como se define en el RGPD. ***Esto no se refleja en el (por lo demás muy útil) esquema de evaluación de riesgos que plantea el* Garante*, y que se reproduce más arriba.***
Lo mismo es cierto en relación con un menor «riesgo para los derechos y libertades de las personas físicas», que surge de las operaciones de tratamiento, y que no se indica que presenten un «alto riesgo» inherente. Esto incluye, en particular, operaciones de tratamiento que no cumplan completamente los requisitos del RGPD.

EJEMPLOS:

- Utilizar los datos personales recogidos para un fin para otro que no sea «compatible» sin una base jurídica adecuada para el tratamiento secundario o sin informar adecuadamente a los interesados de los usos secundarios previstos de sus datos, lo que se vería agravado si ello implicara la revelación de los datos a un tercero.

➢ Esto puede dar lugar a que se deniegue a los interesados la oportunidad de consentir (o no consentir, u oponerse) al tratamiento secundario, lo que puede afectarles negativamente (por ejemplo, en las solicitudes de empleo o de crédito). También es muy probable que los datos personales obtenidos en un contexto no sean lo suficientemente precisos o pertinentes para su uso en un contexto totalmente diferente.

- Retención y/o uso de datos personales (normalmente, una vez que ya no son necesarios para su propósito original) en forma seudónima o supuestamente anónima (normalmente, para su uso posterior en este formulario para un nuevo propósito secundario).

➢ En vista del creciente riesgo de identificación posterior de datos supuestamente anónimos,[345] debe considerarse que la conservación y el uso de datos con seudónimo o supuestamente anónimos supone un riesgo para los derechos y libertades de los interesados (lo que puede incluso suponer un probable "riesgo elevado", que requiere una evaluación de impacto de la protección de datos, tal como se discute en la Función 4). El DPD debe comprobar muy cuidadosamente los riesgos de volver a identificar tales datos en cualquier uso específico, e

---

343 Ver cita de la famosa sentencia Census del Tribunal Constitucional alemán en la página 10 del manual.

344 Ver: Douwe Korff, *First Do No Harm: La posibilidad de que las intervenciones estatales en materia de ciberseguridad afecten a los derechos y libertades fundamentale*s, apartado 2.4, *Vigilancia preventiva y predictiva*, en: Ben Wagner, Matthias C. Kettemann and Kilian Vieth (Eds.), Research Handbook on Human Rights & Digital Technology: Global Politics, Law & International Relations, Centre for Internet and Human Rights, Berlín, publicación para finales de 2018,

Para un resumen fácil de leer de los problemas de desidentificación y reidentificación, véase la presentación de la Fundación para la Investigación de Políticas de Información a la consulta del Gobierno del Reino Unido sobre Hacer de los Datos abiertos una realidad, octubre de 2011, disponible en: www.fipr.org/111027opendata.pdf.
Hace referencia al documento fundamental sobre esta problemática: Paul Ohm, Broken promises of privacy: responding to the surprising failure of anonymization, 57 UCLA Law Review (2010) 1701, disponible en: http://papers.ssrn.com/sol3/paperscfm?abstract_id=1450006.

imponer fuertes factores atenuantes (como la «privacidad diferencial»)[346] en los casos apropiados, o negarse a permitir el tratamiento posterior de los datos.

- Utilizar información irrelevante, incorrecta o desactualizada, con posibles consecuencias negativas similares.
- No dar la importancia adecuada a «los intereses o derechos y libertades fundamentales del interesado que requieran protección de datos personales, en particular cuando el interesado sea un niño», al evaluar si los datos personales pueden ser tratados sobre la base de la condición de «interés legítimo» (artículo 6, apartado 1, letra f), del RGPD).

➢ Esto, por definición, ocasiona daños a dichos intereses de las partes interesadas. El uso del criterio del «interés legítimo» como base jurídica para el tratamiento, requiere por tanto especialmente un profundo escrutinio por parte del DPD en la presente función.

➢ **NB:** Las administraciones no pueden basarse en este criterio «en el ejercicio de sus funciones) (art. 6(1), última frase), pero esto no implica que la cuestión nunca surja en un contexto del sector público, por ejemplo, con relación a funciones no previstas legalmente como envío de correos electrónicos a los ciudadanos sobre eventos culturales, utilizando el censo; o en relación con actividades que lleven a cabo entidades privadas que realicen funciones «para el interés público».

- No informar adecuadamente a las partes interesadas de los numerosos detalles de los que deben ser informadas en virtud de los artículos 13 y 14 del RGPD.

➢ Esto podría resultar en que las partes interesadas no pudieran ejercer completamente sus derechos en virtud del RGPD (que son, en realidad, precisamente los tipos de «intereses o derechos y libertades fundamentales de la parte interesada que requieren protección de los datos personales» que deban protegerse).

- Transferir datos personales a terceros países que no se considere que ofrecen un nivel «adecuado» de protección para los datos personales, sin contar con niveles de garantía adecuados o un conjunto de Normas corporativas vinculantes (NCV) implantadas, o que no se basen de otro modo en alguna de las derogaciones que se especifiquen (ver artículos 46 - 48 del RGPD). Esto incluye el uso de un servicio «en la nube» que utilice un servidor (o servidores) que estén ubicados en dichos terceros países.

➢ Tal y como ha señalado el SEPD en su asesoramiento detallado sobre el uso de servicios en la nube por parte de las instituciones europeas (que también deberían tener en cuenta las entidades públicas a nivel nacional, pues buena parte del asesoramiento podría serles de aplicación igualmente), la computación en la nube supone riesgos específicos que los responsables deben atender de forma más cuidadosa (contando con sus DPD).347 Efectivamente, sus sugerencias indican que la computación en la nube podría tener que ser

---

346 La privacidad diferencial es una medida importante para evitar la reidentificación de los interesados a partir de conjuntos de datos, pero sólo funciona si se aplica en un entorno controlado, en el que los investigadores están limitados en las consultas que pueden enviar a la base de datos, véase:
https://privacytools.seas.harvard.edu/differential-privacy
https://people.eecs.berkeley.edu/~stephentu/writeups/6885-lec20-b.pdf
No proporciona una respuesta a las circunstancias en las que los datos personales se entregan al público en general de forma supuestamente totalmente anónima, o en las que, por lo demás, se comparan grandes conjuntos de datos sin un control total.

347 Supervisor Europeo de Protección de Datos (SEPD), Directrices sobre el uso de los servicios de computación en la nube por parte de las instituciones y organismos europeos, marzo de 2018, disponibles en:
https://edps.europa.eu/sites/edp/files/publication/18-03-16_cloud_computing_guidelines_en.pdf
Ver, en particular, el *Anexo 4: Riesgos específicos de la protección de datos de computación en la nube*

analizada como si planteara inherentemente un alto riesgo y, por tanto, requiriera una Evaluación de impacto de protección de datos. Esto se indica en la función siguiente.

- La externalización del tratamiento de datos personales por parte de las autoridades, en especial si los datos son sensibles en el sentido técnico-legal del RGPD («categorías especiales de datos» – artículo 9), o sensibles en términos más generales, como datos financieros o del censo.

➢ El SEPD indica que el uso de computación en la nube agrava los riesgos inherentes a la externalización del proceso.[348]

Si, una vez que se ha llevado a cabo la evaluación, el DPD considera que una operación de tratamiento de datos no supone un riesgo para intereses relevantes, el DPD deberá **informar** a la persona o personas responsables a nivel interno de dichos riesgos, y sugerir **acciones atenuantes o alternativas.** A menudo, un objetivo legítimo puede alcanzarse por medios distintos, menos intrusivos, o por medio del uso de menos datos (o datos menos sensibles) y en dichos casos, el DPD deberá sugerir enérgicamente que se haga de esa forma. En caso de que no se siga este consejo, el DPD deberá remitir de nuevo la cuestión a la alta dirección (véase más en «*Funciones consultivas*»).

De nuevo, el DPD deberá mantener **registros** completos de todas sus revisiones y evaluaciones, y de dicho asesoramiento.

Si se sigue el consejo del DPD, estos archivos «**demostrarán** que el tratamiento se realiza de acuerdo con esta Norma» – es decir, que dichos riesgos han sido evaluados y que las medidas adoptadas a la luz de dicha evaluación eran adecuadas para esos riesgos (ver art. 24(1) y el debate sobre el «deber de demostrar el cumplimiento normativo» dentro del alcance del RGPD del apartado 2.2, anterior).

Tenga en cuenta que si la evaluación indica que un tratamiento propuesto supone un probable «**alto riesgo**» para los riesgos y libertades individuales, el DPD deberá informar al responsable de que será necesaria una Evaluación de impacto de protección de datos (EIPD), según se analiza en el apartado siguiente, en la Función 4.

Tenga en cuenta que, aunque no sea necesaria una EIPD, el DPD tendrá que continuar supervisando toda la operación de tratamiento de datos personales del responsable de forma continua: ver la discusión tras la Función 4, en el epígrafe «Supervisión del cumplimiento normativo: Repetición de las Funciones 1 – 3 (y 4) sobre una base continua».

Tenga en cuenta, igualmente, que, a menudo, el legislador nacional ya habrá tratado de abordar riesgos especiales que, en su opinión, suponen las operaciones o actividades de tratamiento especiales, en sus normas nacionales-algo que, puedan continuar, en gran medida en virtud de las "claúsulas de especificación" del RGPD.[349]

Ejemplos:

En **Croacia**, el tratamiento de ***datos genéticos*** para el cálculo del riesgo de enfermedad y otros aspectos relativos a la salud de partes interesadas en relación con la formalización de contratos de seguros de vida y contratos con cláusulas sobre la supervivencia está prohibido - y dicha prohibición no puede levantarse mediante el consentimiento de la parte interesada

---

348 El documento Directrices sobre el uso de los servicios de computación en la nube por parte de las instituciones y organismos europeos (pie de página anterior), del SEPD, «incide en el uso de servicios de computación en la nube que proporcionan las entidades comerciales, [pero] también aborda, como consecuencia natural, los asuntos que plantea la externalización de servicios TIC que procesan datos personales». (p. 5).

349 Ver Parte dos, sección 2.2.

(art. 20 de la Ley que implanta el RGPD).
Tanto en ese país como en otros, el uso de ***datos biométricos*** y ***cámaras de vigilancia en circuito cerrado de televisión (CCTV)*** está también sujeto a determinadas condiciones especiales, como un requisito de consentimiento especialmente claro e inequívoco, así como obstáculos, como establecer límites sobre la retención de los datos.
Dichas condiciones legales deben, por supuesto, tomarse completamente en cuenta en cualquier evaluación de riesgos: ningún responsable o DPD podría llegar a la conclusión de que un riesgo es aceptable, incluso si no se cumplieran condiciones y obstáculos legislativos especiales.

- o – O – o -

FUNCIÓN 4 Gestionar operaciones que pueden dar lugar a un «alto riesgo»: llevar a cabo una Evaluación de impacto de protección de datos (EIPD)

Lo que se indica más arriba sobre evaluaciones de riesgos generales (Función 3) se aplica, más aún, a operaciones de tratamiento de datos personales que, sobre la base de la evaluación general de riesgos arriba mencionada, se considera que pueden dar lugar a un «alto riesgo» para los derechos y las libertades de personas físicas» (art. 35(1)). El RGPD aclara que esto podría ser, en especial, el caso cuando se empleen «nuevas tecnologías».

Si la evaluación preliminar de riesgos de la Función 3 indica que una operación concreta de tratamiento de datos personales plantea un muy probable «alto riesgo», el responsable deberá llevar a cabo una **Evaluación de impacto de protección de datos** (EIPD) antes de continuar con la operación.

El RGPD estipula que, en cualquier caso, debe realizarse una EIPD en casos de toma de decisiones basadas en perfiles/totalmente automatizadas, tratamiento a gran escala de datos sensibles, o supervisión a gran escala de un área accesible al público (art. 35(3)). Las APD nacionales deben, asimismo, adoptar listas de operaciones que queden sujetas a la EIPD en su territorio, y pueden adoptar listas de operaciones que no las requieran, pero dichas listas deberán remitirse al CEPD, y podrán ser impugnadas por otras APD en virtud del «mecanismo de consistencia» del RGPD (art. 35(4) - (6)) El RGPD permitirá, asimismo, que el CEPD emita sus propias listas negativas y positivas, que versen sobre las que le remitieran las APD nacionales (quienes deben hacerlo en virtud del artículo 64(1)(a) del RGPD.

En la práctica, lo que ha ocurrido, en primer lugar, es que el Grupo de trabajo del Artículo 29 emitió dictámenes y orientaciones sobre la ejecución de una EIPD, tanto en sus Directrices sobre las EIPD de diciembre de 2016, en su revisión de abril de 2017 (WP243 rev1)[350], así como en sus siguientes Opiniones sobre las EIPD, más elaboradas, adoptadas el 4 de abril de 2017, con sus revisiones y adoptadas el 4 de octubre de 2017 (es decir, antes de que fuera de aplicación el RGPD).[351] Ambos fueron aprobados por el Supervisor Europeo de Protección de Datos el día en que entró en vigor el RGPD el 25 de mayo de 2018.[352] El SEPD proporcionó también unas orientaciones muy útiles en su documento sobre Responsabilidad corporativa sobre el terreno[353], que incluía una lista provisional de operaciones de tratamiento que, en su opinión, requieren o no requieren una EIPD.[354]

Las Directrices revisadas sobre las EIPD, adoptadas por el GT29 y aprobadas por el CEPD, establecieron **nueve criterios** que debían tenerse en cuenta para determinar si una operación de tratamiento puede dar lugar a un «alto riesgo» y decir que:[355]

> ***En la mayoría de casos***, un responsable de datos puede considerar que una reunión que cumpla **dos criterios** requeriría que se llevara a cabo una EIPD. En general, el GT29

---

350 Ver nota al pie 242 anterior.

351 Directrices sobre la Evaluación del impacto de protección de datos (EIPD) del GT29 y que establecen si es «probable que el tratamiento resulte en un alto riesgo» a los efectos del Reglamento 2016/679 (GT248 rev 1, que, en adelante, se denomina Orientaciones sobre las EIPD del GT29), página de contenidos, disponible en: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

352 Ver nota al pie 248 anterior.

353 EDPS, Responsabilidad corporativa sobre el terreno, Parte I: Registros, Archivos y cuándo realizar Evaluación de impacto de protección de datos (nota al pie 302, anterior), sección 4, *¿Cuándo realizar una EIPD?*, en pp. 9 – 11.

354 *Idem*, anexo 5.

355 Directrices sobre las EIPD del WP29 (pie de página 351, arriba), p. 11, énfasis añadido.

> considera que cuantos más criterios cumpla el tratamiento, más probable será que presente un alto riesgo para los derechos y libertades de las partes interesadas y, por tanto, que requiera un EIPD, con independencia de las medidas que desee adoptar el responsable.

Este asunto se analiza más abajo, en el epígrafe «*Cómo evaluar si una operación de tratamiento propuesta puede dar lugar a un «alto riesgo»*, en el que se proporcionan ejemplos de las Normas del GT29 y del documento del SEPD, en el subapartado «*Factores que indican «altos riesgos*».

En este caso, debemos indicar que, a continuación, la mayor parte de las APD nacionales (22 de las 28) [356] adoptaron sus propias listas provisionales, y las remitieron al CEPD para su revisión. El CEPD llevó a cabo dichas revisiones a la luz de las Normas del GT29 que había aprobado, y el 25 de septiembre de 2018, emitió 22 opiniones sobre dichas listas (una en cada borrador de lista).[357] El argumento principal que ofrece el CEPD de forma consistente en estas opiniones fue una recomendación a las APD de que no debían incluir operaciones de tratamiento en la lista de operaciones para las que es obligatoria una EIPD, si la operación en cuestión cumplía tan solo uno de los criterios para determinar si existía un posible «alto riesgo», lo que consta en las Normas. Así, por ejemplo, en su opinión, en el borrador de lista remitido por Reino Unido, dice:[358]

> La lista remitida por la Autoridad de supervisión de Reino Unido para obtener la opinión del Supervisor indica que el tratamiento de datos biométricos forma parte de la obligación de llevar a cabo una EIPD por su cuenta. El Supervisor opina que el tratamiento de datos biométricos por su cuenta no representa necesariamente un alto riesgo. No obstante, el tratamiento de datos biométricos con el objetivo de identificar exclusivamente a una persona física, junto con, al menos, otro criterio, requiere llevar a cabo una EIPD. Como tal, el Supervisor solicita a la Autoridad de supervisión de Reino Unido que modifique su lista, y añade que el elemento que hace referencia al tratamiento de datos biométricos a los únicos efectos de identificar a una persona física requiere que se realice una EIPD únicamente cuando se realice junto con, al menos, otro criterio, que se aplicará sin perjuicio de lo dispuesto en el artículo 35(3) del RGPD.

Desde luego, un responsable podrá realizar una EIPD incluso si tan solo se cumple uno de dichos criterios, sin que esto suponga una obligación.

El requisito de una EIPD puede obviarse en casos en los que una ley regule el tipo de operación en cuestión y se haya realizado una EIPD en el contexto de adopción de la ley (art. 35(10)). Además, «[una] única evaluación [EIPD] podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares» (Art. 35(1), última frase). Tal y como resumía el GT29:[359]

> ¿Cuándo no es necesaria una EIPD? Si «no es probable que el tratamiento entrañe un alto riesgo», o si existe una EIPD similar, o si fue autorizada antes de mayo de 2018, o cuenta con base jurídica, o consta en la lista de operaciones de tratamiento para las que no es necesaria una EIPD.

---

356 Alemania, Austria, Bélgica, Bulgaria, Eslovaquia, Estonia, Grecia, Finlandia, Francia, Hungría, Irlanda, Italia, Lituania, Letonia, Malta, Países Bajos, Polonia, Portugal, Reino Unido, República Checa, Rumanía y Suecia.

357 Todas están disponibles en el enlace que se indica en: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en

358 CEPD, Opinión 22/2018 sobre el borrador de la lista de la autoridad de supervisión competente del Reino Unido, relativa a las operaciones de tratamiento sujetas al requisito de estudio de Impacto de Protección de Datos (artículo 35.4 RGPD), adoptado el 25 de septiembre de 2018, disponible en: https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-opinion_2018_art._64_uk_sas_dpia_list_en.pdf

359 Directrices sobre la EIPD del GT29 (pie de página 315, anterior), contenido de la página, p. 6.

Las APD nacionales han emitido amplias directrices sobre las EIPD, incluyendo orientaciones metodológicas, incluyendo las de Francia, España y Reino Unido, así como la alemana Datenschutzzentrum (aprobada por la APD alemana).[360] La autoridad **francesa** de protección de datos, la CNIL, (en cooperación con otras APD) ha llegado a desarrollar una herramienta de software de código abierto de EIPD para «ayudar a los responsables de datos a desarrollar y mostrar cumplimiento normativo con el RGPD». Tal y como se explica en la página web:[361]

> **¿Quién puede utilizar el software EIP?**
> La herramienta está dirigida principalmente a responsables de datos que estén familiarizados con el proceso EIP. A este respecto, puede descargar y lanzar fácilmente en su ordenador una versión independiente.
> Además, es posible usar la herramienta en los servidores de una organización, para integrarla con otras herramientas y sistemas que ya se utilicen a nivel interno.
> **¿Qué es?**
> La herramienta EIP se ha diseñado en torno a tres principios:
>
> - **Interfaz didáctica para llevar a cabo la EIP:** la herramienta se basa en una interfaz de uso sencillo para el usuario que permite una gestión simple de sus EIP. Explica claramente la metodología de evaluación del impacto de privacidad, paso a paso. Varias herramientas de visualización proporcionan formas de entender rápidamente los riesgos.
> - **Base de conocimiento jurídico y técnico:** la herramienta incluye los puntos jurídicos que garantizan la licitud del tratamiento y los derechos de las partes interesadas. Además, cuenta con una base de conocimiento contextual, disponible en todos los pasos de la EIP, adaptando los contenidos que se muestran. Los datos se extraen del RGPD, las Directrices EIP y la Guía de Seguridad del CNIL, al aspecto del tratamiento estudiado.
> - **Herramienta modular:** diseñada para ayudarle a establecer su cumplimiento normativo, puede adaptar los contenidos de la herramienta para que se ajusten a las necesidades específicas o a su sector de negocios, por ejemplo creando un modelo EIP que pueda duplicar y utilizar para un conjunto de operaciones similares de tratamiento. Se publica bajo licencia libre, y es posible modificar el código fuente de la herramienta para añadir características o incluirlo en herramientas que se usen en su organización.

En este manual, no hay espacio para abordar todo el asesoramiento detallado sobre una EIPD que se proporciona en las directrices (aprobadas por el CEPD) del GT29 sobre EIPD, posterior y más específica, o en la normativa nacional: **se anima al lector a que estudie la guía GT29/CEPD en su totalidad, y el asesoramiento nacional relevante, cuando sea oportuno, y**

---

360 Ver la lista con enlaces en el *Anexo 1* a las Directrices sobre la EIPD del WT29 (pie de página 351, anterior). Las metodologías para las EIPD se analizan con más detalle más abajo, en dicho epígrafe.

