Seminari de Dret Local

Guía para el cumplimiento de protección de datos, especialmente el sector público local

(Uso docente)

Lorenzo Cotino Hueso
Catedrático de Derecho Constitucional
Universitat de València

CONTENIDO GENERAL

ÍNDICE DETALLADO

I. ¿Qué normas se aplican?

1. Normas afines

Normativa de transparencia

Entre otras, cabe tener en cuenta la **normativa de transparencia**, que incluye obligaciones de facilitar información en las webs institucionales o cuando la solicita un ciudadano. Hay que tener especialmente en cuenta la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y la legislación autonómica así como los criterios de las autoridades independientes de transparencia.

Reutilización y normativa de datos no personales

Hay que tener especialmente en cuenta la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público. Esta norma ha sido actualizada en varias ocasiones y pronto habrá de ser reformada para recibir la muy reciente Directiva (UE) 2019/1024, de 20 de junio de 2019.

La información y datos pueden no ser relativos a personas físicas, esto es, **datos no personales**. Además de la protección de los mismos como activo o propiedad, hay que tener en cuenta el reciente Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea, mediante el establecimiento de normas relativas a los requisitos de localización de datos, la disponibilidad de los datos para las autoridades competentes y la portabilidad de datos para los usuarios profesionales.

Normativa penal

La información y los datos en sistemas informáticos son un valor y activo de las organizaciones protegido frente a ataques, robos, intrusiones, etc. En este sentido hay que tener en particular la normativa penal. Así, en particular hay que centrar la atención en los Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, con especial atención a los delitos de los artículos 197-201 (acceso y revelación de secretos, vulneración de seguridad informática, intercepción,). También de especial interés son los delitos de daños a programas o datos informáticos (art. 264), obstaculización o interrupción de sistema informático (art. 264 bis), entre otros delitos.

Normativa de seguridad y ciberseguridad

Cabe remitir al Código de Ciberseguridad (BOE). Entre otras normas, cabe también tener en cuenta el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, exigible a los servicios esenciales y de los servicios digitales, que además establece un sistema de notificación de incidentes. Y muchas veces en paralelo a la normativa de protección de datos para el sector público hay que tener en cuenta el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional

de Seguridad en el ámbito de la Administración Electrónica que adquiere una importancia fundamental para el sector público.

.

2. Marco normativo de protección de datos y privacidad

El régimen de protección de datos viene determinado por una variada normativa española y de la UE. Es un derecho fundamental reconocido por tratados internacionales (en especial, art. 8 CEDH, Convenio n. 108 del Consejo de Europa, de 28 de enero de 1981, actualizado en 2018), la Carta de derechos fundamentales de la UE (Artículos 7 y 8) y por nuestra Constitución (art. 18. 4º CE), si bien la regulación general básica viene establecida por una Reglamento europeo que se aplica directamente a los estados de la UE. No obstante, este reglamento hay que complementarlo con la legislación española, en particular la Ley Orgánica 3/2018, de 5 de diciembre "adapta" el reglamento europeo a España. El jurista necesita tener en cuenta conjuntamente esta dos normas generales de protección de datos.

En buena medida, la normativa es la siguiente, de fácil seguimiento Código BOE de protección de datos.

• Constitución Española. Art. 18.4

• Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, 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.

• Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (Artículos 3, 6, 133, 346 y disposiciones adicionales 15ª, 16ª y 25ª).

• Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, modificada por Ley 18/2015, de 9 de julio y pendiente de incorporar la nueva Directiva de 2020.

• Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

• Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen

• Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas

• Ley 9/2014, de 9 de mayo, General de Telecomunicaciones

• Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza

• Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico

Para el ámbito penal y de justicia hay que tener en cuenta la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de

las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos.

La privacidad de las comunicaciones electrónicas está regulada por la 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) fue modificada mediante la Directiva 2009/136/CE, de 25 de noviembre de 2009.

En la actualidad se está examinando la nueva propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se derogaría la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas) y el nuevo reglamento de Inteligencia artificial en la UE.

3. Derecho "blando" de las instituciones y autoridades de protección de datos

Más allá de la normativa y normativa interna, diversas instituciones especializadas en materia de protección de datos generan documentos que podemos calificar de *Derecho blando*. No se tratan de normas jurídicas obligatorias o *duras*. Sin embargo, se trata de documentos emitidos por las autoridades que controlan el cumplimiento de la normativa de protección de datos. Es por ello, que en buena medida lo que afirman tales documentos acaba siendo la forma de interpretar correctamente las normas. Ello tiene especial importancia en ámbitos especialmente innovadores respecto de los que las normas no son concretas y se generan conflictos y dudas.

Directrices, dictámenes y documentos del Comité Europeo de Protección de datos y del –extinto- Grupo de Trabajo del artículo 29

GRUPO DE TRABAJO DEL ARTÍCULO 29

El Grupo de Trabajo del artículo 29 (GT Art. 29) es el grupo de trabajo independiente formado por las autoridades de protección de datos de los miembros de la UE y el Supervisor Europeo de Protección de datos. En este órgano se aúnan criterios de aplicación de la normativa y se elaboran dictámenes, estudios, informes, etc. Pese a que interpretara la normativa anterior, sus dictámenes e informes siguen siendo la referencia en muchas de las materias[1].

Desde 2018, con el RGPD, dejó paso al nuevo Comité Europeo de Protección de Datos (CEPD)[2]. El mismo establece las directrices generales de la legislación europea de protección de datos para dar una interpretación coherente. Para ello proporciona orientaciones (incluidas directrices, recomendaciones y buenas prácticas). Puede dictar

[1] Puede accederse a más de cien estudios, dictámenes e informes (muchos de ellos en español en) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm

[2] https://edpb.europa.eu/about-edpb/about-edpb_es

resoluciones vinculantes para las autoridades nacionales de supervisión para garantizar una aplicación coherente de la normativa.

Del G 29 cabe destacar ahora por su interés:

- Directrices del Grupo de Trabajo del Artículo 29 (WP 259) sobre el consentimiento regulado en el RGPD.
- Directrices sobre la toma de decisiones y la elaboración de perfiles individuales automatizados a los efectos del Reglamento 2016/679, WP251rev.01
- Dictamen 02/2016, del Grupo de Trabajo del Articulo (WP 239), relativo a datos personales para fines de transparencia en el sector público.
- Directrices sobre notificación de incumplimiento de datos personales en virtud del Reglamento 2016/679, WP250 rev.01
- Directrices sobre el derecho a la portabilidad de datos en virtud del Reglamento 2016/679, WP242 rev.01
- Directrices sobre la evaluación del impacto de la protección de datos (DPIA) y determinar si el procesamiento es "probable que genere un alto riesgo" a los efectos del Reglamento 2016/679, WP248 rev.01
- Directrices sobre oficiales de protección de datos ('DPD'), WP243 rev.01
- Pautas para identificar la autoridad supervisora principal de un controlador o procesador, WP244 rev.01
- Documento de posición sobre las excepciones a la obligación de mantener registros de las actividades de procesamiento de conformidad con el Artículo 30 (5) del RGPD

También de especial interés.

- Dictamen 06/2014, del Grupo de Trabajo del Artículo 29 (WP 217), relativo al concepto de interés legítimo.
- Dictamen 05/2014, del Grupo de Trabajo del Artículo 29 (WP 216), relativo a técnicas de anonimización.
- Dictamen 01/2014, del Grupo de Trabajo del Artículo 29 (WP 211), relativo a la aplicación de los conceptos de necesidad y proporcionalidad.
- Dictamen 03/2012, del Grupo de Trabajo del Artículo 29 (WP 193), relativo al desarrollo de las tecnologías biométricas.
- Dictamen 15/2011, del Grupo de Trabajo del Artículo 29 (WP 187), relativo a la definición de consentimiento.
- Dictamen 04/2007, del Grupo de Trabajo del Artículo 29 (WP 136), relativo al concepto de dato personal.
- Documento de trabajo del Grupo del Artículo 29 (WP 104), relativo a la relación entre protección de datos y derecho de propiedad intelectual.
- Documento de trabajo del Grupo del Artículo 29 (WP 67), relativo a videovigilancia.
- Documento de trabajo del Grupo del Artículo 29 (WP 55), relativo a la vigilancia de las comunicaciones electrónicas en el trabajo.
- Alguno de los documentos de especial interés del Comité Europeo[3]
- Escudo de privacidad UE - EE. UU.
- Declaración EDPB 3/2019 sobre una regulación de privacidad electrónica

[3] Acceso a documentos:
https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en
https://edpb.europa.eu/node/28

- Opinión 3/2019 sobre las preguntas y respuestas sobre la interacción entre el Reglamento de ensayos clínicos (CTR) y el Reglamento general de protección de datos (GDPR) - 23/01/2019
- Declaración de EDPB sobre ePrivacy - 25/05/2018
- Directrices 4/2019 sobre el Artículo 25 Protección de datos por diseño y por defecto - versión para consulta pública
- Directrices 3/2019 sobre el procesamiento de datos personales a través de dispositivos de video: versión para consulta pública
- Recomendación 01/2019 sobre el proyecto de lista del Supervisor Europeo de Protección de Datos con respecto a las operaciones de procesamiento sujetas al requisito de una evaluación de impacto de protección de datos (Artículo 39.4 del Reglamento (UE) 2018/1725)
- Directrices 2/2019 sobre el procesamiento de datos personales en virtud del Artículo 6 (1) (b) GDPR en el contexto de la prestación de servicios en línea a los interesados: versión adoptada después de consulta pública
- Directrices EDPB 3/2018 sobre el alcance territorial del GDPR (artículo 3) - versión adoptada después de consulta pública
- Directrices EDPB 1/2018 sobre certificación e identificación de criterios de certificación de conformidad con los artículos 42 y 43 del Reglamento - versión adoptada tras consulta pública

Durante su primera reunión plenaria, la Junta Europea de Protección de Datos aprobó las Directrices WP29 relacionadas con el GDPR:

Agencia Española de Protección de Datos

La Agencia Española de Protección de Datos es la autoridad independiente de nivel estatal, como función principal tiene la de vigilar y controlar el cumplimiento de la normativa de protección de datos por el sector público y privado. Asimismo, elabora informes y estudios de especial interés.

Entre sus documentos cabe destacar ahora[4]:

- Listado de elementos para el cumplimiento normativo Guía para responsables del tratamiento
- Guía para el cumplimiento del deber de informar
- Directrices para la elaboración de contratos entre responsables y encargados del tratamiento
- Guía para el ciudadano Conoce tus derechos
- Guía práctica de análisis de riesgos para el tratamiento de datos personales
- Guía práctica para las evaluaciones de impacto en la protección de datos personales
- Guía para la gestión y notificación de brechas de seguridad
- Guía para clientes que contraten servicios de Cloud Computing
- Orientaciones para prestadores de servicios de Cloud Computing
- Guía big data AEPD
- Guía para el responsable para el cumplimiento RGPD

[4] Acceso sencillo en https://www.lopdencastellon.com/manuales-aepd-rgpd/

- Guía para el cumplimiento del deber de informar de la AEPD y las agencias catalana y vasca.
- Guía cookies
- Orientaciones protección de datos reutilización
- Guía evaluación de impacto de protección de datos
- Guía cumplimiento RGPD
- Orientaciones y garantías procesos anonimización
- Estudio de impacto Guía eipd
- Resulta de especial interés la Guía EIPD APDCAT de la autoridad catalana
- Nota técnica "La K-anonimidad como medida de la privacidad".
- Orientaciones y garantías en los procedimientos de anonimización de datos personales.
- Guía sobre el uso de videocámaras para seguridad y otras finalidades.
- Orientación para la aplicación provisional de la Disposición Adicional Séptima de la LO 3/2018.