361 Disponible, con más información en inglés, en:
https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment
El CNIL utiliza el acrónimo corto «PIA» (también en el citado texto anterior), probablemente porque las EIPD surgen de «Evaluaciones de impacto de privacidad». Tenga en cuenta que recientemente se ha actualizado la herramienta. Información sobre la actualización disponible aquí (solo en francés):
https://www.cnil.fr/fr/loutil-pia-mis-jour-pour-accompagner-lentree-en-application-du-rgpd
En esa página, el CNIL afirma que el software está disponible en 14 idiomas: francés, inglés, italiano, alemán, polaco, húngaro, finés, noruego, español, checo, neerlandés, portugués, rumano y griego, y que ha sido aprobado (al menos provisionalmente, en la versión beta) por las autoridades de protección de datos de Baviera, Italia, Finlandia, Hungría, Polonia y Noruega. No obstante, es necesario indicar que el software se centra principalmente en seguridad técnica, y será especialmente útil para PYMEs, más que para entidades grandes y complejas.

que se base en ellos en sus acciones y en todo asesoramiento que proporcione.[362]
El lector, y especialmente los DPD, también deben tener en cuenta la lista nacional obligatoria de una EIPD publicada por su respectiva APD, ya que dicha lista contiene ejemplos de situaciones en las que la aplicación de las orientaciones y consejos anteriores ha dado lugar a la prescripción de la realización de una EIPD por parte de entidades tanto públicas como privadas; se espera que los DPD supervisen la realización de una EIPD por parte de los respectivos responsables del tratamiento siempre que se les haya encomendado hacerlo sobre la base de dichas listas. Si se emiten asimismo «listas blancas» en los próximos meses (en virtud del artículo 35(5) del RGPD), estas serán también de gran ayuda, pues descartan la necesidad del responsable de realizar este ejercicio para un conjunto de actividades de tratamiento que no son de alto riesgo.
A continuación, apuntamos brevemente las directrices relativas a: **las distintas tareas y responsabilidades del responsable y del DPD**; la pregunta de **cómo evaluar si una operación de tratamiento propuesta puede dar lugar a un «alto riesgo»**; las **metodologías para la EIPD**, y **qué hacer con el registro de la EIPD**, en concreto, si se concluye que determinados altos riesgos identificados no podrán mitigarse con distintas medidas posibles, en cuyo caso el RGPD requiere que **se consulte a la APD correspondiente** (art. 36).

Las distintas Funciones y responsabilidades del responsable y del DPD en relación con la EIPD

En sus Normas sobre DPD, el GT29 recalcó de nuevo los diferentes funciones y responsabilidades del responsable y del DPD, también en relación con las EIPD. Establecía lo siguiente:[363]

> 4,2. La función del DPD en una evaluación de impacto de protección de datos
> En relación con el artículo 35(1), el responsable, y no el DPD, debe llevar a cabo, cuando sea necesario, un estudio de Impacto de Protección de Datos («EIPD»). No obstante, el DPD puede jugar un papel muy importante y útil para ayudar al responsable. Siguiendo el principio de protección de datos desde el diseño, el artículo 35(2) requiere, específicamente, que el responsable «*busque asesoramiento*» del DPD cuando realice una EIPD. A su vez, el artículo 39(1)(c), encomienda al DPD la Función de «*ofrecer asesoramiento cuando se requiera con respecto a la [EIPD] y supervisar su rendimiento*».
> El GT29 recomienda que el responsable busque el asesoramiento del DPD, sobre los asuntos siguientes, entre otros:[364]
>
> - Si llevar a cabo o no una EIPD
> - Qué metodología seguir cuando se lleve a cabo una EIPD
> - Si llevar a cabo la EIPD a nivel interno o si externalizar la Función
> - qué garantías (incluyendo medidas técnicas y organizativas) aplicar para mitigar los riesgos para los derechos e intereses de las partes interesadas

---

362 Ver las referencias en las notas al pie 249,318,351 y 353 y en la nota al pie anterior, para consultar el asesoramiento principal que haya que estudiar.

363 GT29 Normas sobre DPD (pie de página 242, anterior), sección 4.2, pp. 16 – 17, cursiva original, subrayado del último párrafo añadido.

364 El artículo 39(1) menciona las funciones del DPD e indica que el DPD tendrá, «al menos», las siguientes funciones. Por lo tanto, nada impide al responsable asignar al DPD otras Funciones distintas de las que se mencionan expresamente en el artículo 39(1), o de especificar dichas Funciones con más detalle. [pie de página original]

- Si se ha llevado a cabo adecuadamente la evaluación de impacto de protección de datos y si sus conclusiones (si debe seguirse adelante con el tratamiento y qué garantías se deben aplicar) cumplen con el RGPD.

Si el responsable no está de acuerdo con el asesoramiento que proporciona el DPD, la documentación de la EIPD debería justificar específicamente por escrito por qué no se ha tenido en cuenta este asesoramiento.[365]

El GT29 recomienda, asimismo, que el responsable defina claramente, por ejemplo en el contrato del DPD, pero también en información que se ofrezca a empleados, gestión (y otras partes interesadas, cuando corresponda), las funciones precisas del DPD y su alance, en especial con respecto a la realización de la EIPD.

Las últimas Normas sobre EIPD del GT29 indican que «el responsable, con el DPD y los encargados» deben realizar las EIPD.[366]

En la práctica, y especialmente en organizaciones más pequeñas, el DPD desempeña a menudo un papel destacado en la evaluación.

¿Cómo evaluar si una operación de tratamiento propuesta puede dar lugar a un «alto riesgo»?

El GT29/CEPB explica que:[367]

> La obligación de los responsables de realizar una EIPD en determinadas circunstancias debe entenderse ante el fondo de su obligación general de gestionar de forma adecuada los riesgos que presente el tratamiento de datos personales-

Es decir, decir, como también se indica más arriba, la cuestión de si debe realizarse una EIPD surge de manera natural de la obligación general del responsable, que se realiza con el «asesoramiento», pero en la práctica, en general, con el apoyo del DPD – para evaluar los riesgos inherentes a las operaciones de tratamiento de datos personales del responsable (Función 3, arriba mencionada).

Continúan aclarando el concepto de «riesgo» y los intereses protegidos que deben considerarse:[368]

> Un «riesgo» es un escenario que describa un evento y sus consecuencias, estimadas en términos de gravedad y probabilidad «Gestión del riesgo», por otro lado, puede definirse como las actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
>
> El artículo 35 hace referencia a un posible alto riesgo «para los derechos y libertades individuales». Tal y como se indica en el artículo 29 de la Declaración del Grupo de trabajo sobre Protección de Datos , sobre la función de un enfoque basado en riesgos en marcos legales de protección de datos, la referencia a «los derechos y libertades» de los interesados tiene que ver, principalmente, con los derechos a protección de datos y privacidad, pero puede involucrar, igualmente, otros derechos fundamentales, como libertad de expresión, de pensamiento, de movimiento, prohibición de discriminación, derecho a la libertad, conciencia y religión.

---

365 El artículo 24(1) indica que «*teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento*. ***Dichas medidas se revisarán y actualizarán cuando sea necesario*».** [Pie de página original, cursiva original]

366 Ver Normas sobre EIPD del GT29 (nota al pie 351, anterior), sección III.D.b).

367 *Idem*, p. 6.

368 *Idem*. Tener en cuenta, igualmente, la referencia anterior a ISO 31000:2009*, Gestión del riesgo — Principios y normas,* Organización Internacional de Normalización (ISO) ; ISO/IEC 29134 (proyecto), *Tecnología de la información – Técnicas de seguridad – Evaluación de impacto sobre la privacidad – Normas*, Organización Internacional de Normalización (ISO) (Directrices sobre EIPD del GT29, nota al pie 351, en p. 5).

El GT29 indica a los ejemplos del artículo 35(3) del RGPD de situaciones que entrañan de forma inherente «altos riesgos», mencionadas anteriormente: si un responsable utiliza algoritmos basado automatizados, basados en perfiles, sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar; si el responsable trata datos sensibles o datos sobre condenas penales «a gran escala»; o si el responsable realiza una «observación sistemática a gran escala» de una zona de acceso público Y con razón añade:[369]

> Como indican las palabras «en particular» de la frase introductoria del artículo 35(3) del RGPD, el significado es el de una lista no exhaustiva. Podrían existir operaciones de tratamiento de «alto riesgo» que no consten en esta lista, pero que entrañen altos riesgos similares. Dichas operaciones de tratamiento deben quedar también sujetas a EIPD.

El GT29 enumera un listado de factores, la mayoría de ellos, pero no todos, relativos a los tres ejemplos del artículo 35, que sugieren que una operación de tratamiento entraña «altos riesgos» y ofrece más ejemplos específicos. El SEPD proporciona ejemplos adicionales, tanto en su lista provisional de operaciones de tratamiento que siempre requerirán una EIPD, como en un formulario que podrá usarse para evaluar si las operaciones de tratamiento que no figuren ni en su lista «positiva» (operaciones que, en su opinión, requieran siempre una EIPD), ni en su lista «negativa» (las que, en su opinión no requieran una EIPD) deberán ser objeto de una EIPD.[370] Estos ejemplos del GT29 y del SEPD constan más abajo (algo redactado, con los ejemplos del GT29 eliminados del texto y trasladados al recuadro, y los ejemplos del SEPD indicados con un asterisco (*). Hemos adoptado algunos ejemplos adicionales (o más detalles o variaciones) de relevancia para los responsables del sector público en particular; dichos ejemplos, etc., se enumeran en cursiva.

Factores que indican «altos riesgos»[371]

1. Evaluación o puntuación, incluyendo elaboración de perfiles y predicción, especialmente a partir de «aspectos relativos al rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado» (considerandos 71 y 91).

Ejemplos:
Una institución financiera que investiga a sus clientes utilizando una base de datos de referencia de crédito o una base de datos de prevención de blanqueo de capitales y financiación del terrorismo (AML/CTF) o una base de datos de fraude.
Un banco que selecciona las transacciones de acuerdo con la ley aplicable para detectar posibles transacciones fraudulentas.*
Realización de perfiles de los miembros del personal basados en todas sus transacciones en el sistema de gestión de casos [*de la organización*] con reasignación automática de Funciones.*

---

369 *Idem*, p. 9.

370 Las listas positivas y negativas que se enumeran en el *Anexo 5* al SEPD Responsabilidad corporativa en el terreno (pie de página 353, anterior); el *Formulario de evaluación/criterios de umbral* se incluye en el *Anexo 6* de dicho documento.

371 Según se ha mencionado en las Directrices sobre la EIPD del GT29 (nota al pie 351, anterior), pp. 9 – 10. Los principales comentarios relativos a los factores también se extraen de dichas normas. Obsérvese que los factores se superponen de alguna manera o pueden combinarse, como se indica en los factores bajo el epígrafe «*Operaciones multifactoriales de alto riesgo*».

Una empresa de biotecnología que ofrece pruebas genéticas directamente a los consumidores con el fin de evaluar y predecir los riesgos de salud y de enfermedad.
Una empresa que crea perfiles de comportamiento o de marketing basados en el uso o la navegación en su sitio web.

2. Toma de decisiones automática con efectos significativos a nivel legal o similar: un tratamiento que está dirigido a tomar decisiones sobre partes interesadas que surtan «efectos jurídicos para las personas físicas» o que «les afecten significativamente de modo similar» (artículo 35(3)(a)), en particular (pero no solo) en casos en que el tratamiento pueda entrañar la exclusión o discriminación contra individuos.

Ejemplos:[372]
Valoración automatizada del personal («si usted se encuentra en el 10% inferior del equipo para el número de casos que se gestionen, recibirá un «insatisfactorio» en su evaluación, sin discusión).*
Identificación de defraudadores fiscales «posibles» o «probables», por medio de la atribución automática de perfiles a los contribuyentes.[373]
Identificación de defraudadores «posibles» o «probables», sobre la base de un perfil de defraudadores conocidos.
Identificación de niños «en riesgo» de crecer y desarrollar obesidad o miembros de bandas o criminales, o de niñas «con posibilidad» de quedarse embarazadas en su adolescencia, sobre la base de perfiles.[374]
Identificación de jóvenes y de adultos «en riesgo» de «radicalización».

3. Supervisión sistemática: tratamiento utilizado para supervisar, observar y controlar a interesados, incluyendo datos recogidos mediante redes, o «*supervisión sistemática de un área accesible al público*» (artículo 35(3)(c))15. Este tipo de seguimiento es un criterio porque los datos personales pueden recogerse en circunstancias en las que los interesados pueden no tener conocimiento de quién está recogiendo sus datos y cómo se utilizarán. Además, puede resultar imposible para las personas evitar ser sometidas a dicho tratamiento en espacios públicos (o de acceso público).

---

372 El GT29/CEPD añade que «el tratamiento con poco o ningún efecto sobre los individuos no se ajusta a este criterio específico. Se ofrecerán explicaciones adicionales sobre dichas nociones en las Normas sobre Perfilado del GT29. (p. 9).

373 Dichas atribuciones fueron realizadas en **Italia** por la Agencia Fiscal italiana, utilizando una herramienta denominada *Redditometro*. Los perfiles se basaban, entre otros, en gastos asumidos por los contribuyentes deducidos, según parámetros estadísticos, de su asignación en categorías familiares o áreas geográficas específicas. Esta herramienta de perfilado fue investigada por la APD italiana, la *Garante*. Uno de los principales problemas era la baja calidad de los datos y el elevado índice de error resultante, basado en inferencias poco fiables extraídas de los datos. Sobre la base de su investigación, el Garante prescribió que los ingresos reales de un contribuyente sólo podían calcularse a partir de gastos reales y documentados, y no deducirse de supuestos estadísticamente basados en los niveles de gastos. Ver: https://www.garanteprivacy.it/en/home/docweb/-/docweb-display/docweb/2765110

374 Ver Fundación de Reino Unido sobre Política de información (FIPR), Bases de datos de niños - Seguridad y privacidad, estudio para el Information Commissioner de Reino Unido, 2006, disponible en: https://www.cl.cam.ac.uk/~rja14/Papers/kids.pdf

Ejemplos:
Análisis del tráfico de internet que rompe el cifrado.*
CCTV encubiertas.*
CCTV inteligentes [*por ejemplo, que utilicen software de reconocimiento facial*] en espacios accesibles al público.*
Herramientas de prevención de pérdida de datos que rompan el cifrado SSL.*
tratamiento de metadatos (por ejemplo, tiempo, naturaleza y duración de una transacción en cuenta bancaria) para fines organizativos o para ofrecer presupuestos.[375]

4. Datos sensibles o de carácter muy personal: se incluyen las categorías especiales de datos personales definidas en el artículo 9 *(datos personales que revelen el origen racial o étnico, opiniones políticas, convicciones religiosas o filosóficas, pertenencia a un sindicato, datos sanitarios, genéticos o biométricos y datos sobre la orientación sexual*), así como los datos personales relativos a las condenas penales o delitos definidos en el artículo 10. Más allá de estas disposiciones del RGPD, se puede considerar que algunas categorías de datos aumentan el posible riesgo para los derechos y libertades de las personas. Estos datos personales se consideran sensibles (como se entiende comúnmente este término) porque están vinculados a actividades domésticas y privadas (*véase el tercer ejemplo, más adelante*), o porque afectan al ejercicio de un derecho fundamental (*véase el cuarto ejemplo*) o porque su violación implica claramente graves repercusiones en la vida diaria del interesado (*véase el quinto ejemplo*). A este respecto, puede ser relevante saber si los datos ya han sido puestos a disposición del público por el interesado o por terceros. El hecho de que los datos personales estén a disposición del público puede considerarse un factor en la evaluación, [*teniendo en cuenta si el interesado puede esperar razonablemente que los datos vayan a ser utilizados por otras personas para determinados fines: véase el séptimo ejemplo, a continuación*].

Ejemplos:
Un hospital general [*o una oficina de asistencia social*] que mantiene los registros médicos de los pacientes [*o de los solicitantes de asistencia social*].
Un investigador privado que conserve los detalles de las condenas o delitos penales, [*o una autoridad pública, como una institución educativa estatal, que conserve dichos datos en relación con los alumnos o estudiantes de dichas instituciones*].
[*Un organismo público o una entidad privada (como un empleador)*] que acceda a documentos personales, correos electrónicos, diarios o notas de lectores electrónicos equipados con funciones de toma de notas, propiedad de los miembros del personal [*o utilizados por el personal tanto para fines personales como profesionales, como en situaciones de «Traiga su propio dispositivo [BYOD]*»].
[*Un organismo público o una entidad privada (como un empleador)*] que acceda a información muy personal que incluyan las aplicaciones de registro de vida, *o que utilice información de medios sociales en contextos que pueden tener un impacto significativo sobre los individuos afectados, como la selección de personas para puestos de trabajo (o incluso entrevistas)*.
Exámenes médicos previos a la contratación y verificación de antecedentes penales.*
Investigaciones administrativas y procedimientos disciplinarios.*

[375] Este ejemplo se ha extraído de la lista EIPD **italiana** aprobada por el CEPD.

Cualquier uso de la identificación biométrica 1:n.*
Fotos que se utilicen con software de reconocimiento facial o que se empleen para inferir otros datos sensibles [*por ejemplo, cuando puedan entrañar discriminación en un contexto de selección*].*

5. Tratamiento de datos a gran escala: el RGPD no define qué constituye gran escala, pero el considerando 91 ofrece alguna orientación al respecto[376]. En cualquier caso, el GT29 recomienda que los siguientes factores, en particular, se tengan en cuenta a la hora de establecer si el tratamiento se lleva a cabo a gran escala:

   a. El número de interesados, ya sea como número específico o como proporción de la población correspondiente;

   b. El volumen de datos o el alcance de los distintos elementos de datos que se procesen;

   c. la duración, o permanencia, de la actividad de tratamiento de datos;

   d. El alcance geográfico de la actividad de tratamiento de datos.

Ejemplo:
Bases de datos sobre vigilancia de enfermedades *[a nivel nacional pero, a ser posible, vinculadas con la UE]*.*
Intercambios de datos a gran escala entre responsables del sector público (por ejemplo, Ministros, autoridades locales y regionales, etc.) por medio de redes electrónicas. [377]
La recogida a gran escala de información genealógica sobre familias de personas que son miembros de un grupo religioso particular.[378]
La creación de «bases de datos sobre estilo de vida» muy amplias con fines de marketing (pero que podrían, o, al menos, pueden) usarse también para otros fines).
El registro que realizan partidos políticos de la intención estimada de voto de amplios números de votantes (u hogares), a nivel nacional o de un país, sobre la base de entrevistas puerta a puerta, y su posterior análisis y uso de dichos datos.[379]

6. Comparación o combinación de conjuntos de datos, [*en especial si los mismos*] se originan a partir de dos o más operaciones de tratamiento de datos que se realicen para distintos fines o [*lleven a cabo*] por distintos responsables de datos de modo que pudiera exceder las expectativas razonables del interesado.

---

[376] La aclaración relativa del considerando 91 dice lo siguiente: "Las operaciones de tratamiento a gran escala[son operaciones] que tienen por objeto tratar una cantidad considerable de datos personales a escala regional, nacional o supranacional y que podrían afectar a un gran número de interesados y que pueden dar lugar a un alto riesgo, por ejemplo, debido a su sensibilidad,[o] cuando, de acuerdo con el estado alcanzado de los conocimientos tecnológicos, se utilice una nueva tecnología a gran escala…"

[377] Este ejemplo se ha extraído de la lista EIPD **italiana** aprobada por el CEPD.

[378] Ver la decisión de la APD francesa (el *CNIL*) sobre el registro genealógico mormón, emitido en 2013 y que puede consultarse aquí: https://www.nouvelobs.com/societe/20130613.OBS3162/les-mormons-autorises-par-la-cnil-a-numeriser-l-etat-civil-francais.html

[379] Esta práctica es habitual y, de hecho, es tradicional en Reino Unido, tal y como se reconoce en el considerando 56 del RGPD. Dicho considerando indica que «esto *podría* permitirse por motivos de interés público, *siempre y cuando se establezcan garantías adecuadas*» (cursiva añadida). En su caso, esta necesidad de evaluar si el tratamiento sirve, realmente, para un interés público legítimo y el requisito de adoptar «garantías adecuadas» remarcan la necesidad de un análisis del riesgo y una evaluación de impacto que sean rigurosos.

> **Ejemplo:**
> Verificación encubierta de acceso a registros de control, registros en ordenador y declaraciones de horario flexible [*por parte de un empleado*r] para detectar casos de absentismo.*
> *Una oficina de datos fiscales compara sus registros de declaraciones de impuestos con registros de titulares de yates caros, para buscar a personas que podrían estar cometiendo un fraude fiscal.*[380]

7. Los datos relativos a interesados vulnerables (considerando 75): el tratamiento de este tipo de datos es un criterio debido al aumento del desequilibrio de poder entre los interesados y el responsable de datos, lo que implica que los individuos podrían ser incapaces de aceptar u oponerse fácilmente al tratamiento de sus datos, o ejercitar sus derechos. Entre los interesados vulnerables pueden figurar los **niños** (se puede considerar que no pueden oponerse consciente y deliberadamente o consentir el tratamiento de sus datos), los **empleados**, segmentos más vulnerables de la población que requieren una protección especial (**enfermos mentales, solicitantes de asilo** o **personas mayores, pacientes**, etc.), y en todos los casos en que se pueda identificar un desequilibrio en la relación entre la posición del interesado y la del responsable del tratamiento.

> **Ejemplos:**
> Uso de sistemas de videovigilancia y geolocalización que permitan supervisar la distancia de las actividades de empleados.[381]
> Esencialmente, cualquier tratamiento de datos personales sobre cualquiera de las categorías de personas vulnerables antes mencionadas, y ciertamente cualquier tratamiento de datos sensibles sobre ellas, o el tratamiento a gran escala de dichos datos sobre esas personas, debe tratarse inherentemente como que puede dar lugar a un «alto riesgo».

8. Uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas. El RGPD aclara (artículo 35 (1) y considerandos 89 y 91) que el uso de una tecnología nueva, según se define de «acuerdo con el estado alcanzado de conocimientos tecnológicos» (considerando 91) podría entrañar la necesidad de llevar a cabo una EIPD. Esto es así porque el uso de dicha tecnología podría implicar formas o tipos innovadores de recogida y uso de los datos, posiblemente invisibles y con un alto riesgo para los derechos y libertades de los individuos. De hecho, las consecuencias personales y sociales de implantar una nueva tecnología podrían no ser conocidas. Una EIPD ayudará al responsable de los datos a comprender y abordar dichos riesgos – y las medidas atenuantes deberían hacer posible que los interesados y el público general vean cómo y cuándo y para qué fines se van a usar las nuevas tecnologías, de modo que puedan protegerse frente a aquellas que atenten contra derechos y libertades

---

380 Esto se hizo, hace algún tiempo, en Países Bajos, asumiendo que los defraudadores de impuestos eran los principales compradores de yates grandes. Una persona, que se sentía en el centro de la diana, llamó a su barco «Dinero negro».

381 Este ejemplo se ha extraído de la lista EIPD **italiana** aprobada por el CEPD.

individuales y conlleven un gobierno autoritario o vigilancia en masa por parte de corporaciones (o si actúan en conjunto).

Nota: En muchos de estos casos de nuevas tecnologías o prácticas, las APD (o el CEPD) pueden emitir, o pueden haber emitido ya, dictámenes, directrices o recomendaciones, y los DPD deben estar alerta para estar atentos a estos nuevos documentos. Si consideran que todavía no se ha publicado ninguna orientación pertinente, etc., deben consultar a su APD. Ver también las Funciones 4, 8 y 10 siguientes.

Ejemplos:
El uso combinado de huellas digitales y reconocimiento facial para un mejor control de acceso físico.[382]
Nuevas tecnologías destinadas a controlar el tiempo y la asistencia de los empleados, incluidas las que procesan datos biométricos, así como otras, como el seguimiento de dispositivos móviles.[383]
Tratamiento de datos generados por el uso de aplicaciones del «Internet de las cosas» (dispositivos y cosas conectadas e «inteligentes») si el uso de datos tiene (o puede tener) un impacto significativo en la vida diaria y la privacidad de los individuos.
Aprendizaje automático.*
Coches conectados.*
Examinar redes sociales de los solicitantes de puestos.*

9. Cuando el propio tratamiento «i*mpida a los interesados ejercer un derecho o utilizar un servicio o ejecutar un contrato*» (artículo 22 y considerando 91). Esto incluye operaciones de tratamiento destinadas a permitir, modificar o rechazar el acceso de los interesados a un servicio, o su formalización de contratos.

Ejemplos:
Un banco compara a sus clientes con una base de datos de referencia de crédito para decidir si les concede un préstamo.
Una institución financiera o agencia de referencia de crédito que tiene en cuenta la diferencia de edad entre los cónyuges en un matrimonio para determinar la solvencia (lo que puede impedir el libre ejercicio del derecho fundamental al matrimonio, y que, por lo tanto, fue prohibida en Francia por la APD francesa, la CNIL (que tuvo que evaluar el sistema porque, al tomar decisiones basadas en perfiles, estaba sujeta a una «autorización previa» por parte de la CNIL).
Bases de datos de exclusión.*
Verificación del crédito.*

Operaciones multifactoriales de alto riesgo

Los factores que se enumeran más arriba pueden solaparse o combinarse, por ejemplo, «supervisión sistemática» puede solaparse con, y combinarse con, toma de decisiones automática basada en perfiles, y puede implicar un tratamiento de «datos sensibles» a «gran

---

382 El GT29 y muchas APD nacionales han indicado de forma detallada que esto requiere, entre otros asuntos, que los datos biológicos se almacenen en el chip de micro-procesamiento en el dispositivo del interesado, y no en los archivos centrales del responsable. Ver: GT29 Documento de trabajo sobre biometría (GT80, adoptado el 1 de agosto de 2003), p. 6, disponible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf

383 Ver Opinión 2/2017 sobre tratamiento de datos en el trabajo del GT29 (GT249, adoptado el 8 de junio de 2017), sección 5.5, *Operaciones de tratamiento relativas al tiempo y la asistencia*, en pp. 18 – 19, disponibles en: www.ec.europa.eu/newsroom/document.cfm?doc_id=45631

escala». El GT29 proporciona una serie de ejemplos de operaciones con tales factores (o criterios) combinados para las que se requiere una EIPD, y ejemplos de operaciones en las que uno o más de los factores (o criterios) anteriores están presentes, pero en las que no se necesita una EIPD, del siguiente modo:[384]

Ejemplos de tratamiento	**Posibles criterios relevantes**	**¿Es probable que se requiera una EIPD?**
Un hospital que trata datos genéticos y de salud de sus pacientes (sistema de información hospitalaria).	- Datos sensibles o datos de naturaleza personal. - Datos relativos a interesados vulnerables. - Datos procesados a gran escala.	Sí
El uso de un sistema de cámaras para controlar el comportamiento de conducción en las carreteras. El responsable prevé utilizar un sistema de análisis de vídeo inteligente para identificar los coches y reconocer automáticamente las matrículas.	- Supervisión sistemática. - Uso innovador o aplicación de soluciones tecnológicas u organizativas.	
Una empresa controla sistemáticamente las actividades de sus empleados, incluyendo el control del puesto de trabajo de los empleados, la actividad en Internet, etc.	- Supervisión sistemática. - Datos relativos a interesados vulnerables.	
Recopilación de datos de redes sociales públicas para la generación de perfiles.	- Evaluación o puntuación. - Datos procesados a gran escala. - Coincidencia o combinación de conjuntos de datos. - Datos sensibles o de carácter muy personal:	
Una institución que crea una base de datos de calificación crediticia o de fraude a nivel nacional.	- Evaluación o puntuación. - Toma de decisiones automatizada con efectos legales o similares. - Impide que los interesados ejerzan un derecho o utilicen un servicio o un contrato. - Datos sensibles o de carácter muy personal:	
Almacenamiento con fines de archivo de datos personales confidenciales seudónimos relativos a sujetos de datos vulnerables de proyectos de investigación o ensayos clínicos.	- Datos sensibles. - Datos relativos a interesados vulnerables. - Impide que los interesados ejerzan un derecho o utilicen un servicio o	

384 Directrices sobre EIPD del GT29 (nota al pie 351, anterior), 11– 12.

	un contrato.	
El tratamiento de «datos personales de pacientes o de clientes por parte de un médico individual, de otro profesional sanitario o de un abogado» (Considerando 91).	- Datos sensibles o de carácter muy personal. - Datos relativos a interesados vulnerables.	No
Una revista online que utiliza una lista de correo para enviar un resumen diario genérico a sus suscriptores con su consentimiento, y que incluye un medio fácil para optar por no recibir más correos.	- Datos procesados a gran escala.	
Un sitio web de comercio electrónico que muestra anuncios de piezas de coches de época y que implica perfilado limitado basado en artículos vistos o comprados en su propio sitio web, de nuevo con una opción sencilla de baja voluntaria.	- Evaluación o puntuación.	

Metodología para EIPD:

Los objetivos de una EIPD son:

(i) **Identificar** de forma precisa los (altos) riesgos que implica la operación propuesta de tratamiento, teniendo en cuenta la naturaleza de los datos y el tratamiento, el alcance, contexto y fines del tratamiento y las fuentes del riesgo – no solo en circunstancias normales, sino también en circunstancias especiales; y a corto, medio y largo plazo;[385]

(ii) **evaluar** los riesgos identificados (altos), en particular su origen, naturaleza y particularidad, así como la probabilidad y posible gravedad del riesgo[386];

(iii) determinar qué **medidas** pueden adoptarse para mitigar los riesgos (altos) que sean adecuadas en términos de tecnología disponible y de costes de aplicación, y proponer dichas medidas;[387] y

(iv) **registrar** los resultados, la evaluación y las medidas adoptadas (o no adoptadas, con los motivos para ello), para poder «**demostrar el cumplimiento**» de los requisitos del RGPD, en virtud del principio de «responsabilidad corporativa» en relación con el tratamiento evaluado.[388]

El artículo 35(7) del RGPD estipula que (el registro de) una EIPD debe incluir, «como mínimo», lo siguiente:

a) una descripción sistemática de los tratamientos previstos y de los fines del tratamiento, incluido, en su caso, el interés legítimo que persiga el responsable del tratamiento;

---

385 Ver considerando 90.

386 Ver considerando 84 y norma ISO 31000.

387 Ver considerando 84.

388 Como indica el GT29: «*[Una] EIPD es un proceso para construir y demostrar el cumplimiento normativo*.» – Directrices sobre EIPD del GT29 (nota al pie 351, anterior), p. 4. Para más información sobre el principio de responsabilidad corporativa y las funciones vinculadas sobre «demostración de cumplimiento normativo», ver Parte 2 del manual.

b) una evaluación de la necesidad y proporcionalidad de los tratamientos en relación con los fines perseguidos;
c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y
d) las medidas previstas para hacer frente a los riesgos, incluidas las garantías, las medidas de seguridad y los mecanismos para garantizar la protección de los datos personales y demostrar el cumplimiento normativo con lo previsto presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

El GT29 hace hincapié en que:[389]

> Todos los requisitos pertinentes establecidos en el RGPD proporcionan un marco amplio y genérico para diseñar y llevar a cabo una EIPD. La aplicación práctica de una EIPD dependerá de los requisitos establecidos en el RGPD, que puede complementarse con una orientación práctica más detallada. **Por lo tanto, la implementación de la EIPD es aplicable a distintas escalas. Esto significa que incluso un responsable de datos de menor entidad puede diseñar e implementar una EIPD que sea adecuada para sus operaciones de tratamiento.**

Por lo tanto, los responsables del tratamiento pueden (en consulta a su DPD) elegir una metodología para cualquier EIPD que tengan que llevar a cabo que les convenga. Pueden aprovechar cualquier experiencia que puedan tener con evaluaciones de riesgos más técnicas, por ejemplo, de conformidad con la norma ISO 31000. Sin embargo, el GT29 señala acertadamente la diferente perspectiva desde la cual se deben llevar a cabo las EIPD bajo el RGPD y las evaluaciones basadas en ISO (en cualquier caso, más orientadas a la seguridad)[390]:

> La EIPD en virtud del RGPD es una herramienta para la gestión de riesgos sobre los derechos de los interesados, y así tener en cuenta su perspectiva [es decir, de los interesados]... Al contrario, la gestión del riesgo en otros ámbitos (por ejemplo, seguridad de la información) está enfocada en los riesgos a la organización.

El GT29 ofrece varios ejemplos sobre metodologías de protección de datos e impacto sobre la privacidad preparadas por las APD nacionales,[391] y «*anima al desarrollo de marcos EIPD específicos para el sector*». Ha publicado un Marco de EIPD para Solicitudes de RFID y una Plantilla de EIPD para sistemas de redes inteligentes y medición inteligente.[392]

En este caso, bastará con reproducir los Criterios para una EIPD aceptable, que constan en las Directrices del GT29:[393]

> ## Anexo 2 – Criterios para una EIPD aceptable
>
> El GT29 ofrece los siguientes criterios que pueden usar los responsables de datos para evaluar si una EIPD, o metodología para ejecutar una EIPD, es lo suficientemente global o no para cumplir con el RGPD:
>
> - **Se ofrece una descripción sistemática del tratamiento** (artículo 35(7)(a))**:**
>
> - Se tienen en cuenta la naturaleza, el alcance y los fines del tratamiento (Considerando 90);

---

389 Directrices sobre EIPD del GT29 (pie de página 351, arriba), p. 17, subrayado añadido.
390 Idem
391 Ver, de nuevo, la lista con enlaces en el *Anexo 1* a las Directrices sobre EIPD del GT29 (pie de página 351, anterior).
392 *Idem*, notas al pie 32 y 33.
393 *Idem*, anexo 2. La negrita en los puntos principales se ha añadido con efectos aclaratorios.

- se registran los datos personales, los destinatarios y el período durante el cual se almacenarán los datos personales;
- se proporciona una descripción funcional de la operación de tratamiento;
- se identifican los activos de los que dependen los datos personales (hardware, software, redes, personas, canales de transmisión en papel o en papel);
- se tiene en cuenta el cumplimiento de los códigos de conducta aprobados [*, certificaciones y/o BCR*][394] (apartado 8 del artículo 35);

- **<u>se evalúa la necesidad y la proporcionalidad</u>** (artículo 35(7)(b))**:**

- Se establecen medidas para cumplir con el Reglamento (artículo 35(7)(d) y considerando 90), teniendo en cuenta:
  - Medidas que contribuyan a la proporcionalidad y a la necesidad del tratamiento, sobre la base de:
    - Fin(es) específico, explícito y legítimo(s) (artículo 5(1)(b));
    - legalidad del tratamiento (artículo 6);
    - adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (artículo 5(1)(c));
    - límite de almacenamiento (artículo 5(1)(e));
  - Medidas que contribuyan a los derechos de los interesados:
    - Información proporcionada al interesado (artículos 12, 13 y 14);
    - Derecho de acceso y a la portabilidad de los datos (artículos 15 y 20);
    - Derecho a la rectificación y a la eliminación (artículos 16, 17 y 19);
    - Derecho de oposición y limitación del tratamiento (artículos 18, 19 y 21);
    - Relaciones con el encargado del tratamiento (artículo 28);
    - Garantías sobre transferencia(s) internacional(es) (capítulo V);
    - Consulta previa (artículo 36).

- **Gestión de los riesgos para los derechos y libertades de los interesados (artículo 35(7)(c)):**

- Se evalúa el origen, naturaleza, particularidad y gravedad de dicho riesgo (ver considerando 84) o, de forma más específica, para cada riesgo (acceso ilegítimo, modificación no deseada y desaparición de datos) desde la perspectiva de los interesados:
  - También se tienen en cuenta las fuentes del riesgo (considerando 90);
  - Se identifica el potencial impacto a los derechos y libertades de los interesados en caso de eventos que incluyen el acceso ilegítimo, la modificación no deseada y la desaparición de datos;

---

[394] El GP29 señala anteriormente que:
"El cumplimiento de un código de conducta (artículo 40) debe tenerse en cuenta (apartado 8 del artículo 35) al evaluar el impacto de una operación de tratamiento de datos. Esto puede ser útil para demostrar que se han elegido o establecido medidas adecuadas, siempre que el código de conducta sea adecuado para la operación de tratamiento. También deben tenerse en cuenta las certificaciones, sellos y marcas que demuestren que los controladores y procesadores cumplen con el RGPD de las operaciones de procesamiento (Artículo 42), así como las Normas Corporativas Vinculantes (BCR)".
GP29 Directrices sobre las EPD (nota 351, arriba mencionado), pág. 16.

- se identifiquen las amenazas que puedan dar lugar a un acceso ilegítimo, a una modificación no deseada y a la desaparición de los datos;
- Se valoran la particular gravedad y probabilidad (considerando 90);

- se establecen medidas para tratar dichos riesgos (artículo 35(7)(d) y considerando 90);

- **hay interesados involucrados:**

- Se recaba el asesoramiento del delegado de protección de datos (artículo 35(2));
- se recaba la opinión de los interesados o de sus representantes, cuando sea necesario (artículo 35(9)).

¿Qué hacer con el registro de la EIPD?

El primer y principal objetivo del registro de la EIPD (que cubre todos los «criterios» antes mencionados) es tener **evidencia** de que se ha llevado a cabo una EIPD adecuada y en profundidad, de acuerdo con el RGPD (es decir, cumplir con los criterios anteriores).
Si la EIPD identifica al mismo tiempo tanto los riesgos (altos) como las medidas que pueden tomarse para abordar esos riesgos que son «apropiados» teniendo en cuenta la probabilidad y la gravedad de los riesgos y los costes de las medidas, y cuando tales medidas hayan sido efectivamente aprobadas y adoptadas (y esta aprobación y adopción también ha sido registrada), el registro de la DPIA puede proporcionar **un "elemento" importante en una demostración general de cumplimiento** y un "medio especial" para hacerlo (aunque esto no equivale a una presunción legal de cumplimiento, y aunque el RPD todavía tendrá que **comprobar y supervisar**, de forma continua, que las medidas atenuantes continúan aplicándose y siguen siendo adecuadas a la luz de la evolución práctica, organizativa o tecnológica: ver en esta Función, bajo el epígrafe «*Supervisión continua del cumplimiento*»)

Ejemplos de casos en los que la EIPD identificó tanto los altos riesgos como las medidas atenuantes, que (en este caso, EuroPrise) consideró suficientes para permitir el tratamiento. Por consiguiente, ambos casos permitirían al responsable del tratamiento llegar a la conclusión confidencial de que el resultado de la EIPD muestra que el tratamiento NO tendría que someterse a la APD competente para su consulta:[395]

1. Una agencia de bienestar utiliza autenticación biométrica por voz para la lucha contra el fraude.
Identificación de riesgos: Tal y como ha señalado el GT29, tres de los principales riesgos que entraña el uso de los datos biométricos son: i) el hecho de que las características biométricas de una persona sean irremplazables (lo que significa que una herramienta de autenticación basada en datos biométricos brutos, una vez perdidos, no puede sustituirse); ii) la facilidad con la que pueden utilizarse los datos biométricos para cotejar diferentes conjuntos de datos; y iii) la posibilidad de que los datos biométricos puedan capturarse de forma subrepticia.
Medidas atenuantes: En una herramienta de autenticación biométrica (de voz), utilizada para contrarrestar el fraude al bienestar, se utiliza una plantilla de voz única, creada a partir de los datos

[395] Estos ejemplos han sido tomados de productos que han obtenido el Sello Europeo de Privacidad, y sus evaluaciones legales fueron realizadas por Douwe Korff, ver, respectivamente:
https://www.european-privacy-seal.eu/EPS-en/4F-self-certification (herramienta de autenticación de cuatro factores que incluya una solución biométrica por voz);
https://www.european-privacy-seal.eu/eps-en/valid-pos (se trata de una herramienta que compara la ubicación de una transacción con tarjeta bancaria sospechosa con la ubicación (aproximada) del teléfono móvil del titular de la tarjeta.
En las evaluaciones, ambos productos fueron elogiados por su amplia minimización de datos y características de privacidad por diseño, y por la forma en que atenuaron los riesgos asociados, respectivamente, con el uso de datos biométricos y la verificación de la ubicación.

biométricos originales («brutos»), en lugar de los datos brutos, que se destruyen tras el registro de los interesados. La plantilla de voz es única para cualquier despliegue específico y no puede utilizarse para volver a crear los datos biométricos originales (en bruto). Con ello se abordan los tres riesgos antes mencionados: (i) si la plantilla de voz se viera comprometida, se puede crear una nueva y diferente de forma muy sencilla (con ayuda del interesado, que tendría que volver a inscribirse); (ii) las diferentes plantillas de voz utilizadas en los distintos usos de la misma herramienta no se pueden comparar entre sí o con otras plantillas de voz o datos de voz; y (iii) la plantilla de voz se crea en un proceso de inscripción cara a cara-

2. Una institución financiera verifica la ubicación del teléfono móvil de un cliente para ver si está (aproximadamente) en el mismo lugar que la tarjeta bancaria del cliente (que se está utilizando para una transacción que ha sido marcada como sospechosa).

Identificación de riesgos: Los datos precisos de la ubicación de alguien en un momento concreto pueden ser un asunto sensible, y la comunicación de dichos datos constituye, por tanto, una interferencia seria con la privacidad y la vida privada del correspondiente individuo, tal y como confirmó el Tribunal Europeo de Derechos Humanos en el caso *Naomi Campbell* .

Medidas atenuantes: En la herramienta de prevención del fraude con tarjetas bancarias, los datos de localización del teléfono móvil se reducen, incluso antes de ser transmitidos al usuario de esa herramienta (la institución financiera), a una zona muy accidentada, típicamente un país o un estado. Esto es suficiente para que la herramienta funcione de forma eficaz (es decir, para poder determinar con suficiente certeza si la transacción en cuestión es auténtica o fraudulenta), al tiempo que se reduce al mínimo indispensable la intrusión de la verificación de la ubicación.

El registro también puede ponerse a disposición (o aprovecharse) en **consultas** en las que participen partes o ciudadanos interesados, o en respuestas a **consultas y reclamaciones de los interesados y de organizaciones no gubernamentales** que representen a los interesados (o a la prensa). A este respecto, el GT29 apunta que:[396]

> **La publicación de una EIPD no es un requisito legal del RGPD, la decisión de publicarlo corresponde al responsable. No obstante, los responsables deberán considerar si publican, al menos, algunas partes, como el sumario o una conclusión de su EIPD.**
> El fin de dicho proceso sería ayudar a fomentar la confianza en las operaciones de tratamiento del responsable, y demostrar responsabilidad corporativa y transparencia.
> ***La publicación de una EIPD es, especialmente, una buena práctica, si una operación de tratamiento afectara al público. Esto podría ser, especialmente, el caso, si una administración pública lleva a cabo una EIPD.***
>
> La EIPD publicada no tiene que incluir la evaluación completa, especialmente si la EIPD pudiera presentar información específica relativa a los riesgos de seguridad para el responsable de los datos o distribuir secretos comerciales o información comercial sensible. En esas circunstancias, la versión publicada podría consistir en tan solo un resumen de los resultados principales de la EIPD, o incluso tan solo una declaración de que se ha llevado a cabo una EIPD.

El registro de la EIPD será de especial relevancia a la hora de tramitar cualquier cuestión de las APD, tanto si actúan en su capacidad general de supervisión o en respuesta a una queja.