4. Los estándares o "normas" ISO

El RGPD hace referencia a los códigos de conducta y certificación artículos 40 a 43.

Aunque no son normas "oficiales" por cuanto provengan del Estado o de organizaciones internacionales públicas, son muy relevantes en el sector los estándares internacionales y en particular las normas ISO (International Organization for Standardization), e IEC (International Electrotechnical Comission). Con las mismas se puede para garantizar que los productos o servicios ofrecidos por dichas organizaciones cumplen con los objetivos de cada norma y sirven para acreditar niveles de cumplimiento garantizando a interesados y terceros un tratamiento de seguridad y protección de datos adecuado.

A través de esta normativa se estandarizan normas tanto para organizaciones públicas o privadas a nivel internacional. Ahora bien, en principio son normas de asunción voluntaria. No obstante, hay casos en los que la propia normativa "oficial" afirma que hay que cumplir con determinados estándares.

II. ¿Cuándo y dónde se aplica la normativa de protección de datos?

1. ¿Qué son “datos personales”, “fichero” y “tratamiento”?

¿Qué son "datos personales"?

Datos personales se definen en el RGPD[5] como “toda información sobre una persona física identificada o identificable (el "interesado"); se considerará persona identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente […], en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, unos datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de la persona.

Cabe alertar de un **equívoco común**, que los datos sean **“personales” no significa** “personales” según socialmente se entiende como equivalente a **“íntimos”.** Los datos relativos a personas vinculados a su vida más íntima, en muchos casos serán datos especialmente protegidos (art. 9 RGPD). El Dictamen 4/2007 del Grupo del artículo 29 sobre el concepto de datos personales recuerda que se trata de “Toda información” objetiva o subjetiva y que ni siquiera es necesario que se trate de información cierta.”

Para que la información se consideren datos personales y se aplique el régimen jurídico **ha de versar sobre una persona física “Identificada o identificable”**. Así pues, aunque no se haya identificado todavía a la persona, basta sea posible una identificabilidad potencial por singularización, vinculabilidad o inferencia. Determinar la identificabilidad de una información acaba resultando una cuestión esencial, no en vano, como señala el G29 “mientras los datos sean identificables, se aplica la legislación sobre protección de datos”.

El **juicio de la identificabilidad** puede ser muy complejo y al final “hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona”. El propio RGPD recuerda que para este juicio de identificabilidad “deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos” (Cons. 26). Hay que ir caso por caso de modo contextualizado. Así pues, puede acabar determinándose la identificabilidad en razón de la capacidad, naturaleza, tamaño, poder económico, empresarial o público del responsable de los datos con relación a que la información pueda llegar a ser relativa a personas concretas. Esto es, que una información sea dato personal o no depende sólo de dicha información, sino del sujeto que la trata y en qué contextos.

Por ejemplo se ha considerado dato personal la dirección de correo electrónico (Informe de 1999, SAN, Sección 1ª, de 22 de febrero de 2006, rec. 911/2003). Los datos relativos al ejercicio de una profesión (SAN, Sección 1ª, de 11 de febrero de 2004, rec. 119/2002); el Documento Nacional de Identidad (SAN, Sección 1ª, de 27 de octubre de 2004); el número de matrícula de vehículo ha llevado a respuestas contradictorias, no siendo en un dato personal para la SAN 5832 de 26/09/2013. Sí que lo es el número de historia clínica que pueda asociarse con la identidad del paciente (Informe 0283/2008), también el número de teléfono móvil cuando pueda vincularse con el titular de la línea o un número de teléfono (Informe 0575/2008, SAN, Sección 1ª, de 26 de enero de 2005 rec. 1258/2002); las fotografías o la imagen de una persona (Informe 0615/2008, STC

[5] Al respecto de este concepto de datos personales hay que tener en cuenta el Dictamen 4/2007 del Grupo del artículo 29 sobre el concepto de datos personales.

14/2003); el número de una finca en su inscripción registral (informe 0034/2010); un registro de huellas dactilares (Informe 0082/2010).Especialmente controvertido ha sido el caso del número IP. Así, la STJUE de 19 de octubre de 2016, caso C‑582/14 considera dato personal a la dirección IP dinámica registrada por un gestor de un sitio de Internet si éste dispone de medios legales que le permitan identificar al usuario.

Relacionado con la identificabilidad, está la cuestión de la anonimización, seudonimización y disociación de datos personales, precisamente para evitar la identificabilidad. Se trata de una cuestión esencial, especialmente para el régimen jurídico de la investigación y la protección de datos, si bien proyectable en todos los sectores también para el sector público.

Además del concepto dato personal resulta de interés tener en cuenta en el RGPD los conceptos de “Datos genéticos”, “Datos biométricos” o “Datos relativos a la salud" ahí definidos. Como se dirá, se trata de datos especialmente protegidos con un régimen jurídico y garantías especiales.

¿Qué es un fichero?

Otro de los vértices del triángulo es el concepto de “fichero”. No en vano se aplica la normativa cuando se tratan datos para ser incluidos en un fichero.

Para el RGPD lo es “**todo conjunto estructurado de datos personales**, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica”.

Como el art 5 y 56 Reglamento antigua LOPD ya regulara en España y ahora el artículo 31 LOPD 3/2018, un conjunto estructurado de datos se viene a entender como un fichero cuando puede reconducirse a la unidad en términos lógicos si los múltiples ficheros o aplicaciones están ordenados a una misma finalidad y encontrarse en un mismo repositorio de información.

En cualquier caso, el elemento esencial es que se trate de **información *estructurada*** y que, por ello, sea factible recuperar los datos personales del afectado. Y hay que estar atentos a que existan sistemas o herramientas de indexación que permitan ordenar y localizar información. Y ha llevado a considerar que son ficheros cuando se permiten por ejemplo búsquedas de texto (un mero documento en un procesador de textos); o un fichero por existir una tabla con distintos nombres y direcciones, la agenda de clientes, un conjunto de currículums ordenados o grabaciones de entrevistas de trabajo, registros de imágenes de acceso a locales, una relación de facturas o historiales médicos bajo algún criterio estructural.

Se ha considerado fichero a efectos de protección de datos a toda página web desde la famosa STJUE caso Lindqvist, C-101/01 de 6 de noviembre 2003 (también SAN 17 de marzo de 2006). Sin embargo, la STS de 19 de septiembre de 2008 no consideró ficheros los libros bautismales por la difícil búsqueda que implicaba su conformación al estar sólo ordenados por fechas y dispersos territorialmente.

¿Qué es un tratamiento de datos?

El triángulo que viene a determinar la aplicación de la normativa de datos personales **se cierra con el concepto de "tratamiento".**

Para el RGPD se trata de "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".

La administración local realiza habituales tratamientos como nos recuerda la Guía AEPD para el ámbito local:

- *Padrón municipal de habitantes*
- *Subvenciones y ayudas*
- *Sanciones*
- *Obras y licencias*
- *Policía local*
- *Gestión de tributos*
- *Bolsas de trabajo*
- *Recaudación ejecutiva*
- *Registro de documentos*
- *Cementerio municipal*
- *Recursos humanos*
- *Biblioteca municipal*
- *Servicios sociales*
- *Educación infantil*
- *Gestión económica*

2. ¿Cuándo se aplica el régimen de protección de datos? El triángulo conformado por los vértices de "datos personales", "fichero" y "tratamiento" queda sometido a la normativa de protección de datos

En buena medida, **todo lo que quede dentro del triángulo conformado por los vértices de "datos personales", "fichero" y "tratamiento" queda sometido a la normativa de protección de datos**

. Así, el Reglamento Europeo de protección de datos (RGPD) en razón de su artículo 2 "se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero."

3. ¿Cuándo no se aplica la normativa de protección de datos?

Hay diferentes supuestos en los que no se aplica la normativa de protección de datos. SI los datos están completamente anonimizados, no son datos personales y, en consecuencia, no se aplica la normativa de protección de datos. Baste adelantar que es muy difícil la completa anonimización y el mero hecho de anonimizar datos personales es un tratamiento de datos sujeto a la normativa de modo particular.

Además, la normativa se aplica a los datos relativos a **personas físicas**. Ello lleva, en primer término, a recordar el RGPD "**no regula el tratamiento de datos personales relativos a personas jurídicas** y en particular a empresas constituidas como personas jurídicas (Cons. 14). Así pues, la información sobre empresas, asociaciones, Administraciones, etc. por ejemplo, respecto de su solvencia, localización, información corporativa, económica, etc. no queda afectada por la normativa de protección de datos. Esta exclusión se da, claro está, siempre que dicha información no incluya datos de personas físicas.[6]

En cierto modo **no** se aplican las exigencias de protección de datos respecto del "tratamiento de los datos relativos a los **empresarios individuales y a los profesionales liberales**, cuando se refieran a ellos únicamente en dicha condición y no se traten para entablar una relación con los mismos como personas físicas." (LO 3/2018 en su artículo 19. 2º).

En segundo término, el derecho a la protección de datos lo es respecto de las personas físicas que estén vivas. Así, el RGPD afirma que "**no se aplica a la protección de datos personales de personas fallecidas**" (Cons. 27)[7]. Ello sin perjuicio de la regulación sobre fallecidos en la LO 3/2018[8].

El RGPD **no** es aplicable si un tratamiento es "efectuado por una persona física en el ejercicio de actividades **exclusivamente personales o domésticas**" (art. 2.2.c) RGPD).[9]

---

[6] Debe llamarse la atención de la exclusión del régimen de protección de datos a la información relativa a las personas jurídicas no implica que no haya un régimen jurídico que proteja, por ejemplo, el derecho al honor de las personas jurídico privadas, o el prestigio de las públicas, así como la importante protección normativa conferida al secreto vinculado a empresas o instituciones, e incluso garantías como la inviolabilidad del domicilio o secreto de comunicaciones.

[7] En todo caso, la LO 3/2018 aunque excluye del ámbito de aplicación de la ley el tratamiento de datos de fallecidos (art. 2.3º d), su art. 3 permite que los herederos puedan solicitar el acceso, rectificación o supresión de los datos, en su caso sujetándose a las instrucciones del fallecido al respecto. Asimismo, la LO 3/2018 incluye como derecho digital un "derecho al testamento digital".

[8] Tras excluir del ámbito de aplicación de la ley el tratamiento de datos de fallecidos (art. 2.3º d) art. 3 permite que los herederos puedan solicitar el acceso, rectificación o supresión de los datos, en su caso sujetándose a las instrucciones del fallecido al respecto. Asimismo, la LO 3/2018 incluye como derecho digital un "derecho al testamento digital".

[9] Es especialmente importante tener en cuenta que el RGPD no es aplicable si un tratamiento es "efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas" (art. 2.2.c) RGPD). Se considera en la exclusión los repertorios de direcciones o actividad en redes sociales en estas actividades, eso sí, "sin conexión alguna con una actividad profesional o comercial" (Cons. 18). La previa legislación española (art. 4 a) Reglamento antigua LOPD) concretaba que "solo se considerarán relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares". La sentencia de la Audiencia Nacional de 15 de junio de 2016 señala que "Será personal cuando los datos tratados afecten a la esfera más íntima de la persona, a sus relaciones familiares y de amistad y que la finalidad del tratamiento no sea otra que surtir efectos en esos ámbitos". Baste adelantar que el tratamiento en el ámbito laboral o empresarial, aún realizado en el hogar, no gozaría de esta exclusión. Obviamente hay zonas grises respecto de actividades en internet o redes sociales. Así, el G29 al respecto considera ejemplos que estarían excluidos de la protección de datos, como vender

Aunque pueda resultar algo confuso, hay que advertir que **el hecho de que no se aplique la normativa de protección de datos** y en particular el RGPD y la LO 3/2018, **no quiere decir que no se aplique otras normativas de ámbitos afines**, como pueda ser el derecho al honor, intimidad, propia imagen, la protección de secretos, etc. ya se trate en el ámbito civil, penal, laboral. (por ejemplo: cometer un delito o intromisión por difundir "domésticamente" fotos íntimas de un amigo). En el caso de los datos no personales, sin perjuicio de otras normas, existe incluso el reciente Reglamento (UE) 2018/1807.