De forma más específica, si una EIPD identifica, al mismo tiempo, riesgos (altos) y concluye que **no** puede adoptarse medida alguna para abordar de forma suficiente todos esos riesgos (o, al menos, que no existen medidas «adecuadas», teniendo en cuenta la probabilidad y la gravedad de los riesgos y el coste de las medidas), el responsable deberá **consultar con la APD**

---

396 Directrices sobre EIPD del GT29 (nota al pie 351, anterior) p. 18, negrita en el original, cursiva y negrita añadidas.

(art. 36) – y **deberá enviarse a la APD el registro de la EIPD correspondiente:**[397]

> Si una EIPD revela un alto riesgo residual, el responsable consultará a la autoridad de control antes de proceder al tratamiento (artículo 36(1)). Como parte de ello, deberá facilitarse la EIPD completa (artículo 36(3)(e). La autoridad de supervisión podrá prestar su asesoramiento,[398] y no comprometerá secretos comerciales ni revelará vulnerabilidades secretas, con arreglo a los principios que sean de aplicación en cada Estado Miembro sobre acceso público a documentos oficiales.

El **Derecho de los Estados miembros** podrá obligar a los responsables del tratamiento a consultar a la autoridad de control «en relación con el tratamiento por un responsable en el ejercicio de una misión realizada en interés público, en particular el tratamiento en relación con la protección social y la salud pública» (art. 36(5)), y esto se ha realizado para esos últimos casos en, por ejemplo, Francia e Italia.

Si la APD no quedara satisfecha con la información registrada en la EIPD (o proporcionada de otro modo), la APD podrá **ordenar** al responsable que facilite cualquier información necesaria para el desempeño de sus funciones (ver art. 58(1)(a)).

Normalmente, la APD tratará de ayudar al responsable a encontrar una solución, por ejemplo, identificar medidas que podrían mitigar adecuadamente los (altos) riesgos identificados (en opinión de la APD), y siempre que el responsable acepte adoptar dichas medidas (y que su adopción y uso continuado sean verificados y controlados por el DPD), que resolvieran el asunto (como debería registrar el DPD y que, desde luego, registrará la APD).

No obstante, de forma alternativa, la APD podrá bien emitir una **orden** al responsable, donde le requiera la adopción de medidas específicas para la operación de tratamiento propuesta (ver art. 58(2)(D)), o bien **prohibir** el tratamiento propuesto (art. 58(2)(f)).

El DPD deberá, de nuevo, registrar dichas órdenes, y comprobar de forma continua que se cumplan (y registrar sus conclusiones). Aun así, como siempre, además de realizar dicha verificación, control y registro, el responsable será finalmente quien deberá responder por cualquier error de cumplimiento.

- o – O – o –

---

397 *Ídem*.

398 Solo será necesario el asesoramiento por escrito cuando la autoridad de supervisión opine que el tratamiento que se pretende proporcionar no se alinea con la normativa prevista en el artículo 36(2). [pie de página original]

Supervisión del cumplimiento normativo (incluyendo investigaciones de denuncias):

FUNCIÓN 5: Repetición de las Funciones 1 – 3 (y 4) de forma continua

Tal y como indica el GT29 en sus Directrices sobre DPD, el artículo 39(1)(b) confía al DPD, entre otras funciones, la de «supervisar el cumplimiento» de su organización con el RGPD, y el considerando 97 especifica, además, que el DPD «debe ayudar al responsable o al encargado a supervisar el cumplimiento normativo interno del presente Reglamento».[399] Como indica el término «supervisar», no se trata de una responsabilidad puntual, sino continua.

No obstante, en línea con nuestros comentarios sobre el papel del DPD en la Parte 2, sección 2.3.4, anterior, el GT29 recalcó (de nuevo) que esto:[400]

> No implica que el DPD sea responsable personalmente en caso de incumplimiento. El RGPD deja claro que corresponde al responsables, y no al DPD, «*implantar medidas técnicas y organizativas adecuadas para garantizar y ser capaces de demostrar que el tratamiento se realice de acuerdo con el presente Reglamento»* (artículo 24(1)). El cumplimiento normativo de protección de datos es una responsabilidad corporativa del responsable de los datos, no del DPD.

El GT29 continúa diciendo que, como parte de dichas funciones de control del cumplimiento normativo, el DPD podrá, en particular, de forma continua:

- Recoger información para identificar las actividades de tratamiento,
- Analizar y verificar el cumplimiento normativo de las actividades de tratamiento, e
- Informar, asesorar y emitir recomendaciones al responsable o al encargado.

Tal y como indica en relación con las EIPD (Función 4):[401]

> Debe remarcarse que para poder gestionar los riesgos para los derechos y las libertades de las personas físicas, los riesgos deben identificarse, analizarse, evaluarse, estimarse, tratarse (por ejemplo, con medidas atenuantes...) **y revisarse periódicamente**.

En otras palabras, las Funciones 1 – 4, arriba mencionadas (o, si no hubiera operaciones probables «de alto riesgo», las Funciones 1 – 3), deben repetirse de forma continua y, especialmente, sin duda, si la organización modificara cualquier operación de tratamiento de datos personales, o implantara otras nuevas. Tal y como indica el SEPD (en su asesoramiento a los DPD institucionales de la UE):[402]

> Sus registros deben reflejar la realidad de las operaciones de tratamiento de su institución. Esto significa que deberá asegurar que están actualizadas. Si [su institución] planea realizar cambios en sus operaciones de tratamiento, compruebe si el registro debe ser actualizado. Es una buena idea incluir formalmente esta verificación en su proceso de gestión de cambios. También puede ser una buena idea realizar revisiones

---

399 Directrices sobre DPD del GT29 (nota al pie 242, anterior), sección 4.1, *Supervisión del cumplimiento normativo del RGPD* en p. 16,7.

400 *Ídem*, cursiva en el original.

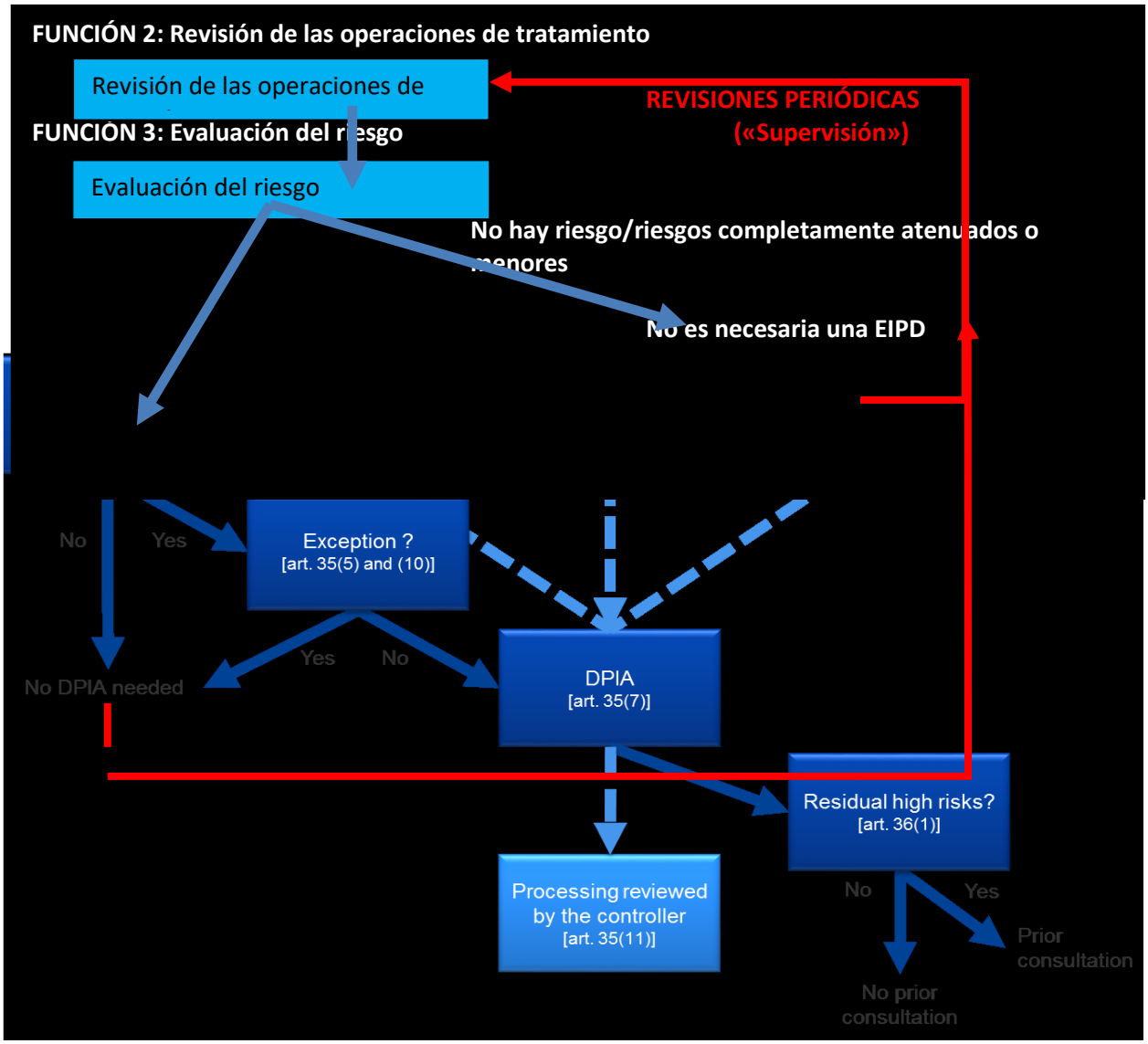
401 Directrices sobre EIPD del GT29 (nota al pie 351, anterior), nota al pie 10 en p. 6, se ha añadido el subrayado.

402 SEPD, Responsabilidad corporativa sobre el terreno (nota al pie 353, anterior).

regulares independientemente de los cambios planificados para detectar cambios que puedan haber pasado desapercibidos.

El GT29 ha ilustrado la última parte de esta secuencia con un diagrama útil, reproducido al dorso, con las etapas anteriores (Funciones 2 y 3) añadidas.

Diagrama del GT29 sobre los pasos que es necesario seguir en relación con la EIPD,[403] cuyos pasos previos (Funciones 2 y 3) se han añadido en el recuadro superior:



Nota: Las excepciones previstas en el art. 35(5), que figuran en el diagrama del GT29, se refieren a seguridad nacional, defensa, prevención de la delincuencia, etc., el art. 35(10) hace referencia a la estipulación de que no se requiere una EIPD en relación con el tratamiento regulado por ley, si se ha llevado a cabo una EIPD general de dicho tratamiento en el período previo a la entrada en vigor de la ley (en el que no participa el DPD).

Como parte de sus funciones de «supervisión del cumplimiento», el DPD también deberá asegurarse de que conoce cualquier cambio en el marco reglamentario y contractual (etc.) en el que opera su organización, tal y como se contempla en la Función preliminar (Función 0), de modo que pueda identificar el impacto de dichos cambios en las operaciones de tratamiento de datos personales de su organización (la legalidad actual y el cumplimiento de los requisitos

403 Directrices sobre las EIPD del GT29 (nota al pie 351 mencionada arriba), p. 7.

del RGPD), y asesore adecuadamente a las personas pertinentes de su organización (incluida la alta dirección, si procede).

De hecho, el DPD debería, en su caso, junto con otros DPD de su red y/o con la APD, y en consulta a su alta dirección, estar dispuesto, en ocasiones, a adoptar posiciones y puntos de vista sobre los cambios propuestos o sugeridos en este marco, tales como las propuestas de un gobierno de que se exija, permita o anime a organizaciones como la suya a compartir determinados datos personales para nuevos fines.

- o – O – o –

FUNCIÓN 6: Gestionar violaciones de la seguridad de datos personales

Dos de las principales e importantes innovaciones que plantea el RGPD en comparación con la Directiva de Protección de Datos de 1995 son (i) un requisito general de notificar a la APD pertinente (es decir, «competente») cualquier violación de los datos personales que pueda suponer un riesgo para los derechos y libertades de las personas; y (ii) un deber de informar a los interesados de tales violaciones en los casos en que la violación pueda suponer un "alto riesgo" para los derechos y libertades de las personas físicas.

El Grupo de trabajo del artículo 29 ha emitido directrices detalladas sobre cómo deben tratarse;[404] y dichas directrices fueron aprobadas por el Comité Europeo de Protección de Datos en su primera reunión.[405] El debate que se desarrolla a continuación se basará en gran medida en estas directrices y remitirá a ellas. Los ejemplos proporcionados también se han extraído de estas Directrices del GT29.[406]

Notificar a la APD correspondiente:

La idea de notificar las violaciones de datos personales no es nueva. Tal y como se indica en la sección 1.3.3, anterior,[407] ya se incluía en la Directiva de Privacidad un deber de notificación de violación de datos personales. No obstante, ese deber se limitaba a proveedores de redes y servicios de comunicaciones electrónicas.[408] El RGPD utiliza la misma definición de «violación de datos personales» que se incluye en la Directiva sobre Privacidad electrónica, pero sin esta limitación:

> toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. (Art. 4(12))[409]

Las Directrices del GT29 aclaran, con cierto grado de detalle, qué términos relevantes deberían escogerse como significado, e indica los distintos tipos de violaciones de datos personales («violación de confidencialidad»; «violación de integridad»; «violación de disponibilidad»)[410]

Ejemplos
Un ejemplo de pérdida de datos personales puede incluir el caso de pérdida o robo de un dispositivo que contenga una copia de la base de datos de clientes de un responsable. Otro ejemplo de pérdida puede darse cuando la única copia de un conjunto de datos personales ha sido encriptada por ransomware (programa informático malicioso que encripta los datos del responsable hasta que se paga el rescate), o ha sido encriptada por el responsable utilizando una clave que ya no está en su poder.
Entre los ejemplos de pérdida de disponibilidad se incluyen los casos en que los datos

---

404 Directrices sobre notificación de violaciones de datos personales, según lo dispuesto en el Reglamento 2016/679 del GT29 (GT250 rev.01, adoptado el 3 de octubre de 2017, según su última revisión y adopción el 6 de febrero de 2018 (en adelante: «Directrices sobre notificación de violaciones de datos del GT29 o, en este apartado, sencillamente «las Directrices del GT29»), disponibles en: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

405 Ver nota al pie 248 anterior.

407 En el sub-apartado sobre «*Elementos clave del Reglamento sobre Privacidad electrónica*», en el sub-epígrafe «Notificación de brechas de seguridad».

408 Tal y como se indica en las Directrices del GT29 en la Introducción, determinados Estados Miembro ya contaban con requisitos mayores de notificación de brechas de seguridad.

409 La Directiva sobre Privacidad electrónica añadía, tras esas palabras, lo siguiente: «en relación con la prestación de un servicio de comunicaciones electrónicas de acceso público en la Comunidad» (art. 2(i)).

410 Directrices del GT29, p. 7, con referencia a una Opinión anterior del GT29 (2014) sobre notificación de brechas de seguridad.

han sido borrados accidentalmente o por una persona no autorizada o, en el ejemplo de los datos cifrados de forma segura, la clave de descifrado se ha perdido. En el caso de que el responsable no pudiera restaurar el acceso a los datos, por ejemplo, a partir de una copia de seguridad, esto se considera una pérdida permanente de disponibilidad. También puede producirse una pérdida de disponibilidad cuando se haya producido una interrupción significativa del servicio normal de una organización, por ejemplo, cuando se produce un fallo en el suministro eléctrico o un ataque de denegación de servicio que haga que los datos personales no estén disponibles.

Incluso una pérdida temporal de disponibilidad podrá constituir una violación de los datos personales:

Ejemplos
En el contexto de un hospital, si no estuvieran disponibles datos médicos críticos sobre pacientes, aunque fuera temporalmente, esto podría entrañar un riesgo sobre los derechos y libertades de los individuos; por ejemplo, podrían cancelarse operaciones y suponer un riesgo para vidas humanas.
Al contrario, en el caso de indisponibilidad de los sistemas de una empresa de medios durante varias horas (por ejemplo, debido a apagón), si dicha empresa no puede enviar *newsletters* a sus suscriptores, no es probable que esto suponga un riesgo para los derechos y las libertades de los individuos.
Una infección con ransomware podría entrañar una pérdida temporal de disponibilidad si los datos pueden restaurarse usando copias de seguridad. Sin embargo, se produjo una intrusión en la red, y podría ser necesaria una notificación si el incidente se califica de violación de la confidencialidad (es decir, si el atacante accede a los datos personales) y esto presenta un riesgo para los derechos y las libertades de las personas.

El artículo 33(1) establece que:

> En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación. (Artículo 33(1)).

El encargado del tratamiento «notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento» (artículo 33(2)). El GT29 recomienda que el encargado del tratamiento:

> lo notifique **sin demora** al responsable del tratamiento, y facilite más información sobre la violación de forma gradual, a medida que lleguen más detalles Esto es importante para ayudar al responsable del tratamiento a cumplir el requisito de notificación a la autoridad de control en un plazo de setenta y dos horas. (Directrices del GT29, p. 14)

Se entenderá que el responsable «**conoce**» la violación una vez que el encargado del tratamiento le haya informado de ello;[411] a continuación el responsable deberá notificarlo a la APD (del modo mencionado), a menos que sea improbable que esta *advertencia constituya* un riesgo para los derechos y las libertades de las personas.
En algunos casos, un encargado podría actuar en representación de varios-quizás incluso un número mayor-de responsables distintos, por ejemplo, como proveedor de almacenamiento

411 Directrices del GT, p. 14.

de datos en la nube. El GT29 indica lo siguiente para dichas situaciones:

> En caso de que el encargado del tratamiento preste servicios a varios responsables del tratamiento afectados por el mismo incidente, el encargado del tratamiento deberá comunicar los detalles del incidente a cada uno de ellos.
> Un encargado del tratamiento podría efectuar una notificación en nombre del responsable del tratamiento si este le hubiera concedido la autorización adecuada y esto formara parte de los acuerdos contractuales formalizados entre el responsable y el encargado del tratamiento. Dicha notificación debe efectuarse con arreglo a lo dispuesto en los artículos 33 y 34. No obstante, es importante señalar que la responsabilidad legal de notificar recae en el responsable del tratamiento. (p.14)

La notificación de la violación de datos a la correspondiente APD («competente»)[412] «deberá, como mínimo»:

a. describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

b. comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;

c. describir las posibles consecuencias de la violación de la seguridad de los datos personales;

d. describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

(Art. 33(3))

A este respecto, el GT29 afirma que el responsable podrá:[413]

> Si fuera necesario, optar por proporcionar más información. Diferentes tipos de violaciones (confidencialidad, integridad o disponibilidad) pueden requerir que se proporcione más información para explicar plenamente las circunstancias de cada caso.

Ejemplo:
Como parte de su notificación a la autoridad de control, un responsable del tratamiento puede considerar útil identificar a su encargado del tratamiento si este es la causa principal de una violación, en particular si ello ha dado lugar a un incidente que afecta a los registros de datos personales de muchos otros responsables del tratamiento que recurren al mismo encargado del tratamiento.

> En cualquier caso, la autoridad de control podrá solicitar más detalles en el marco de su investigación de una violación.

Además:

> Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida. (Art. 33(4))[414]

Ejemplo:
Un responsable del tratamiento notifica a la autoridad de control dentro de las setenta y dos horas siguientes a la detección de una violación que ha perdido una llave USB que contiene una copia de los datos personales de algunos de sus clientes. Con

---

412 Para consultar las directrices sobre notificación de violaciones transfronterizas y en establecimientos no pertenecientes a la UE, ver el apartado C de las Directrices del GT29 (pp. 16-18).

413 Directrices del GT29, p. 15.

414 Para más información y directrices sobre este asunto, ver las Directrices del GT29, pp. 15 – 16.

posterioridad, la llave USB se encuentra mal archivada dentro de las instalaciones del responsable del tratamiento y se recupera. El responsable del tratamiento informa a la autoridad de control y solicita que se modifique la notificación.

Periodo para la notificación:

Las Directrices del GT29 aclaran cuándo puede decirse que un responsable (o encargado) ha «**conocido»** una violación de seguridad, y remarca que existen funciones que anticipan y preparan dicho tipo de eventos:[415]

> Como se ha explicado anteriormente, el RGPD establece que, en caso de una violación, el responsable del tratamiento lo notificará sin dilación indebida y, de ser posible, a más tardar setenta y dos horas después de que haya tenido constancia de ella. Esto puede plantear la cuestión de cuándo puede considerarse que un responsable del tratamiento «tiene constancia» de una violación. El GT29 piensa que debe considerarse que un responsable del tratamiento «tiene constancia» cuando tenga un grado razonable de certeza de que se ha producido un suceso que compromete datos personales
> Sin embargo, como se ha indicado anteriormente, el RGPD requiere que el responsable del tratamiento aplique todas las medidas técnicas de protección y organización oportunas para determinar de inmediato si se ha producido una violación e informar sin dilación a la autoridad de control y a los interesados. Asimismo indica que debe verificarse que la notificación se ha realizado sin dilación indebida teniendo en cuenta, en particular, la naturaleza y gravedad de la violación y sus consecuencias y efectos adversos para el interesado. Esto obliga al responsable del tratamiento a garantizar que tendrá constancia de cualquier violación de forma rápida para que pueda tomar las medidas oportunas.
> El momento exacto en que puede considerarse que un responsable del tratamiento «tiene constancia» de una violación concreta dependerá de las circunstancias de dicha violación. En algunos casos, estará relativamente claro desde el principio que se ha producido una violación, mientras que en otros puede llevar algún tiempo establecer si los datos personales se han visto comprometidos.] No obstante, debe hacerse hincapié en la necesidad de actuar con rapidez para investigar un incidente a fin de determinar si, efectivamente, se ha violado la seguridad de los datos personales y, de ser así, para adoptar medidas correctivas y, en caso necesario, notificarlo.