4. ¿Dónde se aplica la normativa general de protección de datos?

Por cuanto al importante ámbito de aplicación territorial, el artículo 3. 1º RGPD fija el criterio principal básico de aplicación: que sea un tratamiento de datos "en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no."

> *Explicado de una manera más simple, se aplica la normativa europea cuando la decisión efectiva de tratar datos personales, o si el tratamiento efectivo de los datos para otro se hace en territorio europeo.*

Resulta especialmente innovador el **RGPD cuando extiende el ámbito territorial de aplicación en razón de que el interesado esté en la UE**. Así sucede en primer lugar, respecto de: **"a) la oferta de bienes o servicios** […] independientemente de si a éstos se les requiere su pago" vayan **dirigidos a la UE.**

> Para "determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros de la Unión […] la mera accesibilidad del sitio web del responsable o encargado o de un intermediario en la Unión, de una dirección de correo electrónico u otros datos de contacto, o el uso de una lengua generalmente utilizada en el tercer país donde resida el responsable del tratamiento, no basta para determinar dicha intención, hay factores, como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa otra lengua, o la mención de clientes o usuarios que residen en la Unión, que pueden revelar que el responsable del tratamiento proyecta ofrecer bienes o servicios a interesados en la Unión." (Cons. 23).

En segundo lugar, también **se aplica el RGPD fuera de la UE cuando la actividad de tratamiento sean dirigidas al "control de su comportamiento"** (letra b). Y "Para determinar si se puede considerar que una actividad de tratamiento controla el comportamiento de los interesados, debe evaluarse si las personas físicas son objeto de un seguimiento en internet, inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes." (Cons. 24). Sin duda, este criterio tiene un enorme potencial ante el imparable crecimiento de los tratamientos masivos y las decisiones automatizadas.

---

regalos de cumpleaños en una plataforma de e-comercio, tener un blog sobre arreglos florales comentando la propia experiencia laboral, participar en una campaña civil vinculada al ámbito de las flores, compartir datos de interesados en estas aficiones o, incluso, usar sistemas de e-comercio y e-pago para comprar suministros de una afición. Ahora bien, sí quedarían sujetos al RGPD quienes "proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas." (Cons. 18).

Pues bien, en estos casos de aplicación extraterritorial, se da un deber de designar expresamente y por escrito un representante en la UE que actúe en nombre del responsable o encargado respecto a las obligaciones que les incumben En cualquier caso, esta designación no afecta a la responsabilidad del responsable o del encargado, si bien, el representante designado debe estar sujeto a medidas coercitivas en caso de incumplimiento por parte del responsable o del encargado». (Cons. 80).

III. ¿Qué tipos de datos personales hay que distinguir?

En el apartado anterior se vio ¿qué son "datos personales"? Interesa ahora distinguir dentro de los distintos tipos de datos personales por cuanto ello puede conllevar diversas obligaciones y régimen jurídico.

1. Datos personales ordinarios, de carácter identificativo y de características personales.

Dentro de los datos que no implican una especial protección, que podemos denominar ordinarios, puede ser de interés los de carácter identificativo. Respecto de los mismos, en principio, el régimen jurídico es el ordinario y general.

2. Datos del ámbito penal y del ámbito sancionador

Los datos relativos a condenas e infracciones penales están regulados en el artículo 12 RGPD, ya no son especialmente protegidos. No obstante, se impone a una especial supervisión por las autoridades que han de regular las garantías y registro completo de condenas penales es un tratamiento reservado a autoridades públicas.

Los datos relativos a infracciones y sanciones administrativas no tienen un especial régimen en el reglamento europeo, más allá de la referencia genérica del artículo 86 RGPD respecto de su transparencia con remisión a la legislación interna. La LOPD 3/2018 en su artículo 27 impone que los responsables son los órganos competentes para la instrucción del procedimiento sancionador, para la declaración de las infracciones o la imposición de las sanciones y que el tratamiento se limite a los datos estrictamente necesarios. En principio estos datos sólo han de ser tratados por abogados y procuradores o en razón del consentimiento o previsión legal específica.

Desde el punto de vista de la transparencia y derecho de acceso a la información pública hay que tener en cuenta lo dispuesto en el artículo 15 Ley 19/2013, por lo que en principio estos datos quedarían al margen de la transparencia y acceso. No obstante, hay que tener en cuenta la doctrina específica de las autoridades independientes.

Dada la inercia de muchos años de estos datos como datos especialmente protegidos, igual que los datos penales, sin duda las garantías y requisitos "ordinarios" hay que aplicarlos con especial cautela. Com luego se indica el tratamiento de estos datos queda en el ámbito habitual de la exigencia del estudio de impacto.

Datos especialmente sensibles

La normativa establece un régimen de particular protección respecto de unos datos, por lo que hay que estar especialmente alerta respecto del tratamiento de los mismos.

Así, según el artículo 9 RGPD cabe tener en cuenta datos:

- Afiliación sindical
- Datos biométricos
- Datos relativos a la vida sexual
- Convicciones religiosas o filosóficas
- Datos genéticos
- Datos sobre orientación sexual
- Ideología u opiniones políticas
- Datos relativos a la salud
- Origen Racial o étnico

El artículo 4 RGPD define algunos de estos datos especialmente protegidos.

13) «datos genéticos»: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;

14) «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

15) «datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;

3. Otros tipos de datos –o tratamientos- con un régimen o garantías especiales, como el necesario estudio de impacto

Aunque no están bajo el régimen particular del artículo 9 RGPD de datos especialmente protegidos, también hay que tener especiales cautelas respecto de:

- datos de menores, especialmente de 14 años
- datos de sujetos vulnerables o en riesgo de exclusión social, incluyendo
- datos de mayores con algún grado de discapacidad, discapacitados,
- personas que acceden a servicios sociales y víctimas de violencia de género, así como sus
- descendientes y personas que estén bajo su guardia y custodia
- los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10 RGPD. Asimismo y por tradición normativa, los relativos a sanciones de infracciones administrativas.
- Video vigilancia de espacios públicos.

Como se señalará[10], bajo el principio de responsabilidad proactiva se incluye también la obligación de realizar un estudio de impacto de protección de datos en algunos supuestos (art. 35 RGPD).[11] Sobre esta base y para España, la AEPD en 2019 ha concretado las Listas de tipos de tratamientos de datos que requieren EIPD (art 35.4) [12]. Señala que será **necesario** realizar un estudio de impacto en la mayoría de los casos en los que dicho **tratamiento cumpla con dos o más criterios de la lista** expuesta a continuación. Añade que cuantos más criterios reúna el tratamiento en cuestión, mayor será el riesgo que entrañe dicho tratamiento y mayor será la certeza de la necesidad de realizar una EIPD. Del listado no exhaustivo de once tratamientos de mayor riesgo que se recogen en el documento, en el ámbito que aquí interesa, debe haber especial sensibilidad y alerta cuando se traten datos:

- que impliquen perfilado o valoración de trabajo, personalidad y comportamiento
- datos y metadatos a través de redes, aplicaciones o en zonas de acceso público
- procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, TV interactiva, aplicaciones móviles, etc.
- datos especialmente protegidos artículo 9.1 del RGPD y datos relativos a condenas o infracciones penales, 10 del RGPD. Datos biométricos, datos genéticos.
- datos de situación financiera o de solvencia patrimonial
- sujetos vulnerables o en riesgo de exclusión social, incluyendo datos de menores de 14 años, mayores con algún grado de discapacidad, discapacitados, personas que acceden a servicios sociales y víctimas de violencia de género.

Por cuanto a los tipos de tratamientos, propios e incluso **naturales del ecosistema del big data y la inteligencia artificial**, se incluye la garantía del estudio de impacto respecto de:

- toma de decisiones automatizadas
- perfilados de comportamiento.
- uso de datos a gran escala
- asociación, combinación o enlace de registros de bases de datos para varias finalidades.
- utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras

[10] Apartado "¿Qué obligaciones hay que cumplir si se tratan datos y qué medidas hay que adoptar?".

[11] La norma europea impone esta especial garantía respecto de ámbitos que son bien afines al ecosistema inteligencia artificial-big data. Así:

-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 (datos especialmente protegidos), o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10,

-la observación sistemática a gran escala de una zona de acceso público.

[12] Pág. 3.

Sobre la base de lo anterior, en el marco de una gobernanza de datos dentro de la organización al proponer un tratamiento o fichero de datos habrá que tener clara la tipología de los datos, así como los posibles afectados o interesados (personas físicas de quienes se tratan datos).

IV. ¿Quién es quién? Responsables, encargados y contratación. El DPO y la gobernanza de los datos en las organizaciones

1. Gobernanza y procesos internos en las organizaciones

Se habla de **«Data Governance" o la "gobernanza de los datos"** al conjunto de acciones, gestión, procesos, funciones, políticas, normas y mediciones que ha de haber en una organización que trata datos. Implica una estrategia integral con una orgánica y responsabilidad, procedimientos y plan de gestión global todos los datos de la organización. Se busca así que sea eficiente, eficaz y garantice el cumplimiento normativo.

Cada organización tiene y determina su organización y procesos y, obviamente, adopta su gobernanza de datos. El esquema habitual de gobernanza de datos dentro de la organización pasa por procedimientos internos, normas y protocolos que se establezcan en materia de protección de datos[13]. Y hay que estar por lo que ahí se establezca.

No obstante, **la normativa de protección de datos fija unos sujetos con deberes y responsabilidades específicos** para el cumplimiento de las obligaciones por tratar datos y qué medidas hay que adoptar.

Así, suelen formalizarse procedimientos para comunicar quién será la unidad que quiere tratar datos, si va a haber varios responsables que de datos dentro y fuera de la organización, la finalidad o finalidades que se persiguen, el tipo de datos, las estructura del conjunto de datos, tipología de los interesados o afectados, el origen de los datos, si está previsto que haya encargados que vayan a manejar datos en razón de contrato o instrumento jurídico, si está previsto comunicar los datos a otros (terceros). Cada organización establece los procedimientos internos como si se requieren informes técnicos o jurídicos cuando se da la comunicación de los elementos anteriores.

También es habitual que se aplique este esquema o haya un procedimiento por **cuanto lo que vaya a realizarse es un diseño de sistemas, software, aplicaciones dirigido al tratamiento de datos personales**.

Sobre esta información el DPD –si lo hay- en la organización o persona similar debe **evaluar riesgos y planificar la mitigación de impactos**, sobre esta base se proponen las **medidas de seguridad** aplicables, cómo garantizar el principio de **transparencia e información o cómo satisfacer los derechos** de los interesados y las relaciones con terceros.

[13] Ver al apartado anterior "Normativas y protocolos internos".

Es habitual que una unidad en la organización –bajo la autoridad y asesoría del DPD- asuma la atribución de autorizar los tratamientos de datos. Cada orgánica determina figuras responsable interno del tratamiento.

La **orgánica interna debe conectarse con el organigrama de la organización**. Además de un **esquema de autorización interna de tratamientos**, el reparto de papeles lleva a **distribuir funciones** concretas relativas al cumplimiento de medidas de seguridad, responsabilidad ante ejercicio de derecho de acceso, comunicación con autoridades, supervisión de contratos y documentos de encargados de tratamiento, etc.

Un modelo de gobernanza de datos obliga a tener una estrategia y visión de quién es quién en cada tratamiento de datos. Es muy importante desde el inicio diseñar las estrategias en la captación o fuentes de datos, así como el flujo de datos entre responsables, encargados o cesiones de datos a terceros.