Ejemplos

1. En caso de pérdida de una llave USB con datos personales no cifrados, a menudo no es posible determinar si personas no autorizadas han tenido acceso a dichos datos. No obstante, aunque el responsable del tratamiento no pueda determinar si se ha producido una violación de la confidencialidad, tal caso debe notificarse, ya que existe un grado razonable de certeza de que se ha producido una violación de la disponibilidad; el responsable del tratamiento «tendría constancia» cuando se dio cuenta de que la llave USB se había perdido
2. Un tercero informa a un responsable del tratamiento de que ha recibido accidentalmente los datos personales de uno de sus clientes y proporciona pruebas de la comunicación no autorizada. Dado que se han presentado pruebas claras de la existencia de una violación de la confidencialidad al responsable del tratamiento, no cabe duda de que este «tiene constancia» de ella
3. Un responsable del tratamiento detecta que ha habido una posible intrusión en su red. El responsable del tratamiento comprueba sus sistemas para determinar si los datos personales que se encuentran en ese sistema se han visto comprometidos y efectivamente es así. De nuevo, dado que ahora el responsable del tratamiento tiene pruebas claras de una violación, no cabe duda de que este «tiene constancia» de ella.

---

415 Directrices del GT29, pp. 10 – 11.

4. Un ciberdelincuente se pone en contacto con el responsable del tratamiento después de haber pirateado su sistema para pedir un rescate. En ese caso, tras comprobar su sistema para confirmar que ha sido objeto de un ataque, el responsable del tratamiento tiene pruebas claras de que se ha producido una violación y no cabe duda de que tiene constancia de ello.
5. Una persona informa al responsable del tratamiento de que ha recibido un mensaje de correo electrónico de alguien que se hace pasar por el responsable del tratamiento y que contiene datos personales relativos a su uso (real) del servicio, lo cual indica que la seguridad del responsable del tratamiento se ha visto comprometida. El responsable del tratamiento lleva a cabo una breve investigación e identifica una intrusión en su red y pruebas de un acceso no autorizado a los datos personales. En este momento se consideraría que el responsable del tratamiento «tiene constancia» y la notificación a la autoridad de control es necesaria, a menos que sea improbable que esto presente un riesgo para los derechos y las libertades de las personas. El responsable del tratamiento deberá adoptar las medidas correctivas adecuadas para subsanar la violación.

Documentación y evaluación de la violación:

El RGPD estipula, asimismo, que:

> El responsable del tratamiento documentará **cualquier** violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo. (art. 33(5), se ha añadido el subrayado)

Obsérvese que este último requisito se refiere a **toda** («cualquier») violación de datos personales: no se limita a violaciones de datos de las que haya que informar a la APD, es decir, el registro debe incluir también toda violación de datos que (en opinión del responsable) «no sea probable que suponga un riesgo para los derechos y las libertades de personas físicas».
En la práctica, el DPD deberá estar involucrado de cerca y de forma exhaustiva en dichos asuntos. A menudo, es probable que una presunta infracción se le comunique en primer lugar, a nivel interno, al DPD (o al Delegado de Seguridad o Encargado de Tecnologías), y el DPD deberá (según corresponda, con dichos empleados) realizar la primera evaluación inmediata de, como mínimo, los siguientes asuntos:

- Si realmente se produjo una violación de la seguridad de los datos personales, según se define en el RGPD (ver la definición del artículo 4(12), citada más arriba) –

  y si se concluye que se produjo una violación, o que es probable que se produjera una violación:

- qué (categorías de) interesados se vieron o podrían haberse visto afectados por la violación y qué (categorías de) datos personales podrían haberse perdido o haber sido afectados de otra forma –

  NB: El GT29 recomienda que esas categorías también deberán comunicarse a la APD en cualquier notificación de violación, y, además, que: [416]
  si los tipos de interesados o los tipos de datos personales indican un riesgo de que se produzcan daños y perjuicios particulares como consecuencia de una violación (por ejemplo, usurpación de identidad, fraude, pérdida financiera, amenaza al secreto profesional), es importante que la notificación indique estas categorías. De este modo, se vincula al requisito de describir las posibles consecuencias de la violación

[416] Directrices del GT29, p. 14.

Y teniendo en cuenta estos aspectos:

- Si es «probable» o «improbable» que dicha violación tenga como resultado un riesgo para los derechos y libertades de personas físicas –

El GT29 analiza la cuestión de cuándo no es necesaria la notificación en algún tipo de detalle[417] y ofrece el siguiente ejemplo:

> **Ejemplo:**
> Una violación que no requeriría notificación a la autoridad de control sería la pérdida de un dispositivo móvil cifrado de forma segura, utilizado por el responsable del tratamiento y su personal. Siempre que la clave de cifrado permanezca bajo la custodia segura del responsable del tratamiento y no se trate de la única copia de los datos personales, estos serán inaccesibles para un atacante. Esto significa que es poco probable que la violación constituya un riesgo para los derechos y las libertades de los interesados en cuestión. Si más tarde se pone de manifiesto que la clave de cifrado estaba comprometida o que el software o el algoritmo de cifrado es vulnerable, entonces el riesgo para los derechos y las libertades de las personas físicas cambiará y, por tanto, la notificación podría ser necesaria.

Pero si la evaluación concluye que es probable dicho riesgo potencial:

- Si el riesgo es un «alto riesgo para los derechos y libertades de [dichas] personas físicas» (porque esto no solo requeriría una notificación de la violación a la APD, sino también informar a los interesados, tal y como se indica en el siguiente sub-epígrafe).[418]

Tal y como indica el GT29, en el considerando 87 del RGPD se destaca la importancia de poder identificar una violación de la seguridad, evaluar el riesgo para las personas y, a continuación, notificarla en caso necesario:

> Debe verificarse si se ha aplicado toda la protección tecnológica adecuada y se han tomado las medidas organizativas oportunas para determinar de inmediato si se ha producido una violación de la seguridad de los datos personales y para informar sin dilación a la autoridad de control y al interesado. Debe verificarse que la notificación se ha realizado sin dilación indebida teniendo en cuenta, en particular, la naturaleza y gravedad de la violación de la seguridad de los datos personales y sus consecuencias y efectos adversos para el interesado. Dicha notificación puede resultar en una intervención de la autoridad de control de conformidad con las funciones y poderes que establece el presente Reglamento.

Y, desde luego, si la evaluación indicara que se ha producido una violación, y que existen riesgos para los intereses de las personas, deberán buscarse urgentemente **medidas atenuantes**.

Los asuntos arriba mencionados deberán, asimismo, **de forma urgente, tan pronto como sea posible**, transferirse a la dirección. En realidad, cualquier debate interno de los asuntos arriba mencionados no deberá retrasar la información a la alta dirección en cuanto se establezca que se ha producido una violación.

El hecho de que se realizaran dichas evaluaciones, de forma rigurosa debe registrarse **cuidadosamente**,[419] junto con los resultados de las evaluaciones correspondientes y los

---

417 Directrices del GT29, pp. 18 – 19. Ver, asimismo, la lista no exhaustiva de ejemplos que se proporcionan en un anexo (Anexo B) a la Directrices, que se reproduce más abajo, en el siguiente subepígrafe.

418 Ver, en particular, el comentario bajo el sub-apartado «*Evaluación del riesgo y del alto riesgo».*

419 El GT29 sugiere que esto debe hacerse «en los planes de respuesta ante incidentes o en los mecanismos

motivos de dichas evaluaciones; las medidas atenuantes que se tuvieron en cuenta; el hecho de que las evaluaciones y las medidas atenuantes propuestas se comunicaran a la alta dirección; las medidas reales autorizadas por la dirección y si se realizaron, y cuándo; y, por supuesto, el hecho de que la violación de la seguridad de datos (si se determina que era notificable) se notificó a la(s) APD correspondiente(s) y cuándo, con una copia de la notificación; y si así se requiere, el hecho de que se informó a los interesados, y cómo, con una copia de la correspondiente notificación y cualquier comunicado de prensa relevante, etc., (tal y como se indica en el siguiente epígrafe). Además, tal y como indican las Directrices del GT29:

> La documentación de la violación debe realizarse a medida que esta se desarrolla (p. 12).

En aquellas organizaciones que hubieran nombrado a un DPD, tendrá un papel importante en este aspecto, tal y como indica el GT29:[420]

> El responsable o el encargado del tratamiento podrán tener un delegado de protección de datos (DPD) , bien en virtud de lo dispuesto en el artículo 37, bien de forma voluntaria como buena práctica. El artículo 39 del RGPD establece una serie de Funciones obligatorias para el DPD, pero no impide que el responsable del tratamiento le asigne, si procede, otras Funciones.
>
> De especial importancia para la notificación de violaciones, las Funciones obligatorias del DPD incluyen, entre otras, proporcionar asesoramiento e información en materia de protección de datos al responsable o al encargado del tratamiento, supervisar el cumplimiento del RGPD y asesorar en relación con las EIPD. Además, el DPD debe cooperar con la autoridad de control y actuar como punto contacto con dicha autoridad y con los interesados. Asimismo, cabe señalar que, a la hora de notificar la violación a las autoridades de control, el artículo 33, apartado 3, letra b), exige que el responsable del tratamiento facilite el nombre y los datos de contacto de su DPD u otro punto de contacto.
>
> Por lo que se refiere a la documentación de las violaciones, es posible que el responsable o el encargado del tratamiento deseen obtener la opinión de su DPD sobre su estructura, configuración y administración. Además, podría encomendarse al DPD la función de mantener dichos registros.
>
> Estos factores significan que el DPD debe desempeñar un papel clave a la hora de ayudar a prevenir una violación o a prepararse proporcionando asesoramiento y supervisión del cumplimiento, así como durante una violación (es decir, cuando se notifica a la autoridad de control) y durante cualquier investigación posterior por parte de la autoridad de control. En este sentido, el GT29 recomienda que el DPD sea informado con rapidez de la existencia de una violación y que participe en todo el proceso de gestión y de notificación de la misma.

Las Directrices del GT29 dejan claro que las organizaciones no deberán ser solo reactivas a este respecto. En su lugar, deberán contar con una política de seguridad que trate de evitar, con antelación, cualquier violación de seguridad, y que contenga planes para evitarlos, atenuarlos y ponerles fin. En relación con las operaciones de tratamiento de datos personales que puedan dar lugar a un «alto riesgo» para los intereses de las personas, el diseño de dicha política podrá formar parte de una Evaluación de impacto de protección de datos (tal y como se comenta en la Función 4, anterior).[421]

---

de gobernanza del responsable del tratamiento» (p. 12). Esto se analiza en mayor detalle en la Sección V de las Directrices del GT29, *Responsabilidad corporativa y mantenimiento de registros*».

[420] Directrices del GT29, Sección V.B, pp. 27 – 28.

[421] Directrices del GT29, p. 6.

Informar a los interesados:

El GT29 aclara los requisitos sobre información de los interesados de una violación de datos, del siguiente modo:

> En algunos casos, además de notificar a la autoridad de control, el responsable del tratamiento también está obligado a comunicar una violación a las personas afectadas. El artículo 34(1) indica:
>
> > Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.
>
> Los responsables del tratamiento deben recordar que la notificación a la autoridad de control es obligatoria a menos que sea improbable que exista un riesgo para los derechos y las libertades de las personas como consecuencia de una violación. Además, cuando exista la probabilidad de un alto riesgo para los derechos y las libertades de las personas como consecuencia de una violación, también se debe informar a las personas. Por tanto, el umbral para la comunicación a las personas es más elevado que para la notificación a las autoridades de control y, por tanto, no se exigirá la comunicación de todas las violaciones a las personas, protegiéndolas así de un exceso de notificaciones. El RGPD establece que la comunicación de una violación a las personas debe hacerse «sin dilación indebida», lo cual significa lo antes posible. El objetivo principal de la notificación a las personas es proporcionarles información específica sobre las medidas que deben adoptar para protegerse. Como ya se ha señalado, dependiendo de la naturaleza de la violación y del riesgo que entrañe, una comunicación rápida ayudará a las personas a adoptar medidas para protegerse de sus consecuencias negativas.

Se adjunta al texto de la presente función como Adjunto un anexo (anexo B) de las presentes Directrices, en el que figura una lista (no exhaustiva) de 10 ejemplos de violaciones de datos personales y a quién deben notificarse.

Las Directrices del GT29 continúan del siguiente modo:[422]

> **Información que debe proporcionarse**
>
> A la hora de notificar a las personas, el artículo 34, apartado 3, especifica que:
>
> > La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).
>
> Según esta disposición, el responsable del tratamiento debe facilitar, como mínimo, la siguiente información:
>
> - una descripción de la naturaleza de la violación;
> - el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto;
> - una descripción de las posibles consecuencias de la violación; y
> - una descripción de las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Ejemplo:
Como ejemplo de las medidas adoptadas para subsanar la violación y mitigar sus posibles efectos adversos, el responsable del tratamiento podría indicar que, tras haberla notificado a la autoridad de control pertinente, ha recibido asesoramiento sobre

422 Sección III.B, p. 20. Edición del texto para su presentación.

el modo de gestionarla y de reducir su impacto. El responsable del tratamiento también debe, cuando proceda, asesorar de manera específica a las personas para que se protejan de las posibles consecuencias adversas de la violación, como establecer nuevas contraseñas si sus credenciales de acceso se han visto comprometidas. De nuevo, un responsable del tratamiento puede decidir proporcionar más información de la que se requiere aquí. De nuevo, un responsable del tratamiento puede decidir proporcionar más información de la que se requiere aquí.

Las Directrices aclaran, igualmente, que:[423]

> En principio, la violación en cuestión debe comunicarse directamente a los interesados afectados, a menos que ello suponga un esfuerzo desproporcionado. En ese caso, se optará por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados [artículo 34, apartado 3, letra c)].

«Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control» (Considerando 86). Tal y como se indica en las Directrices:[424]

> Por consiguiente, los responsables del tratamiento tal vez deseen ponerse en contacto con la autoridad de control y consultarla no solo para pedir asesoramiento sobre la información a los interesados en relación con una violación de conformidad con el artículo 34, sino también sobre la adecuación de los mensajes que deben enviarse a las personas, así como la forma más adecuada de ponerse en contacto con ellas.
> A este respecto está el consejo del considerado 88 de que la notificación de una violación debe «tener en cuenta los intereses legítimos de las autoridades policiales en caso de que una comunicación prematura pueda obstaculizar innecesariamente la investigación de las circunstancias de una violación de la seguridad de los datos personales». Ello puede significar que, en determinadas circunstancias, cuando esté justificado, y con el asesoramiento de las autoridades policiales, el responsable del tratamiento podrá retrasar la comunicación de la violación a las personas afectadas hasta el momento en que no perjudique dichas investigaciones. No obstante, los interesados deberán ser informados sin dilación una vez transcurrido este plazo.
> Cuando no sea posible que el responsable del tratamiento comunique una violación a una persona porque los datos almacenados sean insuficientes para ponerse en contacto con ella, en esa circunstancia concreta, el responsable del tratamiento deberá informar a la persona tan pronto como sea razonablemente posible (por ejemplo, cuando una persona ejerza su derecho de acceso a los datos personales con arreglo al artículo 15 y facilite al responsable del tratamiento la información adicional necesaria para ponerse en contacto con ella).

Excepciones:

Tal y como se indica en las Directrices del GT29:[425]

> El artículo 34, apartado 3, establece tres condiciones que, si se cumplen, no requieren notificación a las personas en caso de violación. Estas condiciones son:
>
> - • Que el responsable del tratamiento haya adoptado medidas de protección técnicas y organizativas apropiadas para proteger los datos personales antes de la violación, en particular aquellas que los hagan ininteligibles para cualquier persona que no esté autorizada a acceder a ellos. Por ejemplo, esto podría incluir la protección de datos personales con un cifrado de tecnología avanzada o mediante tokenización.

---

423 Sección III.C, p. 21; ver este apartado para consultar más orientaciones sobre las formas alternativas de comunicar una violación de datos a los interesados afectados.

424 *Ídem*, pp. 21 – 22.

425 Sección III.D, p. 22.

- Que, inmediatamente después de una violación, el responsable del tratamiento haya tomado medidas que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades de la persona. Por ejemplo, dependiendo de las circunstancias del caso, el responsable del tratamiento podría haber identificado inmediatamente a la persona que accedió a los datos personales y tomar medidas contra ella, antes de que pudiera hacer nada con ellos. Es preciso prestar la debida atención a las posibles consecuencias de cualquier violación de la confidencialidad, de nuevo, en función de la naturaleza de los datos en cuestión.

- Que suponga un esfuerzo desproporcionado ponerse en contacto con las personas, quizás cuando sus datos de contacto se hayan perdido como resultado de la violación o, de entrada, no se conozcan. Por ejemplo, el almacén de una oficina de estadística se ha inundado y los documentos que contienen los datos personales solo estaban almacenados en papel. A cambio, el responsable del tratamiento debe hacer una comunicación pública o adoptar una medida semejante por la que se informe de manera igualmente efectiva a los interesados. En caso de esfuerzo desproporcionado, también podrían preverse disposiciones técnicas para que la información sobre la violación esté disponible a petición del interesado, lo cual podría resultar útil para las personas que puedan verse afectadas por una violación, pero con las que el responsable del tratamiento no pueda ponerse en contacto de otro modo.

De conformidad con el principio de obligación de rendir cuentas, los responsables del tratamiento deben poder demostrar a las autoridades de control que cumplen una o varias de estas condiciones. Hay que tener en cuenta que, si bien la notificación puede no ser necesaria inicialmente si no existe un riesgo para los derechos y las libertades de las personas, esto puede cambiar con el tiempo y habría que reevaluar el riesgo.
Si un responsable del tratamiento decide no comunicar una violación a la persona, el artículo 34, apartado 4, explica que la autoridad de control puede exigirle que lo haga si considera que dicha violación puede entrañar un alto riesgo para las personas. Por otra parte, puede considerar que se han cumplido las condiciones del artículo 34, apartado 3, en cuyo caso no se requiere notificación. Si la autoridad de control determina que la decisión de no notificar a los interesados no está bien fundamentada, podrá considerar la posibilidad de hacer uso de las facultades y sanciones de que dispone.

Evaluación del riesgo y riesgo alto

De nuevo, bastará con citar las Directrices del GT29:[426]

Aunque el RGPD introduce la obligación de notificar una violación, no es obligatorio hacerlo en todas las circunstancias:

- La notificación a la autoridad de control competente es obligatoria a menos que sea improbable que una violación constituya un riesgo para los derechos y las libertades de las personas.

- La comunicación de una violación a la persona solo se realizará cuando sea probable que entrañe un alto riesgo para sus derechos y libertades.

Esto significa que, inmediatamente después de tener conocimiento de una violación, es de vital importancia que el responsable del tratamiento no trate solo de contener el incidente, sino que también evalúe el riesgo que podría derivarse del mismo. Hay dos razones importantes para ello: en primer lugar, conocer la probabilidad y la gravedad potencial del impacto en la persona ayudará al responsable del tratamiento a adoptar

426 Sección IV.A y B, p. 23, referencias omitidas; de nuevo, se han editado a los efectos de su presentación.

medidas eficaces para contener y poner remedio a la violación; en segundo lugar, le ayudará a determinar si la notificación a la autoridad de control es necesaria y, en su caso, a las personas afectadas.

Como se ha explicado anteriormente, la notificación de una violación es obligatoria a menos que sea improbable que constituya un riesgo para los derechos y las libertades de las personas, y el factor clave que exige la comunicación de una violación a los interesados es cuando sea probable que entrañe un alto riesgo para los derechos y las libertades de las personas. Este riesgo existe cuando la violación puede dar lugar a daños y perjuicios físicos, materiales o inmateriales para las personas cuyos datos han sido violados.

Ejemplos:
Ejemplos de tales daños y perjuicios son la discriminación, la usurpación de identidad o el fraude, la pérdida financiera y el daño para la reputación. Cuando la violación se refiera a datos personales que revelen el origen étnico o racial, las opiniones políticas, la religión o las creencias filosóficas, la militancia en un sindicato, o que incluyan datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas, se considerará probable que tales daños y perjuicios se produzca.

Factores a tener en cuenta a la hora de evaluar el riesgo

Los considerandos 75 y 76 del RGPD señalan que, en general, al evaluar el riesgo, debe tenerse en cuenta tanto la probabilidad como la gravedad del riesgo para los derechos y las libertades de los interesados. Además, se señala que el riesgo debe evaluarse sobre la base de una valoración objetiva.

Cabe señalar que la evaluación del riesgo para los derechos y las libertades de las personas como resultado de una violación tiene un enfoque diferente del riesgo considerado en una EIPD. En la EIPD se consideran tanto los riesgos de que el tratamiento de datos se lleve a cabo según lo previsto, como los riesgos en caso de que se produzca una violación. A la hora de considerar una posible violación, en términos generales, se examina la probabilidad de que esto ocurra y los daños y perjuicios que podrían derivarse para el interesado; en otras palabras, se trata de la evaluación de un acontecimiento hipotético. En caso de violación real, el hecho ya se ha producido, por lo que la atención se centra exclusivamente en el riesgo derivado del impacto de la violación en las personas.