Para el ámbito local, según el tipo de entidad puede ser muy adecuado normativizar o institucionalizar esta gobernanza (a través de un reglamento u otro instumento organizativo para determinar esta gobernanza, el responsable interno, relaciones con encargado-s, con el DPO. Organizar el cumplimiento de obligaciones como el registro de tratamientos, en su caso documento de seguridad.

Esta organización ha de ir ligada a las políticas de datos más amplias, como la apertura de datos. Grandes organizaciones han creado su oficina del dato. El Decreto 76/2020, de 4 de agosto, de Administración digital de Cataluña es el mayor exponente sobre la regulación de la gobernanza de datos a la que dedica buena parte de su contenido (en especial, arts. 10 y ss.).

2. ¿Quién o quiénes son los “responsables” de un tratamiento de datos?

El “**responsable**” es “la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento”. Una persona jurídica muy habitualmente será un responsable, por ejemplo una Administración, el ayuntamiento, la diputación, la entidad pública municipal, una empresa o una asociación. El elemento básico es la toma de decisiones sobre la creación y finalidades del tratamiento de datos. Quién materialmente adopta estas decisiones es el responsable del tratamiento.

La nueva LOPD (artículo 29), concreta que para determinar las responsabilidades debe atenderse a las actividades que efectivamente desarrolla cada uno de los responsables del tratamiento. L**a determinación de quién o quiénes son los responsables depende de la realidad material de la decisión de hacer el tratamiento, y la puesta de medios.**

***No confundir**: Cabe recordar que **quienes actúen bajo autoridad directa del responsable o del encargado**, por ejemplo los trabajadores del instituto, empresa, Administración o asociación, se consideran en el ámbito de tal sujeto obligado y no hay que confundirlos con el “encargado” del tratamiento y, obviamente, tampoco son terceros.*

3. ¿Quién es el "encargado" y cuáles son las obligaciones y requisitos en la contratación?

Por su parte, el **"encargado del tratamiento o encargado"** es "la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento", si bien, no están bajo la autoridad directa de éste, sino que están **unidos a través de un marco contractual u otra fórmula jurídica**.

*Ejemplos de encargados: La **contratación de servicios** –por ejemplo de mantenimiento informático- es un claro ejemplo de encargado que trata datos por cuenta del responsable, o las empresas marketing, de consultoría de protección de datos, de instalaciones de cámaras de videovigilancia, seguridad privada, administradores de fincas, agentes de seguros, procuradores, abogados, etc. Cabe tener en cuenta que una empresa de un grupo de empresas puede en su caso actuar como encargado. En ocasiones puede llamar la atención que un responsable de tratamiento sea un mero usuario de servicios de la nube y el encargado del tratamiento sería en principio el prestador de servicios de la nube por cuenta del cliente.*

En cualquier caso, cualquier prestador de servicios a la entidad local que para ello trate datos, es un encargado. Por ejemplo, cuando el Ayuntamiento encarga a un tercero (una empresa): La elaboración de las nóminas de su personal, la destrucción de documentación, videovigilancia, cobro de impuestos, etc.

El marco jurídico será muy importante para determinar los papeles que se ocupan y, sobre todo, **la normativa obliga a fijar en el marco contractual o jurídico el régimen de deberes y responsabilidades en el marco de la protección de datos entre el responsable y el encargado.**

En particular, ha de incluir las instrucciones del responsable, el deber de confidencialidad, las medidas de seguridad, régimen de la subcontratación, colaboración del encargado para el ejercicio de los derechos de los afectados y otras obligaciones del responsable. Asimismo, el destino de los datos al finalizar la prestación

El artículo 28 del RGPD señala las condiciones en aquellos supuestos en los que un tercero (Encargado de Tratamiento) preste un servicio a miembros de la entidad (local, por ejemplo)

-elegirá únicamente un encargado que ofrezca garantías . Hay responsabilidad por una mala elección. Debe demostrarse que se ha analizado los riesgos de la elección.

-se regirá por un contrato u otro acto jurídico que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. La AEPD ha establecido un contrato modelo para el encargado que hay que seguir, con las adecuaciones que incluya la propia organización. Directrices para la elaboración de contratos entre responsables y encargados del tratamiento

-Se trata de garantizar que el encargado tratará los datos personales únicamente siguiendo instrucciones del responsable.

-Límites a la subcontratación a un tercero por el encargado: el encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. Si existe, el encargado informará al responsable de cualquier

cambio previsto en la incorporación o sustitución de otros encargados. Cuando un encargado del tratamiento recurra a otro encargado se ha de garantizar en todo caso el cumplimiento de las mismas obligaciones de protección de datos. Asimismo, existe el deber de guardar secreto profesional. La fijación y expresión concreta de estos compromisos es especialmente útil.

La **nueva LOPD** incluye algunas novedades o particularidades respecto de los encargados (artículos 28 y 33)[14].

Resulta de especial utilidad seguir las Directrices para la elaboración de contratos entre responsables y encargados del tratamiento de la AEPD y otras autoridades de protección de datos así como su **anexo con modelo de Ejemplo de cláusulas contractuales** para supuestos en que el encargado del tratamiento trate los datos en sus locales y exclusivamente con sus sistemas.

La Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público recuerda la figura del contratista como ncargado y con ella. Recuerd que no es una comunicación de datos así como obligaciones como la destrucción o devoluvión de datos, el bloqueo de los datos por el contratista mientras persistan responsabilidades,

> **Disposición adicional vigésima quinta. Protección de datos de carácter personal**.
>
> 1. Los contratos regulados en la presente Ley que impliquen el tratamiento de datos de carácter personal deberán respetar en su integridad la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarrollo.
>
> 2. Para el caso de que la contratación implique el acceso del contratista a datos de carácter personal de cuyo tratamiento sea responsable la entidad contratante, aquel tendrá la consideración de encargado del tratamiento.
>
> En este supuesto, el acceso a esos datos no se considerará comunicación de datos, cuando se cumpla lo previsto en el artículo 12.2 y 3 de la Ley Orgánica 15/1999, de 13 de diciembre. En todo caso, las previsiones del artículo 12.2 de dicha Ley deberán de constar por escrito.

[14] En relación con los encargados de las Administraciones Públicas (como pueda ser una Universidad) artículo 33. 2 dispone si el encargado actúa en su propio nombre y sin que conste que actúa por cuenta de otro, estableciendo relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 del RGPD, será considerado responsable

Tendrá asimismo la consideración de responsable del tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades.

Cuando se produce un cambio de encargado el responsable del tratamiento determinará si, cuando finalice la prestación de los servicios del encargado, los datos personales deben ser destruidos, devueltos al responsable o entregados, en su caso, a un nuevo encargado. No obstante, no procederá la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deberán ser devueltos al responsable, que garantizará su conservación mientras tal obligación persista.

En el ámbito del sector público podrán atribuirse las competencias propias de un encargado del tratamiento a un determinado órgano de la Administración General del Estado, la Administración de las comunidades autónomas, las Entidades que integran la Administración Local o a los Organismos vinculados o dependientes de las mismas mediante la adopción de una norma reguladora de dichas competencias, que deberá incorporar el contenido exigido por el artículo 28.3 del RGPD.

Según la Disposición transitoria quinta: *Los contratos de encargado del tratamiento suscritos con anterioridad al 25 de mayo de 2018 al amparo de lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal mantendrán su vigencia hasta la fecha de vencimiento señalada en los mismos y en caso de haberse pactado de forma indefinida, hasta el 25 de mayo de 2022.*

Durante dichos plazos cualquiera de las partes podrá exigir a la otra la modificación del contrato a fin de que el mismo resulte conforme a lo dispuesto en el artículo 28 del Reglamento (UE) 2016/679 y en el Capítulo II del Título V de esta ley orgánica.

Cuando finalice la prestación contractual los datos de carácter personal deberán ser destruidos o devueltos a la entidad contratante responsable, o al encargado de tratamiento que esta hubiese designado.

El tercero encargado del tratamiento conservará debidamente bloqueados los datos en tanto pudieran derivarse responsabilidades de su relación con la entidad responsable del tratamiento.

3. En el caso de que un tercero trate datos personales por cuenta del contratista, encargado del tratamiento, deberán de cumplirse los siguientes requisitos:

a) Que dicho tratamiento se haya especificado en el contrato firmado por la entidad contratante y el contratista.

b) Que el tratamiento de datos de carácter personal se ajuste a las instrucciones del responsable del tratamiento.

c) Que el contratista encargado del tratamiento y el tercero formalicen el contrato en los términos previstos en el artículo 12.2 de la Ley Orgánica 15/1999, de 13 de diciembre.

En estos casos, el tercero tendrá también la consideración de encargado del tratamiento.

4. ¿Qué es el delegado de protección de datos (DPD)?

Bajo el nuevo modelo de responsabilidad proactiva, se incluye una garantía material del cumplimiento normativo. Así, el artículo 38 RGPD regula al delegado de protección de datos (DPD). El mismo puede ser obligatorio (art. 37) o voluntario en las organizaciones que tratan datos personales. El DPD pasa a ser una figura clave para el cumplimiento normativo y es obligatorio en todas las Administraciones públicas.

¿Qué hace el DPD? Esencialmente (art. 39) el DPD informa y asesora al responsable o al encargado del tratamiento y a los empleados en materia de protección de datos; supervisa el cumplimiento de la normativa, realiza consultas, coopera y es punto de contacto con las autoridades de protección de datos, notifica las violaciones de seguridad, ha realizar evaluaciones de impacto y analiza la protección de los datos desde el diseño y por defecto. Asimismo, se encarga de la planificación, y la gestión y la supervisión de las medidas de seguridad aplicable a tratamiento de datos en el organización, supervisa las auditorías correspondientes y la asignación de responsabilidades sobre protección de datos. La nueva LOPD incluye su atribución de intervenir en la resolución de reclamaciones, tanto las recibidas directamente de los interesados como de la AEPD.

¿Cuál es su posición? Para todo ello ha de garantizarse que tenga una posición adecuada en la organización y se garantice que no reciba ninguna instrucción, ni pueda ser sancionado o destituido por desempeño de su funciones y sólo responda al nivel jerárquico más alto.

¿Es obligatorio? En el ecosistema de la inteligencia artificial, big data etc. es más que posible que la figura sea obligatoria porque casi de modo seguro se da alguno de las condiciones para que sea obligatorio:

-siempre que se trate de organismos públicos.

-organizaciones que lleven a cabo una observación habitual y sistemática de interesados a gran escala.

-tratamiento a gran escala de categorías especiales de datos personales (artículo 9) o de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

5. El DPO en la Administración local

Se´gun

Es posible para la AEPD,

-un único delegado de protección de datos para varios de estas autoridades u organismos

- un único DPD para, por ejemplo, un ministerio, consejería o ayuntamiento.

-puede ser a tiempo completo o a tiempo parcial

- podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios. Puede ser una empresa privada, pues.

En el ámbito local, si seguimos la Guía de la AEPD (p. 31)

En los Ayuntamientos con población superior a 20.000 habitantes, atendiendo al volumen de datos tratados, el Delegado de Protección de Datos podría contar con un departamento de apoyo.

En los Ayuntamientos con población inferior a 20.000 habitantes, podrían designar su Delegado de Protección de Datos, o articularlo a través de las Diputaciones Provinciales o Comunidad Autónoma respectiva.

Diputaciones provinciales, cabildos y consejos insulares también deberán designar su delegado de protección de datos.

Podría designarse también en las empresas municipales en función de los tratamientos de datos llevados a cabo.

En el caso de que se designe a **secretarios, interventores y tesoreros**, podrían actuar como delegados de protección de datos siempre que no exista conflicto de intereses en relación con el ejercicio de sus respectivas funciones en la gestión ordinaria del ente local en cuestión.

A este respecto, señala la AEPD en su documento sobre el DPD en las AAPP, que el DPD actúa como asesor y supervisor interno, por lo que ese puesto no puede ser ocupado por personas que, a la vez, tengan tareas que impliquen decisiones sobre la existencia de tratamientos de datos o sobre el modo en que van a ser tratados los datos (p.ej.: responsables de ITC, o responsables de seguridad de la información).

También, según se ha dicho cabe la posibilidad de que **se pueda prestar por entidades privadas especializadas.**

Puede consultar el documento elaborado por la AEPD “El Delegado de Protección de Datos en las Administraciones Públicas”.

V. ¿Cómo deben tratarse los datos? los principios del tratamiento de datos

Los pilares estructurales del régimen jurídico de protección de datos han sido y siguen siendo los llamados “principios”. Éstos no sólo constituyen **reglas concretas aplicables a los tratamientos, guías esenciales para responsables** y encargados, sino que son

elementos básicos para la interpretación misma de toda la normativa y pauta de actuación por todos los que traten datos. El artículo 5 RGPD los regula. Así, se afirma que los datos personales serán "a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»)".

Se analizan a continuación los siguientes principios:

1. Licitud del tratamiento

2. Minimización de datos, especialmente en el caso de la investigación. Usar los mínimos datos posibles el menor tiempo

3. Lealtad, información y transparencia

4. Limitación de la finalidad y la posibilidad de usar datos para fines no incompatibles

5. Secreto y confidencialidad

6. Exactitud, corrección y actualización de los datos

1. Licitud del tratamiento

Por cuanto a la licitud del tratamiento, de momento baste señalar que cualquier tratamiento de datos solo es lícito si cuenta con consentimiento, o se da en el marco de la ejecución de un contrato, el cumplimiento de una obligación legal, se hace para proteger intereses vitales o con fines de interés público o en razón del ejercicio de poder público. Asimismo, un tratamiento justificarse por "intereses legítimos".

2. Usar los mínimos datos posibles el menor tiempo

El artículo 5 dispone que los datos han de ser "c) **adecuados, pertinentes y limitados a lo necesario** en relación con los fines para los que son tratados («minimización de datos»)".

> El Considerando 39 afirma que "Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica."

Entre todos los principios, puede decirse que el principio de minimización de los datos adquiere una muy especial relevancia en el RGPD. En buena medida la responsabilidad proactiva y las exigencias para el responsable de la privacidad por defecto y en el diseño vienen a –intentar- garantizar y hacer efectivo el principio de minimización. Baste recordar ahora que el artículo 35.7º sobre Evaluación de impacto relativa a la protección de datos "deberá incluir como mínimo: […] b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad."

3. Lealtad, información y transparencia ¿de qué hay que informar?

El referido artículo 5 RGPD afirma también los principios de lealtad y transparencia, los cuales "exigen que se informe al interesado de la existencia de la operación de tratamiento y sus fines." (Cons. 60).

> "Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados […] en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento. En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida." (Cons. 39). Dicha información puede transmitirse en combinación con unos iconos normalizados que ofrezcan, de forma fácilmente visible, inteligible y claramente legible, una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presentan en formato electrónico deben ser legibles mecánicamente." (Cons. 60).

El RGPD contiene a una muy prolija regulación de los deberes de transparencia que se amplían notablemente respecto de la normativa precedente y se concretan en los extensos artículos 12 a 15 que incluyen el propio derecho de acceso. Se trata de una cuestión abordada en la útil Guía para el cumplimiento del deber de informar de la AEPD y las agencias catalana y vasca de 2017.

Epígrafe	Información básica (1ª capa, resumida)	Información adicional (2ª capa, detallada)
"Responsable" (del tratamiento)	Identidad del Responsable del Tratamiento	Datos de contacto del Responsable
		Identidad y datos de contacto del representante
		Datos de contacto del Delegado de Protección de Datos
"Finalidad" (del tratamiento)	Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles	Descripción ampliada de los fines del tratamiento
		Plazos o criterios de conservación de los datos
		Decisiones automatizadas, perfiles y lógica aplicada
"Legitimación" (del tratamiento)	Base jurídica del tratamiento	Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo.
		Obligación o no de facilitar datos y consecuencias de no hacerlo
"Destinatarios" (de cesiones o transferencias)	Previsión o no de Cesiones	Destinatarios o categorías de destinatarios
	Previsión de Transferencias, o no, a terceros países	Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables
"Derechos" (de las personas interesadas)	Referencia al ejercicio de derechos.	Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento
		Derecho a retirar el consentimiento prestado
		Derecho a reclamar ante la Autoridad de Control
"Procedencia" (de los datos)	Fuente de los datos (cuando no proceden del interesado)	Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público
		Categorías de datos que se traten

4. Limitación de la finalidad y la posibilidad de usar datos para fines no incompatibles

El artículo 5.1º b) RGPD regula que los datos han de ser "recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines […] («limitación de la finalidad»)". **La adecuación a la finalidad es un eje vertebral de todo tratamiento de datos.**

No debe olvidarse que un tratamiento puede ser perfectamente lícito y legítimo para una o varias finalidades, pero decae como castillo de naipes en la ilegalidad en cuanto pasa a darse un uso incompatible con la finalidad.

La **finalidad pasa a ser esencial para la determinación de su período de conservación**.

Y hay que advertir que aunque se cuente con una causa de legitimización de **un tratamiento** (consentimiento, interés público, etc.), éste **puede pasar a ser ilícito por una desproporción o inadecuación con relación a la finalidad**.

Desproporción puede llevar a que incluso sea ilegal un tratamiento con consentimiento o si tenía una base legal pero para una finalidad particular. Incluso el RGPD atisba la posibilidad de que se considere que el consentimiento no ha sido libre y por tanto es nulo si "la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato." (art. 7. 4º). Este precepto podría llevar a considerar que no cuentan con la legitimación del tratamiento de datos aquellos servicios –tan habituales en internet- que captan una ingente cantidad de datos que poco o nada tienen que ver con el servicio que brindan al sujeto a cambio de tales datos.

Ahora bien, como **regla general usar los datos "con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales"** si se cumplen unos requisitos (art. 5 RGPD)[15]. Ello a *cambio* de garantías y "que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales."

El Informe 175/2018 AEPD señala que ha de haber una visión amplia de no incompatibilidad cesión de datos entre Administraciones Públicas, por ejemplo para ceder datos entre administraciones del domicilio del interesado. [16] sin que ello implique la posibilidad de cesiones masivas de datos para el ejercicio de otras competencias.

[15] Así, y como principio, el artículo 5 RGPD precisamente cuando afirma el principio de lealtad y finalidad, prevé expresamente que "de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales."

[16] STC 139/2016, de 21 julio 2016: c)
la comunicación de datos limitada a la mera indicación del tramo de entre los tres previstos en que se halla el usuario, se encuentra amparada por el art. 11.2 a) LOPD, en conexión con el art. 94 ter de la Ley 29/2006 (art. 103 del Real Decreto Legislativo 1/2015).
STC 17/2013, de 31 enero 2013, FJ 7 y 8.

5. Secreto y confidencialidad

Hay que seguir el principio de integridad y confidencialidad establecido en el art. 5.1.f) RGPD y regulado con alguna mayor concreción en el artículo 5 de la nueva LODP 3/2018[17].

Este deber de confidencialidad se da en todos los casos y puede añadirse y superponerse a las reglas y exigencias más concretas del mismo, como las regulaciones del secreto profesional, reglas para servidores públicos, secreto industrial, etc. Estas obligaciones se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

El responsable del tratamiento **no sólo debe preocuparse por respetar su propio deber de secreto, también debe asegurarse de que todo el personal a su servicio mantiene la confidencialidad del tratamiento,** para lo cual se deben adoptar, **al menos, las siguientes medidas**[18]:

- *Informar al personal de su deber de secreto.*
- *Adoptar las medidas necesarias para garantizar la confidencialidad de los datos a los que se ha accedido, implantando las medidas técnicas y de carácter organizativo necesarias para impedir que el personal a su servicio pueda revelar datos de carácter personal a terceras personas.*
- *Firmar compromisos de confidencialidad con todos los usuarios de los sistemas de información con acceso a datos de carácter personal.*

6. Exactitud, corrección y actualización de los datos

El artículo 5 RGPD también dispone que los datos serán "d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines

---

Audiencia Nacional se ha pronunciado igualmente de manera reiterada acerca de esta posibilidad. Véase al respecto la Sentencia de 21 septiembre 2016, (rec. 68/2016) con cita de otras como las sentencias de 13 de abril (recurso de apelación 19/2016), 25 de mayo, (recurso de apelación 41/2016), 1 junio (recurso de apelación 32/2016), 6 junio (recurso de apelación 52/2016) y 15 de junio de 2016 (recurso de apelación 59/2016).
CONCLUSIÓN: No sería por tanto necesario, en el caso planteado, el consentimiento del interesado para que por otra Administración diferente se ceda el dato personal del domicilio del interesado con la finalidad de notificarle algún trámite en un procedimiento administrativo

[17] Artículo 5. Deber de confidencialidad.

1. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.

2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.

3. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

[18] *Código de Conducta UNED*, 2.6.5. . 13.

para los que se tratan («exactitud»)". A nadie puede escapar la gravedad e importancia que tiene esta regla para todo responsable o encargado de datos y la responsabilidad activa que conlleva: **"Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos."** Toda empresa, Administración, etc. debe actualizar sus datos de modo que responsan a la realidad[19].

Cabe recordar que frente a datos inexactos podrá ejercerse el derecho de rectificación o, en su caso, el derecho de supresión u olvido.

VI. ¿Cuándo se pueden tratar –o ceder- datos? La "legitimación" de los tratamientos del sector público

1. La legitimación para tratar datos en la Administración por lo general NO es el consentimiento

El punto de partida es que no pueden tratarse datos personales. Y que **sólo se pueden tratar los datos cuando hay una base de legitimación de datos**. Para entendernos, **como si el tratamiento hubiera de estar *bautizado***, de lo contrario se está en el *pecado* de la ilegalidad.

El artículo 6 RGPD[20] determina cómo bautizar los tratamientos de datos.

a) consentimiento libre, inequívoco, específico, informado, acción positiva, que sea demostrable

b) ejecución de un contrato

c)cumplimiento de una obligación legal;

d) intereses vitales

e) misión realizada en interés público o en el ejercicio de poderes públicos (con ley que lo regule)

f) satisfacción de intereses legítimos (con garantías compensatorias)

[19] En todo caso, la LO 3/2018 en su artículo 4 concreta que no habrá responsabilidad si se adoptan tales medidas razonables para que se supriman o rectifiquen sin dilación cuando los datos inexactos se han obtenido directamente del afectado, cuando se hubiera recibido los datos de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad, cuando el responsable obtuviese del mediador o intermediario cuando las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establezcan la posibilidad de intervención de un intermediario o mediador. Tampoco habrá responsabilidad por la inexactitud de los datos obtenidos de un registro público por el responsable.

[20] El tratamiento solo será lícito si puede enmarcarse dentro de alguna de las siguientes condiciones:

a) El interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos

b) El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales.

c) El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento

d) El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

En esencia, un tratamiento solo es lícito si cuenta con consentimiento, o se da en el marco de la ejecución de un contrato, el cumplimiento de una obligación legal, se hace para proteger intereses vitales o con fines de interés público o en razón del ejercicio de poder público. Asimismo, un tratamiento justificarse por "intereses legítimos". Hay que buscar siempre la base de legitimación y además informar de la misma a los interesados.

Sin embargo, para el ámbito del sector público, el punto de partida es otro. **Es la ley la que legitima con carácter general los tratamientos de datos en la Administración y NO el consentimiento**.