Ejemplo:
Una EIPD indica que el uso propuesto de un determinado programa informático de seguridad con el fin de proteger los datos personales es una medida apropiada para garantizar un nivel de seguridad adecuado al riesgo que, de otro modo, entrañaría el tratamiento para las personas. Sin embargo, si posteriormente se tiene conocimiento de una vulnerabilidad, esto cambiaría la idoneidad del programa informático respecto de la contención del riesgo para los datos personales protegidos, por lo que habría que volver a evaluarla como parte de una EIPD continua.
Con posterioridad, se explota una vulnerabilidad del producto y se produce una violación. El responsable del tratamiento debe evaluar las circunstancias específicas de la violación, los datos afectados y el nivel potencial de impacto en las personas, así como la probabilidad de que este riesgo se materialice.

Por consiguiente, al evaluar el riesgo para las personas derivado de una violación, el responsable del tratamiento debe tener en cuenta las circunstancias específicas de la violación, incluida la gravedad del impacto potencial y la probabilidad de que esto ocurra. Por tanto, el GT29 recomienda que la evaluación tenga en cuenta los siguientes

criterios:[427]

El tipo de violación

El tipo de violación que se haya producido puede afectar al nivel de riesgo que presente para las personas.

[427] El artículo 3.2 del Reglamento 611/2013 ofrece directrices sobre los factores que deben tenerse en cuenta en relación con la notificación de casos de violación de datos personales en el sector de servicios de comunicación, que podrán ser útiles en el contexto de una notificación en virtud del RGPD. Ver: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF [pie de página original]

Ejemplo:
Una violación de la confidencialidad por la que se haya revelado información médica a partes no autorizadas podría tener para una persona un conjunto de consecuencias diferente que las que podría tener una violación en la que los datos médicos de una persona se hayan perdido y ya no estén disponibles

La naturaleza, el carácter sensible y el volumen de datos personales

Por supuesto, al evaluar el riesgo, un factor clave es el tipo y la sensibilidad de los datos personales que se hayan visto comprometidos a causa de la violación. Por lo general, cuanto más sensibles sean los datos, mayor será el riesgo de daño para las personas afectadas, pero también deben tenerse en cuenta otros datos personales que ya puedan estar disponibles sobre el interesado. Por ejemplo, es poco probable que la divulgación del nombre y la dirección de una persona cause daños y perjuicios sustanciales en circunstancias normales Sin embargo, si se revela el nombre y la dirección de un padre adoptivo a un padre biológico, las consecuencias podrían ser muy graves tanto para el padre adoptivo como para el niño.

Las violaciones que implican datos relativos a la salud, documentos de identidad o datos financieros como detalles de tarjetas de crédito, pueden causar daño por sí mismas, pero juntas podrían utilizarse con fines de usurpación de identidad. Una combinación de datos personales suele ser más delicada que un único dato personal.

Algunos tipos de datos personales pueden parecer al principio relativamente inocuos, sin embargo, la información que esos datos puedan revelar sobre la persona afectada debe examinarse cuidadosamente. Una lista de clientes que aceptan entregas regulares puede no ser especialmente sensible, pero los mismos datos sobre los clientes que han solicitado que se interrumpan sus entregas durante las vacaciones serían una información útil para los delincuentes.

Del mismo modo, una pequeña cantidad de datos personales muy sensibles puede tener un impacto elevado en una persona, y una gran variedad de detalles puede revelar una mayor diversidad de información sobre esa persona. Asimismo, una violación que afecte a un gran volumen de datos personales sobre muchos interesados puede tener efectos para el correspondiente gran número de personas.

Facilidad de identificación de las personas

Un factor importante a tener en cuenta es lo fácil que será para una parte que tenga acceso a datos personales comprometidos identificar a personas específicas, o comparar los datos con otra información para identificar a esas personas. Dependiendo de las circunstancias, la identificación podría ser posible directamente a partir de los datos personales violados sin necesidad de realizar una investigación especial para descubrir la identidad de la persona, o cotejar los datos personales con los de una persona en particular podría ser extremadamente difícil, pero esto aún sería posible en determinadas condiciones. La identificación sería posible de forma directa o indirecta a partir de los datos violados, pero también podría depender del contexto específico de la violación y el acceso público a datos personales relacionados. Esto puede ser más relevante para las violaciones de la confidencialidad y la disponibilidad.

Como se ha indicado anteriormente, los datos personales protegidos mediante un nivel adecuado de cifrado serán ininteligibles para personas no autorizadas que no dispongan de la clave de descifrado. Además, una «seudonimización» correctamente realizada (definida en el artículo 4(5) como «el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable») también puede reducir la probabilidad de

identificación de personas en caso de una violación. Sin embargo, no se puede considerar que las técnicas de seudonimización por sí solas hagan que los datos sean ininteligibles

Gravedad de las consecuencias para las personas

Dependiendo de la naturaleza de los datos personales implicados en una violación, por ejemplo, si se trata de categorías especiales de datos, los posibles daños y perjuicios que se derivan para las personas pueden ser especialmente graves, en particular cuando la violación podría dar lugar a una usurpación de identidad o fraude, daño físico, sufrimiento psicológico, humillación o daño para la reputación. Si la violación se refiere a datos personales de personas vulnerables, estas podrían correr un mayor riesgo de sufrir daños

El hecho de que el responsable del tratamiento tenga constancia de que los datos personales están en manos de personas cuyas intenciones se desconocen o son posiblemente maliciosas puede influir en el nivel de riesgo potencial. Puede producirse una violación de la confidencialidad por la que se revelen datos personales a un tercero, tal como se define en el artículo 4, apartado 10, o a otro destinatario por error. Esto puede ocurrir, por ejemplo, cuando los datos personales se envían accidentalmente al departamento equivocado de una organización, o a una organización proveedora habitualmente utilizada. El responsable del tratamiento podrá pedir al destinatario que devuelva o destruya de forma segura los datos que haya recibido. En ambos casos, dado que el responsable del tratamiento mantiene una relación permanente con ellos, y puede conocer sus procedimientos, historia y otros detalles relevantes, el destinatario puede considerarse «de confianza». En otras palabras, el responsable del tratamiento puede tener un cierto grado de garantía con el destinatario, de modo que puede esperar razonablemente que no lea ni acceda a los datos enviados por error y que cumpla con sus instrucciones de devolverlos. Incluso si se ha accedido a los datos, el responsable del tratamiento todavía puede confiar en que el destinatario no hará nada con ellos, los devolverá rápidamente al responsable del tratamiento y cooperará para su recuperación. En tales casos, esto puede tenerse en cuenta en la evaluación del riesgo que el responsable del tratamiento lleve a cabo tras el incumplimiento: el hecho de que se confíe en el destinatario puede eliminar la gravedad de las consecuencias del incumplimiento, pero no significa que dicho incumplimiento no se haya producido. Sin embargo, esto puede eliminar también la probabilidad de riesgo para las personas, por lo que ya no es necesario notificarlo a la autoridad de control ni a las personas afectadas. De nuevo, esto dependerá de cada caso particular. No obstante, el responsable del tratamiento debe conservar la información relativa a esta violación como parte de la obligación general de llevar registros de las violaciones (...).

También se debe tener en cuenta la permanencia de las consecuencias para las personas cuando se considere que el impacto es mayor si los efectos son a largo plazo.

Características particulares de la persona

Una violación puede afectar a los datos personales de niños u otras personas vulnerables que, como consecuencia de ello, pueden verse expuestos a un mayor peligro. Puede haber otros factores relativos al individuo susceptibles de afectar el nivel de impacto que dicha violación puede tener en ellos.

Características particulares del responsable del tratamiento

La naturaleza y el papel del responsable del tratamiento y sus actividades pueden afectar al nivel de riesgo que una violación podría tener para las personas. Por ejemplo, una organización médica tratará categorías especiales de datos personales, lo cual significa que si se violan sus datos personales la amenaza para las personas es mayor que si se tratara de la lista de distribución de un periódico.

El número de personas afectadas

Una violación puede afectar solo a una persona, a unas pocas o a varias miles, o incluso a muchas más. En general, cuanto mayor sea el número de personas afectadas, mayor puede ser su impacto. Sin embargo, una violación puede tener un impacto grave incluso en una sola persona, dependiendo de la naturaleza de los datos personales y del contexto en el que se hayan visto comprometidos. De nuevo, la clave es tener en cuenta la probabilidad y la gravedad del impacto en los afectados

Consideraciones generales

Por tanto, a la hora de evaluar el riesgo que puede entrañar una violación, el responsable del tratamiento debe tener en cuenta una combinación de la gravedad del impacto potencial en los derechos y las libertades de las personas y la probabilidad de que este se produzca. Evidentemente, cuando las consecuencias de una violación son más graves, el riesgo es más elevado y, del mismo modo, cuando la probabilidad de que se produzcan es mayor, el riesgo también aumenta. En caso de duda, el responsable del tratamiento debe pecar por exceso de precaución y notificar. En el anexo B se proporcionan algunos ejemplos útiles de diferentes tipos de violaciones que implican riesgo o riesgo alto para las personas.

La Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) ha elaborado una serie de recomendaciones para una metodología de evaluación de la gravedad de una violación, que los responsables y los encargados del tratamiento pueden considerar útil a la hora de diseñar su plan de respuesta de gestión de violaciones.[428]

- o – O – o -

[428] ENISA, Recomendaciones para una metodología de la evaluación de la gravedad de violaciones de datos personales, https://www.enisa.europa.eu/publications/dbn-severity [pie de página original]

Adjunto:
Ejemplos de violaciones de datos personales y a quién notificarlos (De las Directrices del GT29)

Ejemplo:	**¿Informar a la autoridad de supervisión?**	**¿Informar a los interesados?**	**Notas/recomendaciones**
i. Un responsable almacenó una copia de seguridad de un archivo de datos personales encriptado en una llave USB. Durante un robo, se roba la llave.	No.	No.	Siempre y cuando los datos estén encriptados con un algoritmo de última generación, existan copias de seguridad de los datos, la clave única no se vea comprometida y los datos pueden ser recuperados a tiempo, no podrá tratarse de un incumplimiento notificable. No obstante, si posteriormente se viera comprometida, será necesaria una notificación.
ii. Un responsable mantiene un servicio online. Como resultado de un ciberataque sobre dicho servicio, se infiltran los datos personales de personas. El responsable tiene clientes en un solo Estado Miembro.	Sí, informar a la autoridad de supervisión si es posible que haya consecuencias para las personas.	Sí, informar a las personas en función de la naturaleza de los datos personales afectados y en caso de gravedad alta de las consecuencias probables a personas.	
iii. Corte de luz breve que dura varios minutos en el *call centre* de un responsable, que implica que los clientes no puedan llamar al responsable y acceder a sus registros	No.	No.	No se trata de una violación notificable, pero sí es un incidente registrable en virtud del artículo 33, apartado 5. El responsable deberá mantener registros adecuados.
iv. Un responsable	Sí, informe a la	Sí, informar a las	Si hubiera disponible una

sufre un ataque con un programa de secuestro, que se traduce en el cifrado de todos los datos. No existen copias de seguridad y los datos no pueden recuperarse. Tras realizar una investigación, queda claro que la única función del programa de secuestro era cifrar los datos y que no había ningún otro malware presente en el sistema.	autoridad supervisora, si hay consecuencias probables para las personas, ya que se trata de una pérdida de disponibilidad.	personas, según la naturaleza de los datos personales afectados y el posible efecto de la no disponibilidad de los datos, así como de otras posibles consecuencias.	copia de seguridad y los datos pudieran restaurarse a su debido tiempo, no sería necesario informar de ello a la autoridad supervisora o a los particulares, ya que no se habría producido una pérdida permanente de disponibilidad o confidencialidad. No obstante, si las autoridades de supervisión hubieran tenido conocimiento del incidente por otros medios, podrán considerar la posibilidad de llevar a cabo una investigación para evaluar el cumplimiento de los requisitos de seguridad más extensos que constan en el artículo 32.
v. Una persona llama al call centre de un banco para informar de una brecha de seguridad. Dicha persona ha recibido el extracto de cuenta de otra persona. El responsable lleva a cabo una investigación rápida (es decir, que se cierra en 24 horas) y establece, con un nivel aceptable de confianza, que se ha producido una violación de datos personales y si tiene un fallo sistémico que podría implicar que otras personas se vean o puedan verse afectadas.	Sí.	Únicamente las personas afectadas son notificadas en caso de alto riesgo, y está claro que no hubo otras personas afectadas.	Si, después de llevar a cabo más investigaciones, se identifica que se hay más personas afectadas, se realizará una actualización a la autoridad de supervisión y el responsable tomará la medida adicional de informar a otros de si están sometidos a un alto riesgo.

vi. Un responsable opera un mercado en línea y cuenta con clientes en distintos Estados Miembros. El mercado sufre un ciberataque y el atacante publica en la red los nombres de usuario, contraseñas e historial de compras.	Sí, informar a la autoridad de supervisión encargada si implica tratamiento transfronterizo.	Sí, pues podría implicar un alto riesgo.	El responsable deberá tomar acciones, por ejemplo, ordenando que se restablezca la contraseña de las cuentas afectadas, así como otros pasos para atenuar el riesgo. El responsable deberá tener en cuenta, igualmente, cualquier otra obligación de notificación, por ejemplo, en virtud de la Directiva SRI como proveedor de servicios digitales.
vii. Una compañía de hosting web que actúe como encargado de datos identifica un error en el código que controla la autorización de usuarios. El efecto de dicho fallo implica que cualquier usuario podrá acceder a los datos de la cuenta de cualquier otro usuario.	Como encargada, la compañía de hosting web deberá notificar a sus clientes afectados (los responsables) sin retrasos injustificados. Si asumimos que la compañía de hosting web ha llevado a cabo sus propia investigación, el responsable afectado deberá estar lo suficientemente convencido de si cada uno ha sufrido una violación y, por tanto, es probable que se entienda que «tuvo conocimiento» una vez informado por la compañía de hosting (el encargado). El responsable deberá posteriormente informar a la autoridad de supervisión.	Si es probable que no haya un alto riesgo para las personas, no es necesario que se les informe.	La empresa de alojamiento de sitios web (encargado) debe tener en cuenta cualquier otra obligación de notificación (por ejemplo, en virtud de la Directiva SRI como proveedor de servicios digitales). Si no hubiera pruebas de que se esté explotando esta vulnerabilidad con ninguno de sus responsables del tratamiento, es posible que no se haya producido una infracción notificable, pero es probable que sí deba registrarse o que se trate de un caso de incumplimiento con arreglo al artículo 32.
viii. Los registros médicos de un hospital no están	Sí, el hospital está obligado a informar, ya que puede existir	Sí, informe a las personas afectadas.	

disponibles durante el período de 30 horas debido a un ataque cibernético.	un alto riesgo para el bienestar y la privacidad del paciente.		
ix. Los datos personales de un gran número de alumnos se enviaron por error a una lista de distribución errónea con más de 1000 destinatarios.	Sí, avisar a la autoridad de supervisión.	Sí, avisar a las personas en función del alcance y del tipo de datos personales afectados y de la gravedad de las posibles consecuencias.	
x. Se envía un e-mail de marketing a los destinatarios en los campos «para» o «cc:», permitiendo así a cada destinatario ver la dirección de correo electrónico de los demás.	Sí, puede ser obligatorio informar a la autoridad de supervisión si afectara a un alto número de personas, si se revelan datos sensibles (por ejemplo, una lista de distribución de un psicoterapeuta), o si otros factores presentan altos riesgos (por ejemplo, el correo contiene las contraseñas iniciales).	Sí, avisar a las personas en función del alcance y del tipo de datos personales afectados y de la gravedad de las posibles consecuencias.	Es posible que la notificación no sea necesaria si no se comunican datos sensibles y si tan solo se comunica un número bajo de direcciones de correo electrónico.

FUNCIÓN 7: Función de investigación (incluyendo el tratamiento de denuncias internas y externas)

Nota: Esta función es individual y distinta del tratamiento de solicitudes de interesados de acceso, corrección, etc., tal y como se indica en la Función 8.

Investigación

Aunque no se menciona expresamente en el RGPD, se deriva de las descripciones generales del puesto y funciones generales del DPD y, en especial, de su deber de «supervisar el cumplimiento» de lo dispuesto en el presente Reglamento: art. 39, apartado 1, letra b, que el DPD podrá, a su propia iniciativa o a solicitud de la dirección o, por ejemplo, del organismo de representación o sindicato del personal o, de hecho, de cualquier persona (de dentro o de fuera de la organización, o incluso un denunciante, que, con suerte, esté protegido en el país relativo) **investigar** asuntos y eventos que estén directamente relacionados con sus funciones, e **informar** de nuevo a la persona o entidad que encargó o solicitó la investigación, o a la dirección. Tal y como indica el SEPD en su Documento expositivo sobre DPD:[429]

> **Supervisión del cumplimiento normativo** (…): el DPD deberá garantizar la aplicación del Reglamento dentro de la institución. El DPD podrá, a su propia iniciativa o a solicitud de la institución u organismo, el responsable, el comité del personal o cualquier individuo, investigar asuntos o eventos relativos a sus funciones, e informar de nuevo a la persona que encargara la investigación, o al responsable.

El RGPD aclara, aunque en términos menos específicos que el *Anexo* a la normativa institucional de la UE sobre protección de datos, que los DPD deberán poder contar con **todos los recursos necesarios** y **acceso a todos los datos e instalaciones, instalaciones de tratamiento de datos y soportes de datos** (con todos los poderes relevantes y necesarios sobre ***autenticación*** y ***acceso y retención de registros***) necesarios para llevar a cabo sus funciones (ver art. 38, apartado 2, por ejemplo, también en relación con dichas investigaciones.[430] De igual modo, aunque, una vez más, esto se mencione de forma más explícita en relación con DPD a nivel institucional de la UE que con DPD nombrados en virtud del RGPD, **todo el personal relevante del responsable – e igualmente, el personal de agencias externas, incluyendo, especialmente, a los encargados (incluyendo proveedores de servicios en la nube a los que recurra el responsable) – deberán colaborar totalmente con el DPD en dichas investigaciones**, y ofrecer ***respuestas e información completa*** como respuesta a preguntas o solicitudes del DPD.[431] **Los responsables deberán explicar esto claramente en las directrices internas del personal, e incluir cláusulas que sean claras a estos efectos en sus contratos con los proveedores y encargados externos.**

Ejecución

A pesar de contar con competencia para supervisar el cumplimiento del RGPD, para gestionar denuncias e investigar posibles violaciones del Reglamento, **el DPD cuenta con poderes**

---

429 SEPD, Documento expositivo sobre el papel de los Delegados de Protección de Datos en asegurar el cumplimiento eficaz de lo dispuesto en el Reglamento (CE) 45/2001 (nota al pie 243, arriba), p.6, negrita en el original.

430 El *Anexo* al Reglamento (UE) 45/2001 estipula que los DPD institucionales de la UE: «tendrán acceso en todo momento a los datos objeto de las operaciones de tratamiento y a todos los locales, instalaciones de tratamiento de datos y soportes de datos». (*Anexo*, artículo 4, segunda frase).

431 El *Anexo* al Reglamento (UE) 45/2001 estipula que: «Los responsables del tratamiento interesados asistirán al responsable de la protección de datos en el ejercicio de sus funciones y le proporcionarán la información que solicite». (*Anexo*, artículo 4, primera frase).

limitados de ejecución. En principio, tal y como se indica más arriba, si el DPD averigua que su organización, o cualquier proveedor o encargado externo, han incumplido de alguna manera el RGPD, el DPD deberá informar de ello a la alta dirección, momento a partir del cual corresponderá a la alta dirección adoptar medidas correctivas, incluyendo, cuando corresponda, sanciones contra miembros del personal, agentes o encargados que hubieran incumplido sus respectivas obligaciones, por ejemplo, emitiendo avisos u otras sanciones o, en casos extremos, despido o rescisión de contratos. Por ejemplo, si se utiliza un proveedor de servicios externo para recopilar datos (por ejemplo, mediante sistemas automatizados gestionados por el proveedor) y ese proveedor no cumple con el RGPD, por ejemplo, en términos de notificaciones de información o, lo que es peor, utilizando subrepticiamente los datos recopilados para otros fines (no declarados), el DPD deberá proponer que el responsable del tratamiento recurra a otro proveedor y alertar al mismo tiempo a la APD.
El hecho de que no se tome dicha medida se atribuirá al responsable del tratamiento (la organización) en la consideración de las medidas de ejecución por parte de la autoridad estatal de protección de datos (APD), incluyendo el establecimiento del nivel de cualquier «multa administrativa» que pueda imponerse (ver el artículo 83).
Además, una de las funciones del DPD será «consultar» con la APD correspondiente «cuando sea necesario», con respecto a cualquier asunto que pueda surgir (art. 39, apartado 1, letra e).
En caso de que surja una grave divergencia de opiniones entre el DPD y la alta dirección de su organización, cuando el DPD considere que una determinada operación de tratamiento infringe o infringirá (de forma significativa) el RGPD o la legislación nacional pertinente, pero que la dirección sigue queriendo llevar a cabo, o contra la que no tiene intención de adoptar ninguna sanción, no cabe duda de que sería «adecuado» que el DPD ejerciera esta facultad y remitiera (de manera efectiva) el asunto a la APD. A continuación, corresponderá a la APD hacer uso de sus importantes funciones de investigación y ejecución, incluida la posibilidad de ordenar la no ejecución o el cese de la operación, según lo considere oportuno (la APD) (ver el artículo 58, apartado 2, letras d y f en particular).
Ver más abajo, en los epígrafes «*Cooperación con y consulta a la APD»* y «*Procesamiento de consultas y denuncias*».