La AEPD pone como ejemplo de consentimiento:

- *La suscripción a través de un servicio ofrecido por un Ayuntamiento en su página web para recibir comunicaciones referidas a las actividades culturales.*
- *La inscripción en una bolsa de trabajo. (quien suscribe cuestiona la afirmación)*

Asimismo en España NO es posible la legitimación del tratamiento de datos basada en el interés legítimo.

Como recuerda el Informe 175/2018 AEPD:

"Como CONCLUSIÓN en este punto, cabe decir que, con carácter general, la base jurídica del tratamiento en las relaciones con la Administración, en aquellos supuestos en que existe una relación en la que no puede razonablemente predicarse que exista una situación de equilibrio entre el responsable del tratamiento (la Administración), y el interesado (el administrado) no sería el consentimiento (art. 6.1.a) RGPD), sino, según os casos, el cumplimiento de una obligación legal (art. 6.1.c) RGPD) o el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos (art. 6.1.e) RGPD)."

2. La cobertura legal de los tratamientos y de las competencias o atribuciones

Así pues y como regla general hay que buscar la cobertura legal para el tratamiento de datos sin consentimiento en las Administraciones Públicas. No se trata sólo del general principio de legalidad de la administración, sino de una restricción general al derecho fundamental de protección de datos .

EJEMPLOS de legitimación (AEPD):

- *Tratamiento de datos del Padrón Municipal: Ley de Bases de Régimen Local.*
- *Tratamiento de datos de los impuestos municipales: Texto Refundido de la Ley reguladora de las Haciendas Locales.*
- *Tratamiento de datos de recursos humanos: normativa de función pública aplicable.*

Ello es igualmente predicable para las comunicaciones de datos entre administraciones. El punto de partida (STC 17/2013, de 31 de enero, FJ 4º) es que la Ley Orgánica de protección de datos no permite la comunicación indiscriminada de datos personales entre Administraciones Pública. Se requiere una previsión legal expresa bien

una norma de Derecho de la Unión, o del Derecho del Estado miembro aplicable al responsable del del tratamiento.

También con carácter general el sector público tratará datos en razón del "cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos" y ello siempre que derive de "derive de una competencia atribuida por la ley." (ART. 8. 2 º LOPD)

Como afirma la AEPD (175/2018) ello "equivale, en la regulación española de protección de datos, a "obligación establecida en una norma con rango de ley" del art. 6 RGPD.

Lo cierto es que es ciertamente complejo determinar el alcance e intensidad de la reserva d e ley que legitime el tratamiento de datos en el sector público. Y no está tampoco nada claro que si una ley determina una competencia ello implica la legitimación para el concreto tratamiento de datos. Los tribunales. En ocasiones han sido muy exigentes (como en la misma STC 17/2013, de 31 de enero sobre el padrón) con mención del principio de calidad de la ley, que ha sido muy subrayado por el TC en 2019. Sin embargo, en ocasiones, la mera mención de una competencia de la Administración parece considerarse más que suficiente y, si acaso, complementada con normativa reglamentaria, como puede ser la municipal.

El RGPD por su parte recuerda -y la AEPD-:

> El RGPD regula la posibilidad no sólo de que una misma norma pueda prever varios posibles tratamientos o finalidades (véase Considerando 45 RGPD: El presente **Reglamento no requiere que cada tratamiento individual se rija por una norma específica. Una norma puede ser suficiente como base para varias operaciones de tratamiento** de datos basadas en una obligación legal aplicable al responsable del tratamiento, o si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos. **La finalidad del tratamiento** también debe determinase en virtud del Derecho de la Unión o de los Estados miembros.), sino que **permite que los datos personales puedan ser utilizados para finalidades diferentes ("distintas")** en el art. 6.4 RGPD.

Es importante subrayar con la AEPD que también **la actuación del sector público bajo forma privada requiere de la cobertura legal y no es posible acudir al interés legítimo.**

> "que la interpretación ha de ser la de sostener que la Administración no puede utilizar como base jurídica del tratamiento el interés legítimo del apartado f) del párrafo 1 del artículo 6, siempre que se entienda que el apartado e) "misión de interés público" habrá de interpretarse en un sentido amplio de forma que permita a las Administraciones, incluso en el ámbito del Derecho Privado, los tratamientos de datos personales necesarios para las finalidades legítimas que el ordenamiento les concede o permite." (AEPD 175/2018)

2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley.

Cuando se tratan **datos especialmente protegidos** (ej; salud, genéticos, biométricos, etc.) aún resulta **más difícil *bautizar*** el tratamiento y son mayores los requisitos. Así, la forma de tratarlos legalmente es porque una ley específica así lo permita por causa de "intereses públicos esenciales" o que haya un consentimiento explícito. En el

caso del sector público, más allá de ámbitos afines a la salud o investigación, ha de prevalecer una visión restrictiva que exige una fuerte regulación legal de la posibilidad de uso de datos especialmente protegidos que incluya además las garantías compensatorias.

3. Las cesiones o comunicaciones de datos a terceros o a otras Administraciones Públicas

La comunicación de datos a terceros es un tratamiento de datos que en principio está prohibido y requiere también una base de legitimación, estar *bautizada*. En general, se podrá comunicar datos cuando una Ley obliga -o más bien lo permita o habilite- o el interesado consienta. No obstante, como se ha insistido, el consentimiento sólo excepcionalmente es la fuente de legitimiación en el sector público, por lo que se requiere de la cobertura legal para las comunicaciones.

Como se ha insistido, en el sector público se requiere una ley o norma de la UE que dé cobertura al tratamiento, en este caso, a la comunicación de datos. Y como regla general, **no es posible acudir al deber general de colaboración entre Administraciones Públicas para permitir las cesiones de datos masivas entre las mismas.**[21]

AEPD 175/2018: cabrán cesiones de datos entre las Administración Públicas (entre otros supuestos a que se hace referencia más adelante) cuando sus competencias no sean diferentes o no versen sobre materias distintas.

Cuestión diferente es que las distintas Administraciones Públicas estén ejerciendo la misma competencia, supuesto en el que sí que es posible la cesión de datos. Pero **no si son competencia claramente diferentes (por ej., ejercicio de competencia sancionadora y de disciplina en materia de planeamiento urbanístico).**

La comunicación de datos entre administraciones como señala el TC, se ha de dar siempre de modo **"específico en cada caso ajustado a los datos que resulten precisos para la tramitación de un expediente determinado y no de un acceso masivo e indiscriminado";** "tal acceso sólo podría producirse cuando ese dato resulte necesario o pertinente **en relación con la tramitación de un concreto expediente**, lo que permite analizar o determinar en cada caso la conformidad del acceso con lo establecido en el régimen General que le resulte de aplicación." (**STC 19/2013, FJ 7º).**

Error habitual: El acceso a datos por corresponsables de datos o por encargados, no son comunicaciones de datos,

Como se ha subrayado en el apartado relativo a la gobernanza y las figuras de responsable y encargado, en los procedimientos internos en las organizaciones y desde el inicio hay que tener clara una estrategia que incluya la previsión de la comunicación de datos. Así, por ejemplo, cabe tener en cuenta supuestos de diversos responsables de conjuntos estructurados datos. Cabe

[21] El art. 13 h) de la ley 39/2015 así lo establece expresamente, por lo que el deber de colaboración interadministrativa previsto en el art. 3 k) de la ley 40/2015 ha de entenderse modulado por dicho precepto
artículo 155 de la propia ley 40/2015, en cuanto que sujeta el acceso de los datos
deber de colaboración entre las distintas Administraciones Públicas, y sobre la base del respeto que dicha colaboración ha de tener por la normativa de protección de datos de carácter personal.

también recordar que tratar datos en nombre de otro para prestar servicios en el marco de un contrato, subvención, etc. no es una comunicación de datos, sino que sigue el régimen y responsabilidades de responsable y encargado de datos personales.

- En cualquier caso, desde el inicio cabe intentar prever las cesiones o comunicaciones de datos.

4. El artículo 28.2. de la Ley 39/2015 y que el interesado no se oponga a que las administraciones se comuniquen datos

> "2. Los interesados tienen derecho a no aportar documentos que ya se encuentren en poder de la Administración actuante o hayan sido elaborados por cualquier otra Administración. La administración actuante podrá consultar o recabar dichos documentos salvo que el interesado se opusiera a ello. No cabrá la oposición cuando la aportación del documento se exigiera en el marco del ejercicio de potestades sancionadoras o de inspección."

La ley fue actualizada para evitar un posible consentimiento implícito contrario al RGPD. Así, ahora se trata de un supuesto de tratamiento de datos legitimado por la ley respecto del cual el interesado lo que puede hacer es oponerse. Afirma la AEPD (Guía Administraciones Públicas, p. 13) que "será suficiente con que la Ley hubiese determinado quién es la Administración competente."

-

VII. ¿Para qué finalidades se pueden manejar o tratar datos?

1. ¿Se pueden usar datos para otras finalidades que las inicialmente previstas?

Según se ha adelantado (artículo 5.1º b) RGPD) regula que los datos han de ser "recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines […] («limitación de la finalidad»)". Y hay que advertir que **lo prohibido son los usos "incompatibles",** no las finalidades distintas: "El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial." (Cons. 50) Recuerda el RGPD que para admitir nuevos fines, "no se requiere una base jurídica aparte, distinta de la que permitió la obtención de los datos personales" (Cons. 50). Y es que si hay un cambio de finalidades pero las mismas cuentan con una base de legitimación (consentimiento, ley, etc.) no habría problema.

2. ¿Cuándo un uso de datos es incompatible con la finalidad inicial?

Es posible que los datos que se tienen inicialmente recogidos para una finalidad quieran utilizarse para otras finalidades. En estos casos**, la clave es determinar si el desvío de finalidad en el tratamiento de datos es aceptable o se trata de un prohibido uso incompatible.**

La posibilidad de usar datos para fines no incompatibles es una cuestión jurídica y técnica que debe ser puesta en conocimiento de la organización para efectuar una evaluación de incompatibilidad.[22] Como punto de partida, el G29 señala que en los supuestos en los que la compatibilidad resulta obvia, no habrá que hacer mayor esfuerzo y análisis. Sin embargo, en otros casos no será obvia la compatibilidad entre la finalidad para la que se recogieron los datos y a lo que se destina. Así ha de analizarse con intensidad y profundidad el supuesto[23].

En este análisis son muchos los factores a tener en cuenta. Este juicio de incompatibilidad consiste en definir la finalidad o finalidades iniciales y determinar la adicional o nueva finalidad. Obviamente, a mayor distancia entre la finalidad original y la adicional, más difícil será sostener la relación de compatibilidad. Hay que atender a la realidad y contexto del caso concreto, analizar si había expectativas razonables desde el inicio de que los datos serían usados para fines adicionales; hay que tener en cuenta la legitimidad de base (consentimiento, contrato, interés legítimo, etc.). Se ha de apreciar qué garantías se dieron en aquel momento inicial. No hay que obviar la real capacidad de elección o consentimiento del interesado, la relación que se da entre responsable e interesado, la asimetría que puede darse entre ambos, la naturaleza, cualidad y capacidad del responsable. Asimismo, el análisis de compatibilidad también exige tener en cuenta el impacto efectivo y real, así como en la percepción, del propio afectado por el cambio de finalidad. También hay que tener en cuenta si en el nuevo tratamiento entran nuevos sujetos, nuevas comunicaciones de datos a terceros, etc. Resulta clave en la valoración precisar si se ha compensado el desvío de la finalidad con garantías para el interesado, especialmente a través de buena información y mecanismos efectivos para el ejercicio de sus derechos ante el desvío de finalidad.

La AEPD acude a la no incompatibilidad para señalar que los concejales pueden acceder a la documentación del ayuntamiento (-administraciones públicas página 38). No obstante, quien suscribe considera que se trata de una comunicación de datos con la base legal del derecho fundamental de acceso de los concejales.

Por otra parte, pone ejemplos que vendrían a ser nuevas finalidades de tratamiento, en principio amparadas por otras leyes

[22] Al respecto cabe tener especialmente en cuenta la Opinión 3/2013 del Grupo del Artículo 29 que detalla el análisis jurídico, un test o juicio de la incompatibilidad que se hace caso por caso bajo una serie de parámetros y con diferentes intensidades.

[23] Este juicio de compatibilidad en buena medida ha sido recogido en el artículo 6. 4 RGPD:

"el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:

a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;

b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;

c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;

d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;

e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización."

¿Se pueden publicar en Internet, incluyendo en la web de una Administración Local, imágenes de las fiestas patronales? (en su caso, si hay interés público, por la libertad de expresión libertad de información).

¿Se pueden publicar sanciones administrativas en el Boletín Oficial del Estado? (cobertura legal)

comunicar a los representantes de los trabajadores datos de carácter personal del personal que presta sus servicios en la correspondiente Administración Local (cobertura legal)

¿Es posible publicar en la web de una Administración Local las licencias de obras concedidas? En este caso, señala que no existe una obligación legal de las Administraciones Públicas de realizar tal publicación será necesario el consentimiento del afectado para proceder a la citada publicación.

Se considera en principio incompatible "instalar GPS en los coches del personal al servicio de un Ayuntamiento con la finalidad de localizar los vehículos y ubicación para mejorar la prestación del servicio"

VIII. ¿Qué obligaciones hay que cumplir si se tratan datos y qué medidas hay que adoptar?

1. "Más vale prevenir que curar". El modelo proactivo del RGPD

El nuevo Reglamento europeo de protección de datos apuesta por mecanismos proactivos y preventivos en vez de reactivos, en otras palabras, más vale prevenir que curar. El principio de responsabilidad proactiva incorpora una filosofía de acción que apuesta por el valor del diseño tecnológico basado en el cumplimiento normativo. El RGPD ha subrayado la obligación de actuación en defensa y prevención de riesgos a través de la llamada *accountability* o deber proactivo de adoptar medidas ordenadas a garantizar el cumplimiento normativo, procesos del diseño basado en privacidad o el desarrollo de metodologías de análisis de riesgos o *Privacy Impact Assessment*[24]. Así, impone la protección de datos desde el diseño y por defecto (art. 25)[25], de modo que la privacidad se

[24] Considerando 78: "el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. 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."

[25] "el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la

integre desde el inicio en el diseño, la gestión y ciclo de vida del tratamiento de datos. La protección de datos se ha de seguir desde el mismo desarrollo y diseño de productos.

En consecuencia, quienes traten datos como responsables o encargados, según el tipo de datos y tipo de tratamiento que realizan y sus riesgos deben elegir las medidas técnicas y organizativas de seguridad más eficaces para garantizar la seguridad de los datos tratados. Además, bajo la responsabilidad demostrada, han de poder demostrar el cumplimiento de los requisitos exigibles.

Este enfoque se basa en el necesario análisis y la gestión de riesgos para hacer un diagnóstico y adoptar las medidas técnicas y organizativas apropiadas atendiendo a la naturaleza, el ámbito, el contexto y la finalidad del tratamiento, así como considerando el riesgo. Procede (1) identificar, analizar y determinar cuáles son los riesgos; (2) la evaluación del riesgo y (3) tomar las medidas para reducir la probabilidad y el impacto.

Como se ha expuesto, en el ámbito de la investigación, (en ocasiones en archivo público o estadística) se flexibilizan no pocas obligaciones y requisitos en el tratamiento de datos. Y el modelo básico es que esta flexibilización se da *a cambio* de la efectiva disposición de garantías y adopción de técnicas (art. 89. 1º RGPD). Garantías como acuerdos de confidencialidad y cláusulas contractuales de compromiso de no reidentificación y mantenimiento de la anonimización auditorías de uso de la información anonimizada, etc.

2. Obligaciones concretas que implica la responsabilidad proactiva

De modo más concreto, en el RGPD la responsabilidad proactiva implica:

-Art. 25 RGPD. **Protección de datos desde el diseño y por defecto** con anterioridad al inicio del tratamiento y también mientras se esté desarrollando, las medidas técnicas y organizativas adecuadas para ofrecer las garantías necesarias y garantizar el cumplimiento de los requerimientos del RGPD.

-Art. 28 RGPD. Cuando se precise un encargado del tratamiento hay que ser diligente en su elección para que ofrezca las garantías suficientes para aplicar **medidas técnicas y organizativas apropiadas**

-Art. 29 RGPD. Tratamiento bajo la autoridad del responsable o del encargado.

-Art. 30 RGPD. **Registro interno de las actividades del tratamiento** que realice la organización, todas deben ser revisadas y documentadas identificando el análisis del riesgo en cada tratamiento. El artículo 31 Ley Orgánica 3/2018, de 5 de diciembre, vincula el registro de actividades de tratamientos (en la línea de la anterior LOPD al concepto de “conjuntos estructurados de datos”, no tanto a ficheros en particular. Igualmente prescribe que el responsable y el encargado que designen un delegado de protección de datos lo incluyan en el registro de actividades. También, para el sector público, el artículo 31 con el artículo 77.1 impone publicar un inventario de actividades de tratamiento, el mismo ha de expresar también la base que legitima el tratamiento de cada actividad.

-Art. 31 RGPD. Cooperación con la autoridad de control.

---

debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. 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.””

-Art. 32 RGPD. Decidir qué **medidas técnicas y organizativas** son las adecuadas según los riesgo que comporte el tratamiento.

-Art. 33 RGPD. **Notificación de una violación de la seguridad** de los datos personales a la autoridad de protección de datos.

-Art. 34 RGPD. **Comunicación de una violación de la seguridad** de los datos personales al interesado.

-Art. 35 RGPD. **Evaluación de impacto** relativo a la protección de datos. De especial importancia para el ecosistema del big data y la inteligencia artificial, el uso de decisiones algorítmicas y perfilados respecto de humanos obliga efectuar la evaluación de impacto de protección de datos (art. 35 RGPD-UE, AEPD mayo 2019), esto es, el análisis y descripción de todas las operaciones, su necesidad y la proporcionalidad y la evaluación de los riesgos (al respecto, G29-UE, 2018: 3 y ss.).

-Art. 36 RGPD. **Designación del delegado de protección de datos**.

*Excede a este documento el detalle de cómo cumplir con las obligaciones. No obstante, hay **documentos especialmente preparados para facilitar el cumplimiento**. A este respecto cabe destacar:*

Listado de elementos para el cumplimiento normativo

Guía para responsables del tratamiento

Guía práctica para las evaluaciones de impacto en la protección de datos personales

Guía cumplimiento RGPD

Estudio de impacto Guía eipd

Guía de Privacidad desde el Diseño [oct 2019]

Guía para clientes que contraten servicios de Cloud Computing [sep 2018]

Orientaciones para prestadores de servicios de Cloud Computing [sep 2018]

Guía para la gestión y notificación de brechas de seguridad

La Agencia Española de Protección de Datos (AEPD) ha elaborado una guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD para la realización de análisis de riesgos de las actividades de tratamiento con el objetivo de establecer una hoja de ruta para afrontar los riesgos del tratamiento con el fin de establecer las medidas de seguridad y los controles que garanticen los derechos y libertades de los individuos.

Guía práctica de análisis de riesgos para el tratamiento de datos personales [feb 2018]

La AEPD en su Guía Administraciones Públicas señala elementos básicos que implica la responsabilidad proactiva y la privacidad por defecto.

Recogida de datos: analizar los tipos de datos que se recaban con un criterio de minimización en función de los productos y servicios seleccionados por el usuario;

Tratamiento de los datos: analizar los procesos asociados a dichos tratamientos para que se acceda a los mínimos datos personales necesarios para ejecutarlos;

Conservación: implementar una política de conservación de datos que permita, con un criterio restrictivo, eliminar aquellos datos que no sean estrictamente necesarios;

Accesibilidad: limitar el acceso por parte de terceros a dichos datos personales.

3. Respecto del registro de actividades de tratamiento

Los responsables y encargados de tratamientos de la Administración Local deben mantener este Registro de Actividades de Tratamiento por escrito, incluso en formato electrónico, que estará a disposición de la Autoridad de Control, en el que se incluya una descripción de los tratamientos de datos.

Puede seguirse el ejemplo e información de la Guía Administraciones Públicas de la AEPD.

· ANÁLISIS DE RIESGO

En los Ayuntamientos con población inferior a 20.000 habitantes el análisis de riesgo podría llevarse a cabo con el soporte de la correspondiente Diputación Provincial.

Para facilitar el análisis de riesgo se puede utilizar esta *Guía* publicada por la Agencia Española de Protección de Datos, las herramientas de análisis de riesgos proporcionadas por el Centro Criptológico Nacional o una herramienta que incorpore una metodología de análisis de riesgo de reconocido prestigio.

· REGISTRO DE ACTIVIDADES PADRÓN DE HABITANTES

ADMINISTRACIÓN LOCAL
Nombre y datos de contacto del responsable (o representante).

ACTIVIDAD DE TRATAMIENTO.
Padrón municipal de habitantes.

FINES DEL TRATAMIENTO.
Gestión del padrón municipal de habitantes acorde a los fines que establece al respecto la Ley de Bases de Régimen Local y demás normativa local aplicable. Usos también con fines históricos, estadísticos y científicos.

NOMBRE Y DATOS DE CONTACTO DEL DELEGADO DE PROTECCIÓN DE DATOS.
Correo electrónico de contacto
Dpd@ayuntamiento.es

CATEGORÍAS DE DATOS PERSONALES.
Datos identificativos: DNI/Nº de tarjeta de residencia/número de identificación de extranjero, nombre, apellidos, domicilio habitual, nacionalidad, sexo, lugar y fecha de nacimiento.
Datos académicos y profesionales.

CATEGORÍAS DE AFECTADOS.
Ciudadanos residentes en el municipio.

DESCRIPCIÓN DE LAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS DE SEGURIDAD.
Las medidas de seguridad implantadas corresponden a las aplicadas de acuerdo al Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y que se encuentran descritas en los documentos que conforman la Política de Seguridad de la Información del Ayuntamiento.

CATEGORÍAS DE DESTINATARIOS DE COMUNICACIONES, INCLUIDOS TERCEROS PAÍSES U ORGANIZACIONES INTERNACIONALES.
Instituto Nacional de Estadística. Fuerzas y Cuerpos de Seguridad. Órganos del Estado y Comunidades Autónomas cuando se pueda realizar la comunicación de datos conforme al artículo 6 del RGPD relativo a la legitimación del tratamiento.

TRANSFERENCIAS INTERNACIONALES. DOCUMENTACIÓN DE GARANTÍAS ADECUADAS EN CASO DEL 49.1.
No existen.

CUANDO SEA POSIBLE, PLAZOS PREVISTOS PARA LAS SUPRESIÓN DE LAS DIFERENTES CATEGORÍAS DE DATOS.
No existe la supresión de los datos, ya que aunque se produzca la baja del padrón, es necesario conservar los datos a efectos históricos, estadísticos y científicos.

· REGISTRO DE ACTIVIDADES SEGURIDAD

ADMINISTRACIÓN LOCAL
Nombre y datos de contacto del responsable (o representante).

ACTIVIDAD DE TRATAMIENTO
Seguridad

LEGITIMACIÓN DEL TRATAMIENTO
Artículo 6.1.e) del RGPD: Cumplimiento de una misión de interés público.