- o – O – o -

Funciones consultivas

FUNCIÓN 8: Función consultiva - general

El DPD deberá asegurar que se respete el Reglamento y asesorar a los responsables sobre el cumplimiento de sus obligaciones. Por tanto, el DPD podrá **informas,** ofrecer **asesoramiento** o realizar **recomendaciones** para la ***mejora práctica*** de protección de datos por parte de la organización o sobre los asuntos relativos a la aplicación de las disposiciones sobre protección de datos (es decir, del RGPD y de otras leyes europeas sobre protección de datos – como, de momento, la Directiva de 2002 sobre Privacidad electrónica y, en el futuro, un posible Reglamento e-Privacy y cualquier otra ley nacional que amplíe las cláusulas «claúsulas de especificación" del RGPD o que sean de aplicación de otro modo); y en el caso de ***la mejora y actualización de las políticas y prácticas de protección de datos de la organización***, a la luz de nuevos instrumentos legales, decisiones, medidas o directrices (ver art. 39(1)(a)).

Con ese fin, deberá permitirse al DPD **seguir de cerca los desarrollos legislativos y normativos en las áreas de protección de datos, seguridad de datos, etc.**, para poder informar a la alta dirección o a mandos inferiores de los futuros ***nuevos instrumentos europeos*** (como el Reglamento e-Privacy, mencionado más arriba), o nuevas ***decisiones judiciales o ejecutivas a nivel europeo*** (como cualquier nueva decisión sobre «adecuación» que adopte la Comisión Europea relativa a terceros países a los que transfiera datos la organización del DPD, o sentencias relevantes que dicte el TJUE); ***nuevas directrices a nivel europeo*** (en especial, toda opinión o recomendación, etc., que emita el ***CEPD***); así como ***instrumentos, decisiones, medidas o directrices similares que se emitan en el país*** (o países) de establecimiento ***del DPD.*** El RGPD **requiere** que cada responsable con un DPD proporcione al DPD «***[todos] los recursos necesarios*** *para llevar a cabo [su] función… y* ***mantener su conocimiento de experto***» (art. 38, apartado 2). Por lo tanto, deberá permitirse y, de hecho, fomentarse, que el DPD asista a seminarios, conferencias y reuniones, en particular las organizadas por la (o las) autoridad nacional o regional de protección de datos de su Estado.

El DPD también **puede ser consultado** por la dirección, el órgano representativo del personal o el sindicato, o incluso por cualquier miembro del personal, incluidos, por supuesto, los «propietarios de empresas»/personas dentro de la organización con responsabilidades específicas para una operación de tratamiento específica, siempre que dicha persona pueda necesitar asesoramiento y, de hecho, en general, **debe ser consultado** sobre cuestiones pertinentes (véase también la Función 7, que se discute a continuación).

Tal y como indica el GT29 en sus Directrices sobre DPD (desde que fuera aprobado formalmente por el CEPD):[432]

> En consecuencia, la organización deberá asegurar, por ejemplo, que:
>
> - Se invite al DPD a participar periódicamente en reuniones de los altos cargos/directivos de nivel medio.
> - Se aconseje su presencia cuando se toman decisiones con implicaciones en materia de protección de datos. Toda la información pertinente deberá transmitirse al DPD de forma oportuna, para que pueda prestarle el asesoramiento adecuado.

---

[432] GP29 Directrices sobre DPD (nota al pie 242, arriba), pp. 13 – 14.

- La opinión del DPD debe tenerse siempre en cuenta debidamente. En caso de desacuerdo, el GT29 recomienda, como buena práctica, documentar las razones por las que no se ha seguido el consejo del DPD.
- El DPD deberá ser consultado sin demora cuando se produzca una violación de datos u otro incidente.

En su caso, el responsable del tratamiento o el encargado del tratamiento podrían elaborar directrices o programas de protección de datos que establezcan cuándo debe consultarse al DPD.

- o – O – o -

FUNCIÓN 9: Respaldar y fomentar la «Protección de datos por diseño y defecto»

Tal y como consta en el análisis de la Función 6 anterior, el DPD deberá, en general, ser consultado sobre cualquier asunto que esté relacionado con protección de datos y que surja dentro de su organización, incluyendo en la elaboración de directrices generales sobre política, etc.

No obstante, hay un asunto que es de especial relevancia a este respecto. Este es el nuevo requisito explícito del RGDP (que la Directiva de Protección de Datos de 1995 todavía no explicaba, aunque ya podía inferirse, como así se hizo),[433] que los responsables incorporen el principio de «protección de datos por diseño y defecto» (que incluye el principio de «***seguridad por diseño [y defecto]***»)[434] en todas sus operaciones. Tal y como se menciona en el artículo 25:

Artículo 25

Protección de datos desde el diseño y por defecto

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.
2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.
3. … [435]

Aquí tan solo podemos comentar brevemente el principio. El SEPD resume el **concepto general y su contexto** como sigue:[436]

---

[433] Ver, por ejemplo, la referencia repetida al principio en la Opinión 8/2014 del GT29, sobre los Desarrollos recientes del Internet de las cosas (GT223), adoptada el 16 de septiembre de 2014, disponible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

[435] El apartado 3 estipula que: «Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo». Esto se analiza en relación con la Función 9, que consta más abajo.

[436] SEPD, Opinión preliminar sobre privacidad por diseño (Opinión 5/2018), emitida el 31 de mayo de 2018, p. 4, párr. 17 (cursiva en el original), disponible en: https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf (se ha añadido el subrayado)
Obsérvese que el SEPD distingue el principio amplio de «privacidad por diseño», que tiene una «dimensión ética y visionaria», de los requisitos legales más específicos sobre «protección por diseño» y «protección de datos por defecto» del artículo 25 del RGPD: p. 1, párr. 4.

> El término «privacidad por diseño» fue utilizado por primera vez por Ann Cavoukian cuando era Directora de Privacidad e Información de Ontario, Canadá. En su concepto, la privacidad por diseño puede desglosarse en «**7 principios básicos**»,[437] con énfasis en la necesidad de adoptar un **enfoque proactivo** al abordar los requisitos de privacidad [o en términos de la UE, protección de datos] en la fase de diseño durante todo el ciclo de vida de los datos, que deben «*implantarse en el diseño y la arquitectura de sistemas TIC y prácticas comerciales... sin disminuir la funcionalidad...*», con la privacidad como configuración predeterminada, la seguridad de principio a fin, incluida la destrucción segura de los datos, y una fuerte transparencia sujeta a verificación independiente. El principio de privacidad por defecto se recabó como el segundo principio fundacional, estableciendo que la privacidad por defecto implica «*garantizar que los datos personales queden protegidos automáticamente en cualquier sistema o práctica comercial de TI*. *Si una persona no hace nada, su privacidad continúa intacta. No es necesario tomar ninguna acción por parte de la persona para proteger su privacidad — **se incorpora en el sistema, por defecto».*** Esta declaración es una definición operativa muy potente del principio de privacidad por defecto, en el que la persona no soporta la carga de tener que esforzarse por conseguir la protección al usar un producto o servicio, sino que disfruta «automáticamente» (sin necesidad de un comportamiento activo) del derecho fundamental a la privacidad y a la protección de datos personales.

En opinión del SEPD, «protección de datos por diseño» tiene **varias dimensiones**; para parafrasear:[438]

- la **primera dimensión** es que las operaciones de tratamiento de datos personales deben ser ***el resultado de un proyecto de diseño***, que cubra ***el ciclo total del proyecto***, dentro del cual puedan identificarse claramente los riesgos y requisitos de protección de datos;
- la **segunda dimensión** es que el proyecto de diseño debe basarse en un ***enfoque de gestión del riesgo*** dentro del cual los activos que se han de proteger son ***las personas cuyos datos se van a tratar y, en especial, sus derechos y libertades fundamentales***;
- la **tercera dimensión** es que las medidas que se han de adoptar para proteger los derechos y libertades de dichas personas deben ser ***adecuados y eficaces*** en relación con dichos riesgos, puestos a la luz de los principios de protección de datos indicados en el artículo 5 del RGPD, que pueden verse como ***objetivos que se han de alcanzar***;
- la **cuarta dimensión** es la obligación de ***integrar las garantías identificadas [necesarias, adecuadas y eficaces] en el tratamiento***.

Añade que:[439]

> **Las cuatro dimensiones son igualmente importantes, y suponen una parte fundamental de la responsabilidad corporativa,** y quedarán sujetas a supervisión por

---

437 Veáse: Los «siete principios fundacionales» son: 1. Proactivo, no reactivo, preventivo, no correctivo; 2. La privacidad como configuración por defecto; La privacidad implantada en el diseño; 4. Funcionalidad plena — Resultado positivo, no suma cero; 5 Seguridad de terminal a terminal — Protección del ciclo de vida completo; 6. Visibilidad y transparencia — Mantener un enfoque abierto; 7 Respeto de la privacidad del usuario — Mantener el enfoque centrado en el usuario. [original footnote] https://www.ipc.on.ca/wp-content/uploads/2018/01/pbd.pdf

438 Para acceder a los datos completos de dichas dimensiones según las ve el SEPD, ver su Opinión Preliminar 5/2018 (nota al pie 437, anterior), pp. 6 – 7 (párr. 27 – 32).

439 *Ídem*, p. 7, párr. 32, se ha añadido la letra negrita.

> parte de las autoridades de supervisión de protección de datos pertinentes, cuando corresponda.

El SEPD remarca la importancia de la protección de datos por diseño y defecto en relación con variedad de actores: responsables y encargados a nivel general;[440] desarrolladores de productos y tecnologías (sensibles a efectos de privacidad);[441] servicios de comunicación electrónica;[442] servicios de identidad electrónica;[443] proveedores de contadores y redes «inteligentes».[444] En relación con las **administraciones públicas**, el SEPD destaca que:[445]

> El artículo 25 es de aplicación a todo tipo de organizaciones que actúen como responsables, incluyendo las administraciones públicas, que, atendiendo a su papel al servicio del interés público, **deben dar ejemplo en lo que concierne a la protección de los derechos y libertades individuales fundamentales.** El RGPD subraya el papel de protección de datos desde el diseño y por defecto, cuando las administraciones públicas deben identificar a sus proveedores de productos y servicios en el Considerando 78, e indica que ***«Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos».*** **Las administraciones públicas deben estar en primera línea en lo que se refiere a la aplicación de esos principios de forma responsable, y listas para demostrar su implantación**, si fuera necesario, ante la autoridad de supervisión competente.

Es especialmente relevante la referencia a los **contratos públicos**: El DPD deberá aconsejar a su organización que, en la emisión de dichos contratos, las administraciones públicas deberán convocar expresamente a solicitantes que puedan «demostrar» que su producto o servicio cumple, en su totalidad, con el RGPD (y cualquier otra ley relevante en materia de protección de datos a nivel nacional o de la UE),[446] y que han incorporado «protección de datos desde el diseño y por defecto» en el producto o servicio correspondiente. Deberá ser posible dar una ***ventaja competitiva*** a dichos solicitantes, por encima de aquellos otros cuyos productos o servicios no cumplan con dichos requisitos.[447]

El CEPD comenta, con cierta amplitud, las distintas metodologías que se han desarrollado para implantar la protección de datos desde el diseño y por defecto.[448] No pueden desarrollarse aquí por completo, ni parafrasearse, pero los DPD deberán familiarizarse completamente con ellos (de hecho, con más detalle del que se indica en el documento del SEPD). Basta señalar que **el SEPD vincula adecuadamente la privacidad desde el diseño y por defecto con las evaluaciones de impacto de protección de datos (EIPD)**, tal y como se analiza en la Función 4, anterior);[449] y de forma más general que, como también subraya el CEPD:[450]

> **El papel de los delegados de protección de datos y de privacidad es fundamental, y su**

---

440 *Ídem*, p. 7, párr. 35 – 36.

441 *Ídem*, p. 7, párr. 37.

442 *Ídem*, pp. 8 – 9, párr. 42 – 44 (con referencia a la Directiva sobre Privacidad electrónica y a la propuesta de Reglamento sobre Privacidad electrónica).

443 *Ídem*, p. 9, párr. 45 (con referencia al Reglamento eIDAS).

444 *Ídem*, pp. 9 – 10, párr. 46 – 50 (con referencia a la Recomendación sobre plantilla de la EIPD de medición inteligente).

445 *Ídem*, p. 8, párr. 38, cursiva en el original, se ha añadido la letra negrita.

446 Ver el análisis del principio de «responsabilidad corporativa» de la Parte Dos, apartado 2.4, anterior.

447 Este enfoque se adopta expresamente en virtud de la ley de protección de datos de Schleswig-Holstein.

448 CEPD, Opinión preliminar 5/2018 (nota al pie 437, anterior, pp. 13 – 15, párr. 63 – 72. Ver, asimismo, las referencias específicas al programa de ingeniería de privacidad NIST de EE.UU., y su informe sobre ingeniería de privacidad y gestión del riesgo para los sistemas federales de EE.UU. (P. 11, párr. 56, pies de página 76 y 74) y el análisis ENISA 2014 de las posibilidades técnicas (en ese momento) 12, párr. 59, pie de página 82).

449 *Ídem*, p. 8, párr. 39 – 40.

450 *Ídem*, p. 15, párr. 76, énfasis añadido.

> **implicación es crucial en un enfoque desde el diseño y por defecto.** Es necesario que estén al tanto desde las fases tempranas, cuando las organizaciones planifican sistemas para el tratamiento de datos personales, de modo que puedan dar apoyo a los directivos, propietario del negocio, y departamentos de TI y de tecnologías, según sea necesario. Su conjunto de habilidades deberá ajustarse a dichos requisitos.

Dicho «conjunto de habilidades» deberá incluir estar **totalmente formado y cualificado en las metodologías y tecnologías relevantes** (si fuera necesario, mediante formación adicional en el mercado de trabajo), y estar **profundamente involucrado en el diseño, desarrollo, ensayo, y ajuste de todos los productos, servicios y acciones sensibles para la privacidad de su organización** (incluyendo los concursos públicos, como se ha indicado), en todas las fases.

- o – O – o –

FUNCIÓN 10: Asesorar y supervisar sobre el cumplimiento normativo de las políticas de protección de datos, de los contratos de corresponsables del tratamiento, responsable-responsable y responsable-encargados, Normas corporativas vinculantes y cláusulas de transferencia de datos

Para cumplir con el RGPD y, especialmente, para «demostrar» dicho cumplimiento normativo, los responsables pueden y deben adoptar o adherirse a un conjunto de medidas. Tal y como se indica en el apartado 2.2.2, anterior, estas incluyen:

- Preparación y adopción formal de **políticas internas de protección de datos** (ver artículo 24, apartado 2), para regular asuntos como:
  - ✓ **Formularios en papel, electrónicos, declaraciones sobre privacidad/protección de datos en páginas web**, uso de **cookies** y otros rastreadores de la organización;
  - ✓ **registros de acceso y alteración**, etc., en software y hardware relevante;
  - ✓ la emisión de «**parches de seguridad**» para su propio software;
  - ✓ etcétera;
- la adopción de **acuerdos administrativos** («**acuerdos**») entre autoridades o entidades públicas, especialmente si puede afirmarse que sean «corresponsables» sobre determinadas operaciones de tratamiento;
- Adhesión y aceptación de **contratos relevantes con otros responsables y encargados**; y
- Adhesión o aceptación de **contratos de transferencia de datos aprobados individualmente o estándar**.

El punto principal en el que debemos insistir aquí es que todas estas responsabilidades (medios para «demostración del cumplimiento normativo») del responsable más que del DPD (ver el subapartado sobre «*La no responsabilidad del DPD sobre cumplimiento normativo con el RGPD*», en el Apartado Dos, sección 2.5.4 anterior).

No obstante, en la práctica, el DPD debe estar involucrado en todos esos asuntos. Como mínimo, cualquier nuevo DPD y, especialmente cualquier DPD nombrado para una organización que no tuviera un DPD previamente, deberá **revisar** cualquier documentación e instrumentos existentes de este tipo, para comprobar si continúan cumpliendo con todos los requisitos legales de protección de datos.

Sobre la base de dicha revisión, deberá **recomendar cambios sobre los documentos actuales**, etc., especialmente si hubieran sido preparados y adoptados con anterioridad a la adopción y entrada en vigor del RGPD; y deberá **recomendar la preparación y la adopción de dichos documentos, etc.**, si (en su opinión) debieran existir dichos documentos, etc., pero no existen.

Además, el DPD *está* formalmente a cargo de **supervisar** el cumplimiento de lo dispuesto en cualquier política, acuerdo y contrato que adopte o formalice el responsable en relación con el tratamiento de datos personales (ver art. 39, apartado 1, letra b).

FUNCIÓN 11: Implicación en códigos de conducta y certificaciones

Tal y como comentamos en la Parte dos, apartado 2.2.2, anterior, la adhesión a, y total cumplimiento de, un **código de conducta** aprobado, o una **certificación de protección de datos** aprobada, podría servir asimismo como elemento o medio relevante para demostrar el cumplimiento del RGPD en relación con los asuntos que abarquen dichos códigos o certificaciones. (sin que esto pueda equivaler a una prueba legal de cumplimiento)

De nuevo, será, en última instancia el responsable – y no el DPD – quien decidirá si adherirse a un código relevante para el sector en el que opere la organización, o si tratar de obtener una certificación de protección de datos del tipo que se contempla en el Reglamento (ver arts. 40 – 43). No obstante, es totalmente aceptable que un DPD **recomiende** dicha acción.

De hecho, puede ser bastante apropiado que los DPD u organizaciones que operen en un determinado sector se impliquen en la **preparación de (un) código(s) de conducta** para dicho sector, aunque deberá implicar asesoramiento jurídico y a los miembros del personal de la organización sectorial al amparo de la cual se prepare (incluyendo, especialmente, al personal de TIC si el código aborda asuntos técnicos como seguridad TIC, cifrado, etc.).

El DPD podrá, además, **colaborar en la obtención de un certificado** por parte de su organización, ayudando a agrupar o proporcionar, al Organismo de certificación correspondiente, «toda la información y acceso a sus actividades de tratamiento que necesite para llevar a cabo el procedimiento de certificación». (art. 42, ap. 6). No obstante, si un sistema de certificación se basa en una **evaluación** de las operaciones de tratamiento de datos del responsable por parte de uno más ***peritos independientes*** certificado por el órgano de certificación relevante (tal y como ocurre en el sistema de certificación de la UE, el sistema *European Privacy Seal [EuroPriSe]*),[451] el DPD no podrá actuar como tal, pues incurriría en un conflicto de intereses.

Nota: En cierta medida, el registro detallado de las evaluaciones de impacto de protección de datos (EIPD), que se examina en la Función 4 anterior, y el seguimiento continuo de las operaciones, discutido en la Tarea 5, arriba (y los registros de ese seguimiento continuo) cumplen una función similar a la de las certificaciones, en la medida que estos registros muestran que el responsable del tratamiento y su personal han examinado detenidamente todas las implicaciones para la privacidad y la protección de datos de las operaciones pertinentes de tratamiento de datos personales, han identificado y cuantificado los riesgos que entrañan para los derechos fundamentales de las personas afectadas y han adoptado las medidas atenuantes adecuadas. La ventaja de las certificaciones sobre este asunto es que la evaluación es realizada por expertos externos e independientes. Sin embargo, mucho dependerá de la calidad de los sistemas de certificación acreditados y de cómo se interrelacionarán con la aplicación por parte de las APD.

- o – O – o -

[451] Veáse: https://www.european-privacy-seal.eu/EPS-en/fact-sheet

Cooperación con y consulta a la APD

FUNCIÓN 12: Cooperación con la APD

El DPD tendrá la Función de responder a solicitudes que provengan de la APD y, dentro de la esfera de su competencia, cooperará con la APD cuando así se lo solicite o a su propia iniciativa (art. 39, ap. 1, letra d).

A este respecto, el GT29 apunta que:[452]

> Dichas funciones hacen referencia al papel de «facilitador» del DPD que se menciona en la introducción a estas Directrices. El DPD actúa como punto de contacto para facilitar el acceso a la autoridad de supervisión a los documentos y la información para llevar a cabo las funciones mencionadas en el artículo 57, así como para el ejercicio de sus poderes de investigación, correctivos, de autorización y consultivos mencionados en el artículo 58. El delegado de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros (artículo 38, apartado 5). No obstante, la obligación de guardar secreto/confidencialidad no prohíbe al DPD contactar y consultar a la autoridad de supervisión. El artículo 39, apartado 1, letra b establece que el DPD podrá realizar consultas a la autoridad de control sobre cualquier otro asunto, cuando sea necesario.

El SEPD ha aumentado más la información, de forma útil, sobre las funciones equivalentes de los DPD institucionales de la UE, en sus relaciones con el SEPD, tal y como se indica en las citas siguientes con enmiendas textuales para aplicar las palabras del SEPD, *mutatis mutandis*, a la relación entre las autoridades de protección de datos de los Estados Miembros (APD) (y el CEPD) y los DPD nombrados en virtud del RGPD. En primer lugar indica, en términos generales, que:[453]

> El DPD tendrá la Función de responder a solicitudes que provengan de la [autoridad de protección de datos relevante] y, dentro de la esfera de su competencia, cooperará con la [APD] cuando así se lo solicite o a su propia iniciativa. Esta función pone en énfasis en el hecho de que el DPD facilita la cooperación entre la [APD] y la institución, especialmente en el marco de investigaciones, gestión de denuncias o verificaciones previas. El DPD no cuenta únicamente con conocimientos internos de la entidad, sino que también es probable que sepa quién es la mejor persona con la que contactar dentro de la entidad. El DPD también puede estar informado, e informar debidamente a la [APD], de desarrollos recientes que puedan afectar a la protección de datos personales.

El SEPD aborda con más detalle, seguidamente, los distintos asuntos mencionados en términos que son de aplicación también a los asuntos en virtud del RGPD, del siguiente modo:[454]

> **IV. Relación DPD – [APD]**
>
> El proceso de garantía del cumplimiento del Reglamento se verá afectado por la relación laboral entre el DPD y la [APD correspondiente]. No debe considerarse al DPD como un agente de la [APD], sino como parte de la institución/organismo en que trabaja. Tal y como se ha mencionado anteriormente, la idea de proximidad le sitúa en una situación idónea para asegurar el cumplimiento desde dentro y poder asesorar o intervenir en una etapa más temprana, evitando de este modo la posible intervención de la entidad de

---

452 Directrices sobre DPD del GT29, (nota al pie 242, arriba), p. 18.

453 Documento expositivo sobre DPD del SEPD (nota al pie 243, anterior), p. 6. Cambios textuales entre corchetes.

454 *Ídem*, Parte IV (pp. 10 – 11).

supervisión. Al mismo tiempo, la [APD] puede ofrecer un apoyo útil para los DPD con respecto al desarrollo de sus funciones.[455]
[Cabe esperar que las APD][456] apoyen, por tanto,[] la idea del desarrollo de sinergias posibles entre los DPD y las [APD], que contribuiría a alcanzar el objetivo general de protección eficaz de datos personales dentro de las instituciones....

IV. 1. Asegurar el cumplimiento normativo

Asegurar el cumplimiento normativo comienza, principalmente, por aumentar el nivel de concienciación. Tal y como se ha mencionado más arriba, los DPD juegan un papel importante en el desarrollo de conocimientos sobre asuntos de protección de datos a nivel interno de la institución/organismo. [Puede esperarse que las APD][457] acojan esto con satisfacción, así como sus consecuencias en términos de estimular un enfoque preventivo eficaz en lugar de una supervisión represiva de protección de datos.
El DPD proporciona, igualmente, asesoramiento a la institución/entidad sobre recomendaciones prácticas para la mejora de protección de datos a nivel de la institución/entidad o con relación a la interpretación o aplicación del [RGPD].[458] Esta función consultiva se comparte con las [APD], quienes asesorarán a todas sus instituciones/entidades [nacionales] relativas al tratamiento de datos personales ([artículo 57, apartado 1, letra c del RGPD]). En esta área, los [DPD nacionales han sido, en el pasado] a menudo llamados a asesorar a los DPD sobre asuntos específicos relativos a protección de datos (enfoque caso por caso). Puede esperarse que las [APD y el CEPD] emitan documentos expositivos sobre determinados asuntos, para ofrecer directrices sobre asuntos más generales a las instituciones/organismos.[459]

IV.2 Verificaciones previas

Las opiniones que emita [una APD] en el marco de una [consulta previa de las previstas en el artículo 36 del RGPD] [y las opiniones que expresa la APD en el proceso de emisión de autorizaciones previas, tal y como contempla el artículo 36, apartado 5, del RGPD], son, asimismo, una ocasión para que la [APD] supervise y garantice el cumplimiento del [RGPD]. ...[460]

---

455 Ver la disposición de la autoridad **francesa** de protección de datos, el CNIL, de una «extranet» especial para DPD registrados, a la que solo podrán acceder mediante un nombre de usuario y contraseña, que les ofrece textos legales (leyes, decretos, etc.), así como formación e información, incluyendo información sobre nuevos informes o directrices emitidas por el CNIL, y sobre otros desarrollos legales y prácticos, y les permite intercambiar opiniones y debatir asuntos. Véase el apartado 2.3.5, bajo el epígrafe "Formación y certificación formales", y nota al pie 274 anterior.

456 La frase original dice que el SEPD «apoya» la idea. Puede esperarse que tanto las APD (como el SEPD) adopten la misma postura.

457 La frase original afirma que el SEPD «acoge con satisfacción» este enfoque, pero puede esperarse, de nuevo, (también a la luz de sus prácticas anteriores) que las APD (y el CEPD) adopten la misma postura.

458 En el documento del SEPD se hace referencia al Reglamento por el que se establecen las normas de protección de datos para las instituciones de la UE (Reglamento (CE) 45/2001) (nota al pie 148, anterior), pero, por supuesto, lo mismo ocurre en relación con el RGPD en lo que respecta a los DPD nombrados en virtud de este último Reglamento. Hemos hecho reemplazos similares en otros lugares de la cita.

459 La frase original dice que el SEPD «pretende elaborar» documentos expositivos y directrices. Una vez más, puede esperarse que las APD nacionales y el CEPD hagan lo mismo en relación con el RGPD.
La sentencia omitida dice lo siguiente: «Con respecto a los DPD nombrados en virtud del RGPD, las APD nacionales, pero también especialmente el nuevo CEPD, emitirán, sin duda alguna, directrices similares».

460 El resto de este apartado, y la frase omitida al principio del siguiente, se refieren al hecho de que la diferencia de tiempo entre la entrada en vigor del Reglamento y el nombramiento del SEPD dio lugar a un gran retraso de casos que están siendo «controlados previamente» a posteriori. Todavía no está claro si están surgiendo problemas similares en el marco del RGPD. En caso afirmativo, la petición del SEPD de que los DPD y el regulador sean «socios estratégicos» en la resolución de este problema también debería tenerse en cuenta en ese contexto.

...[Antes de la adopción final de una opinión previa de control, la[APD podrá][461] enviar[] un proyecto provisional al DPD con información sobre las recomendaciones previstas, abriendo así un espacio para el debate sobre la eficacia y las consecuencias de las recomendaciones previstas. [Puede esperarse que las APD] presten atención a los asuntos de la institución, según indica el DPD, para trabajar en recomendaciones que sean factibles.

IV. 3. Ejecución

En el área de implantación de medidas específicas de protección de datos, el potencial de sinergias entre los DPD y [APD] emerge con respecto a la adopción de sanciones y al procesamiento de denuncias y preguntas.

Tal y como ya se ha mencionado, el DPD cuenta con poderes limitados de ejecución. La [APD] contribuirá a garantizar el cumplimiento normativo del [RGPD], adoptando medidas eficaces en el ámbito de [consultas o autorizaciones] previas y de denuncias y otras investigaciones. Las medidas serán eficaces si su objetivo está bien definido y es factible: el DPD puede ser visto, asimismo, como un socio estratégico a la hora de determinar la aplicación bien orientada de una medida.

La gestión de denuncias y consultas por parte del DPD a nivel local[462] deberá ser fomentada, al menos, en lo relativo a una primera fase de investigación y de resolución. Por tanto,[463] [podrá esperarse que la APD adopte la postura] de que los DPD deban tratar de investigar y resolver denuncias a nivel local antes de recurrir a la [APD]. El DPD deberá, asimismo, …consultar con la [APD] cuando tenga dudas sobre el procedimiento o el contenido de las denuncias. No obstante, esto no impide al interesado presentar una reclamación ante una autoridad de control directamente [artículo 77, apartado 1 del RGPD]. Los poderes limitados de ejecución del DPD implican, igualmente, que en algunos casos, la denuncia o consulta deba escalarse a la [APD]. Por tanto, la [APD] ofrece un soporte válido en el ámbito de la ejecución. A su vez, puede confiarse en que el DPD proporcione información a la [APD] y ofrezca seguimiento de las medidas adoptadas.

IV.4. Medición de la eficacia[464]

En lo que respecta a la medición de la eficacia de la implantación de los requisitos de protección de datos, el DPD debe ser visto como un socio útil para evaluar el progreso en esta área. Por ejemplo, en lo relativo a la medición del rendimiento de la supervisión interna de protección de datos, [puede esperarse que las APD fomenten [] que los DPD desarrollen su criterio propio de supervisión óptima (normas profesionales, planes específicos para la institución, programa anual de trabajo...) Dichos criterios, a su vez,

---

461 La práctica de enviar «borradores de recomendaciones provisionales» a un responsable en el contexto de un proceso de una «consulta previa»/ «autorización previa» no se especifica en el RGPD (o en el Reglamento 45/2001). No obstante, el hecho de que el RGPD se refiera a «consulta previa» sugiere en gran medida que la APD, en virtud de dicho instrumento, adoptará un enfoque similar; y esto se refleja en la redacción entre corchetes que se añade dos veces al presente apartado.

462 Es necesario indicar que la gestión de solicitudes y denuncias de interesados se comenta con más detalle en la Función 11, más abajo.

463 Las dos primeras frases de este párrafo remiten, de nuevo, a prácticas promovidas por el SEPD, pero, de nuevo (también a la vista de prácticas anteriores) se espera que las APD nacionales adopten el mismo enfoque (que se indica en el texto entre corchetes).

464 No hay ningún requisito específico, en el Reglamento 45/2001 (con respecto a las instituciones de la UE), o en el RGPD (con respecto a entidades cubiertas por ese instrumento), para el organismo regulador correspondiente, el SEPD y las APD nacionales) para «medir la eficacia» de las medidas que adopten los responsables, con el objetivo de garantizar el cumplimiento normativo del instrumento de aplicación. Dentro del marco institucional de la UE, el SEPD lo ve (acertadamente) como parte natural de su trabajo. Cabe esperar que las APD de los Estados Miembros (y el CEPD) «fomentan» también que los DPD contribuyan al cumplimiento de alto nivel durante el proceso de adopción o de adhesión de «normas profesionales, planes específicos para la institución, programa de trabajo anual», etc.; tal y como se refleja de nuevo en el texto entre corchetes.

> permitirán a la [APD], si se la invita a hacerlo, evaluar el trabajo del DPD, pero servirán de igual modo para medir el estado de implantación del [RGPD] dentro de la institución/entidad.

También es probable que las DPO soliciten a los responsables de la protección de datos que contribuyan a las consultas celebradas por las autoridades responsables de esta materia, y que aporten su contribución cuando una autoridad de protección de datos esté preparando un dictamen oficial sobre propuestas o proyectos de ley en el ámbito de la protección de datos que se refieran al contexto en el que opera el responsable de la protección de datos.

Por último, debe señalarse **que el DPD juega un papel importante ayudando a la APD en su ejecución de las inspecciones in situ**, en las consultas del DPD con los responsables en sectores específicos, etc. Por ejemplo, es raro que una APD lleve a cabo inspecciones sin aviso previo, esto se hace tan solo en relación con elementos peligrosos sospechosos que puedan ocultar datos u otras evidencias, si se les informa previamente de una inspección. En la práctica, las APD suelen acordar las inspecciones previamente, con la ayuda del responsable, y en especial el DPD del responsable, quien podrá garantizar que esté disponible la persona adecuada y que puedan inspeccionarse los lugares y sistemas adecuados. Esto es, a menudo, crucial, especialmente en relación con sistemas complejos de tratamiento, cuando se requieran procesos internos y conocimientos exhaustivos de la arquitectura TIC para una revisión adecuada. Asimismo, en el caso de que una APD pretenda examinar en detalle el tratamiento de datos personales en un contexto o sector particular, pues la mayoría lo hacen en un plan determinado anualmente y selección de prioridades- recurrirán al DPD de los responsables activos en el contexto o sector para obtener información real, celebrando reuniones con ellos y solicitando respuesta a sus consultas. Esto es, también, parte de lo que el SEPD denomina «asociación estratégica» entre los DPD y las APD.

- o – O – o -

Gestión de peticiones sobre protección de datos personales

FUNCIÓN 13: Gestión de peticiones sobre protección de datos personales y denuncias

El RGPD establece que:

> Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento.
> (Art. 38, apartado 4)

Los interesados que deseen ejercitar alguno de sus **derechos como interesados** - derechos de acceso, rectificación y eliminación («derecho al olvido»), restricción del tratamiento, portabilidad de los datos, derecho a oponerse en general y en relación con toma de decisiones automática y perfilado, con respecto a cualquier organización, o que tengan **preguntas generales** o **denuncias** vinculadas a protección de datos sobre la organización, se dirigirán, por lo general, en primer lugar al DPD de dicha organización (si existe uno).

Esto se ve facilitado por los requisitos incluidos en el RGPD de que los datos de contacto del delegado de protección de datos serán publicados por la organización (art. 37, ap. 7) y que el responsable deberá asegurar «*que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales*» (art. 38, ap. 1). (Así, si un interesado tiene que dirigirse a otra persona de dentro de la organización, como al asesor general o el director general, deberán enviar la solicitud al DPD.)

Además, la independencia del DPD (art. 38, ap.3) deberá garantizar que la solicitud, pregunta o denuncia sea gestionada por el DPD – o por los miembros del personal a quienes supervise el DPD – de **forma adecuada, sin tendencia en favor de la organización o contra el interesado**.

En cualquier caso, el DPD deberá escribir o revisar la respuesta al interesado. Esto incluirá el consejo de que, si el interesado no queda satisfecho con la respuesta, podrá elevar el asunto a la APD.

Esto es porque, en todo caso, el derecho de los interesados a enviar solicitudes, consultas y denuncias a la organización (es decir, al DPD de la organización) lo es **sin perjuicio de su derecho a presentar una reclamación ante la APD**. De manera específica, cada APD, en su propio territorio, tiene la obligación y la capacidad de:

> tratar las reclamaciones presentadas por un interesado... e investigar, en la medida que corresponda, el motivo de la reclamación e informar al reclamante sobre el progreso y el resultado de la investigación...
> (Art. 57(1)(f))

En dichas reclamaciones a la APD, los interesados podrán ser representados por una entidad sin ánimo de lucro relevante (art. 80), y la obligación y capacidad arriba mencionadas de la APD de tratar dichas reclamaciones se amplía a casos que se tramiten de esta forma (ver el texto del artículo 57(1)(f), que se ha omitido de la cita anterior).

En ese contexto, tendría sentido que los DPD también estén dispuestos a tener en cuenta solicitudes y **reclamaciones que provengan de dichas organizaciones de representación**, y no solo de los interesados.

Tal y como consta en relación con la Función 10 (*Cooperación con la APD*), es de esperar (habida cuenta de la práctica pasada) que las APD nacionales (como el SEPD en relación con los DPD institucionales de la UE) fomentarán que los interesados (y dichas organizaciones) aborden siempre en primer lugar cualquier asunto con el responsable, y más específicamente,

con el DPD del responsable, para saber si el asunto no puede investigarse y ser resuelto de forma satisfactoria en dichas interacciones, sin involucrar a la APD, con arreglo a la disposición de que el DPD deberá consultar a la APD si surge cualquier cuestión sobre la interpretación general y aplicación del RGPD. No obstante, esto nunca deberá llegar al punto de disuadir a los interesados (u organizaciones representantes) de remitir asuntos, y, especialmente, cuestiones de principio, ante la APD.

Tal y como indica el SEPD, el regulador y los DPD forman una «asociación estratégica»: las APD pueden fomentar que los interesados, en primer lugar y, sobre todo, resuelvan cualquier asunto directamente con los DPD; y los DPD deberán poder, y se requiere que trabajen con el organismo regulador para asegurar que las respuestas a las preguntas y a las denuncias se gestionen de forma adecuada y, si fuera necesario, conlleven cambios en las prácticas relevantes del organismo regulador. La APD deberá poder contar con el DPD para apoyar realmente a los interesados en cualquier reclamación; y los DPD deberán poder contar con las APD para garantizar que se ejecuten las recomendaciones de cambio.

Con esto, se refuerza la sutilidad del puesto del DPD, que se comenta en la Parte Dos, apartado 2.5: el DPD actúa como puente entre responsable y organismo regulador, y (para combinar, de alguna manera, las metáforas, salvo que se entienda puente como pasarela) no debería poder caer entre el barco y el muelle.

- 0 – O – o -

Información y sensibilización

FUNCIÓN 14: Funciones de información y sensibilización interna y externa

El RGPD establece que las funciones del DPD deberán incluir, «como mínimo»

> informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros
> (Art. 39(1)(a))

A nivel interno (dentro de la organización en la que trabaja el DPD), esto conlleva, por un lado, que el DPD **debe informar** al personal de sus derechos y, por el otro, que el DPD **debe instruir** a los responsables y a la organización y miembros del personal, incluyendo, en particular, a «propietarios de negocios»/personas responsables de la operación específica, sobre sus obligaciones y responsabilidades, y **formales** sobre cómo cumplirlas.

Tal y como indica el SEPD en un fragmento citado más arriba:[465]

> Asegurar el cumplimiento normativo comienza, principalmente, por aumentar el nivel de concienciación. ...los DPD juegan un papel importante en el desarrollo de conocimientos sobre asuntos de protección de datos a nivel interno de la institución/organismo.

La sensibilización «estimula un enfoque preventivo eficaz, en vez de un modelo represivo de supervisión de protección de datos».[466]

Las medidas adoptadas por el DPD hacia estos objetivos podría incluir la emisión de **notas informativas para el personal**, la organización de **sesiones de formación** interna sobre protección de datos, que deberán estar orientadas a inculcar en el personal una conciencia y sensibilidad con respecto a la protección de datos y a los derechos de los interesados, un «reflejo sobre protección de datos», en sus distintos roles sociales, ya sea como un ciudadano de a pie, un trabajador, un jefe de equipo o un alto directivo.

Asimismo, la creación de una **página web** sobre formación e información en protección de datos, y la preparación y emisión de **declaraciones de privacidad** en sitios y páginas web de personal.[467]

Externamente, además de garantizar que se ofrezca información relevante a los interesados cuando se recojan por primera vez sus datos personales (según se indica en los artículos 12 – 14 del RGPD), por ejemplo, mediante avisos claros en páginas web, el DPD deberá trabajar, igualmente, con personal de relaciones públicas para garantizar **la plena transparencia sobre las operaciones personales de protección de datos de la organización**: sobre los fines para los que recoge y trata datos personales; las categorías de los interesados y los datos involucrados; los receptores de datos; si los datos se transfieren a terceros países (externos a la UE/EEE), etc.

El RGPD no requiere a los responsables poner a plena disposición del público el registro de sus operaciones de tratamiento de datos personales.[468] No obstante, el RGPD tampoco lo prohíbe.

El SEPD argumenta enérgicamente a favor de la publicación a las instituciones de la UE, en particular a la luz del hecho de que (como en la Directiva de 1995 sobre Protección de Datos)

---

465 Documento expositivo sobre DPD del SEPD (nota al pie 243, anterior), p. 10.

466 *Ídem*.

467 *ídem*, p. 5.

468 Por el contrario la Directiva de 1995 sobre Protección de Datos requería a las APD hacer públicos los detalles de las operaciones de tratamiento que se les notificaran (art. 21).

una norma anterior requería que publicaran sus detalles de notificación «funcionalmente equivalentes»:[469]

> Los registros son una herramienta importante para verificar y documentar que su organización controle sus actividades de tratamiento. ….
> **El SEPD recomienda enérgicamente que [las instituciones de la UE] pongan sus registros a disposición del público, preferiblemente mediante su publicación en internet...**
> Existen muchas razones por las que el registro de archivos debería ser público:
>
> - Contribuye a la transparencia de las IUE;
> - Ayuda a reforzar la confianza del público;
> - Facilita la transmisión del conocimiento entre las IUE;
> - Si no se publica, implicaría dar un paso atrás hacia las [normas] antiguas.

Puede decirse prácticamente lo mismo en relación con el registro de operaciones de tratamiento que deban mantener los responsables en virtud del RGPD, al menos, en lo que concierne a las autoridades públicas. Algunos Estados Miembros podrán, dentro de su ley nacional, imponer dicho deber de publicar los datos del registro; pero las autoridades públicas en las que esto no sea obligatorio deberán plantearse hacerlo, a la luz de las conclusiones del SEPD.

Desde luego, los responsables y los controladores no deben sentirse obligados a publicar información sobre sus acuerdos en materia de seguridad que pudieran emplearse para incumplir dicha seguridad (esto ya se reconocía en la disposición de la Directiva de 1995 de Protección de Datos sobre publicación de operaciones de tratamiento que habían sido notificadas a las APD).[470]

En cualquier caso, la información básica sobre las operaciones de tratamiento de datos personales de la organización debe ser fácilmente accesible desde el **sitio web** de la organización, así como en **folletos** y **formularios** (incluidas las versiones accesibles para personas con discapacidad).

El sitio web y dichos formularios también deben proporcionar información clara sobre **la forma en que los interesados pueden ejercer sus derechos** (incluyendo un aviso público claro con los **datos de contacto del DPD**, aunque no es necesario incluir un nombre); qué **códigos de conducta** ha suscrito la organización y qué **certificaciones** ha obtenido (estas cuestiones pueden demostrarse por medio de **logotipos** o **sellos** reconocidos); etcétera.

Por supuesto, todo sitio web debe cumplir plenamente los requisitos de la legislación de la UE en materia de protección de datos, así como cualquier otra legislación nacional pertinente, en cuestiones como las **cookies** y otros **rastreadores**, etc.

- o – O – o -

---

469 SEPD, Responsabilidad corporativa sobre el terreno (nota al pie 353, anterior), p. 8, subrayado en el original.

470 Ver, de nuevo, el artículo 21 de la Directiva de 1995 de Protección de Datos, que excluye la información que se enumera en el artículo 19, apartado 1, letra f – es decir, una descripción general de las medidas de seguridad del responsable, de la información que debe hacerse pública. Obsérvese que la creencia en la «seguridad por oscuridad» fue descartada hace mucho tiempo, ver: https://en.wikipedia.org/wiki/Security_through_obscurity

FUNCIÓN 15: Planificación y revisión de las actividades del RPD

Por último, dado el gran número y alcance de las funciones del RPD, éste deberá preparar un plan anual de sus actividades, teniendo en cuenta el tiempo necesario para realizar cada una de ellas, planificando los nuevos eventos previsibles y teniendo tambien en cuenta los posibles acontecimentos imprevistos; para ello revisará y actualizará periodicamente esta planificacion.

Douwe Korff y Marie Georges
Cambridge/París, diciembre de 2018/ junio 2019