FINES DEL TRATAMIENTO
Garantizar la seguridad de personas e instalaciones

NOMBRE Y DATOS DE CONTACTO DEL DELEGADO DE PROTECCIÓN DE DATOS
Correo electrónico de contacto
Dpd@ayuntamiento.es

CATEGORÍAS DE DATOS PERSONALES.
Respecto al control de acceso: nombre, apellidos, DNI/NIF, empresa/administración.
Respecto a la videovigilancia: Imagen.

CATEGORÍAS DE AFECTADOS.
Ciudadanos que realizan trámites en el Ayuntamiento.
Personas físicas que acuden a reuniones convocadas por el Ayuntamiento.
Personal al servicio del Ayuntamiento.

DESCRIPCIÓN DE LAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS DE SEGURIDAD.
Las medidas de seguridad implantadas corresponden a las aplicadas de acuerdo al Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y que se encuentran descritas en los documentos que conforman la Política de Seguridad de la Información del Ayuntamiento.

CATEGORÍAS DE DESTINATARIOS DE COMUNICACIONES, INCLUIDOS TERCEROS PAÍSES U ORGANIZACIONES INTERNACIONALES.
Fuerzas y Cuerpos de Seguridad. Juzgados y Tribunales.

TRANSFERENCIAS INTERNACIONALES. DOCUMENTACIÓN DE GARANTÍAS ADECUADAS EN CASO DEL 49.1.
No existen.

CUANDO SEA POSIBLE, PLAZOS PREVISTOS PARA LAS SUPRESIÓN DE LAS DIFERENTES CATEGORÍAS DE DATOS.
Transcurrido un mes, salvo comunicación a Fuerzas y Cuerpos de Seguridad, o/y Juzgados y Tribunales.

4. Las variadas medidas técnicas y organizativas de seguridad, el ENS

Las medidas técnicas y organizativas de seguridad son muy variadas y su marco básico son **los artículos 32 y 33 RGPD**.

> "El RGPD no establece medidas de seguridad estáticas, por lo que **corresponderá al responsable determinar aquellas medidas de seguridad que sean necesarias** para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales" (Guía AEPD Administraciones Públicas. p. 20).

Se trata de **adaptarse dinámicamente** a la situación y riesgos de cada organización y tratamientos específicos para adoptar, entre otras muchas, las siguientes medidas:

- *análisis de riesgos*
- *Definición de funciones y obligaciones del personal*
- *Se ha formado al personal*
- *Se aplica un estándar ISO*
- *Sistemas de identificación y autenticación*

- *Declaración y gestión de incidentes de seguridad*
- *Se aplica el Esquema Nacional de Seguridad*
- *Trazabilidad (log de acceso y acciones de los usuarios)*
- *Protocolos de notificación de la violación de la seguridad de los datos*
- *Se aplica el RLOPD*
- *Copia de respaldo y recuperación (back-up) en los servidores propios y servidores en cloud*
- *Medidas en la sincronización de Protocolos de recuperación de datos*
- *Se han adoptado medidas de Seudoanonimización*
- *Cifrado Controles de acceso físico*
- *Protección del entorno de comunicaciones del sistema de información*
- *Seguridad en soportes no automatizados*
- *Auditoría de los sistemas de información*
- *Controles de acceso lógico*
- *Existe una persona responsable de la seguridad*
- *Existe un documento de seguridad*
- *Gestión de soportes y documentos (inventario de activos, entradas y salidas de datos etc.)*
- *Existen medidas de seguridad cuando se usan los datos fuera de los locales de la organización*
- *Se adoptan medidas de seguridad cuando se crean, exportan y usan datos personales en ficheros de uso temporal*
- *Existen contratos con obligaciones de seguridad en servicios externalizados*

El RGPD contempla medidas de seguridad que deben adaptarse a las características de los tratamientos, al tipo de datos tratados o a la tecnología disponible en cada momento.

Para cada uno de los tratamientos se realizará su respectivo análisis de riesgo o evaluación de impacto de privacidad para determinar las medidas de seguridad a aplicar.

En todo caso se tendrán en cuenta:

a) El cifrado de datos personales en el tratamiento de categorías especiales de datos.

b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

d) La coordinación de la gestión en materia de seguridad por el Comité de Seguridad de la Información. Para ello evalúa y valora la eficacia de las medidas técnicas y organizativas para garantizar la seguridad de los tratamientos.

Además de los artículos 32 y 33 RGPD hay que tener en cuenta la Disp. Ad. 1ª LOPD con referencia al ENS, que deben ser equivalentes en las formas privadas del sector público. Cabe remitir al Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad .

Y cabe señalar que este nivel de seguridad se impone asimismo a “los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato”

5. Las quiebras de seguridad y el deber de su notificación y comunicación

El RGPD define las violaciones de seguridad de los datos, más comúnmente conocidas como “quiebras de seguridad”, de una forma muy amplia, que incluye todo incidente 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. Sucesos como la pérdida de un ordenador portátil, el acceso no autorizado a las bases de datos de una organización (incluso por su propio personal) o el borrado accidental de algunos registros constituyen violaciones de seguridad a la luz del RGPD y deben ser tratadas como el Reglamento establece.

Cuando se produzca una violación de la seguridad de los datos, el responsable debe notificarla a la autoridad de protección de datos competente, a menos que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados.

La notificación de la quiebra a las autoridades debe producirse sin dilación indebida y, a ser posible, dentro de las 72 horas siguientes a que el responsable tenga constancia de ella.

La notificación ha de incluir un contenido mínimo:

- *La naturaleza de la violación*
- *Categorías de datos y de interesados afectados*
- *Medidas adoptadas por el responsable para solventar la quiebra*
- *Si procede, las medidas aplicadas para paliar los posibles efectos negativos sobre los interesados*

Los responsables deben documentar todas las violaciones de seguridad.

En los casos en que sea probable que la violación de seguridad entrañe un alto riesgo para los derechos o libertades de los interesados, la notificación a la autoridad de supervisión deberá complementarse con una notificación dirigida a estos últimos.

El objetivo de la notificación a los afectados es permitir que puedan tomar medidas para protegerse de sus consecuencias. Por ello, el RGPD requiere que se realice sin dilación indebida, sin hacer referencia ni al momento en que se tenga constancia de ella ni tampoco a la posibilidad de efectuar la notificación dentro de un plazo de 72 horas. El propósito es siempre que el interesado afectado pueda reaccionar tan pronto como sea posible.

IX. ¿Puedo enviar los datos fuera de España?

Sin perjuicio de lo afirmado de los requisitos para comunicar datos, así como del acceso a los datos por corresponsables y encargados, hay **requisitos específicos para que los datos puedan moverse internacionalmente**.

Como punto de partida y para el sector público hay que partir de **la más reciente regulación por el nuevo Artículo 46 bis**. Ubicación de los sistemas de información y comunicaciones para el registro de datos **Ley 40/2015** reformado en 2019.

> Los sistemas de información y comunicaciones para la recogida, almacenamiento, procesamiento y gestión del censo electoral, los padrones municipales de habitantes y otros registros de población, datos fiscales relacionados con tributos propios o cedidos y datos de los usuarios del sistema nacional de salud, así como los correspondientes tratamientos de datos personales, **deberán ubicarse y prestarse dentro del territorio de la Unión Europea.**
>
> Los datos a que se refiere el apartado anterior no podrán ser objeto de transferencia a un tercer país u organización internacional, con excepción de los que hayan sido objeto de una decisión de adecuación de la Comisión Europea o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España.

El resto de datos que trate el sector público en principio seguirán el régimen ordinario de las transferencias internacionales de datos. Así, el resto de los datos personales que se manejen, en principio pueden transferirse dentro de la UE y del llamado Espacio Económico Europeo[26].

Sin embargo, en principio no pueden transferirse a otros países (terceros países, salvo que se den unos requisitos (artículos 45, 47 y 49 RGPD)[27].

- Sí que pueden transferirse a países respecto de los que la Comisión ha adoptado una decisión reconociendo que ofrecen un nivel de protección adecuado **(Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda, Japón y Estados Unidos, Japón**[28].

En todo caso, el **sistema con Estados Unidos hay que estar por la situación desde 2020 con la nueva declaración de ilegalidad del acuerdo Privacyshield.**

También pueden transferirse internacionalmente datos si se cuenta con unas garantías adecuadas sobre la protección que los datos recibirán en su destino (Cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión; Códigos de conducta junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías

---

[26] que incluye también (Liechtenstein, Islandia y Noruega

[27] Una información general sobre transferencias internacionales de la AEPD en https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/transferencias-internacionales

[28] Suiza. Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000

Canadá. Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos

Argentina. Decisión 2003/490/CE de la Comisión, de 3 de junio de 2003

Guernsey. Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003

Isla de Man. Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004

Jersey. Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008

Islas Feroe. Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010

Andorra. Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010

Israel. Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011

Uruguay. Decisión 2012/484/UE, de la Comisión de 21 de agosto de 2012.

Nueva Zelanda. Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012

Estados Unidos. Aplicable a las entidades certificadas en el marco del Escudo de Privacidad UE-EE.UU. Decisión (UE) 2016/1250 de la Comisión, de 12 de julio de 2016.

Japón. Decisión de 23 de enero de 2019.

adecuadas, incluidas las relativas a los derechos de los interesados o Mecanismos de certificación).

Si no se está en los casos anteriores, también es posible transferir datos si se dan una serie de requisitos, entre los que hay que destacar el **consentimiento del interesado**[29].

Si no se da alguna de los supuestos anteriores, se requiere **autorización** previa del Director de la Agencia Española de Protección de Datos.

Así pues, si se prevé la cooperación o contratación con organizaciones de fuera de la UE (o del EEE) es de interés tener en cuenta el tipo de país de que se trata. En el caso de datos tratados a través del consentimiento cautelarmente interesa contar con el consentimiento para la transferencia internacional de datos por los interesados.

Téngase en cuenta especialmente el uso público de plataformas o redes sociales y la difusión de imágenes o datos de la ciudadanía. .

De particular interés es el **uso de sistemas de nube**[30] ubicados fuera de la UE, particularmente en EEUU. Igualmente en el ámbito académico y de investigación hay que tener especiales cautelas en el ámbito de títulos, certificaciones y la propia investigación con organismos extranjeros.

Ahora bien, dicho lo anterior, en el ámbito del sector público hay que estar especialmente atento

tratamiento de datos lo dispuesto en el Esquema Nacional de Seguridad. A este respecto, puede consultar los siguientes documentos:

Guía estratégica en seguridad para Entes locales.

Guía para Entidades locales de menos de 2000 habitantes.

[29] a) El interesado haya dado explícitamente su consentimiento

b) La transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado

c) La transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica

d) La transferencia sea necesaria por razones importantes de interés público

e) La transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones

f) La transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento

g) La transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta.

[30] Sobre el tema son de interés las Guías de la AEPD, así como Cotino Hueso, Lorenzo, "Algunas cuestiones clave de protección de datos en la nube. Hacia una 'regulación nebulosa'", en *Revista Catalana de Derecho Público* nº 51 (diciembre 2015), pp. 85-103 DOI: 10.2436/20.8030.01.55. Acceso texto completo http://revistes.eapc.gencat.cat/index.php/rcdp/article/view/10.2436-20.8030.01.55/n51-cotino-es.pdf

X. ¿Pueden las personas ejercer derechos y reclamaciones ante la entidad local?

1. ¿Qué derechos pueden exigir los interesados?

La regulación de protección de datos reconoce diversos derechos a los interesados cuyos datos se tratan (derechos de acceso, rectificación, supresión -derecho al olvido-, oposición, portabilidad y limitación del tratamiento).

De modo muy sucinto cabe recordar:

-el derecho de acceso como el derecho del interesado a solicitar y obtener del responsable del tratamiento, gratuitamente, **información sobre el tratamiento** de sus datos de carácter personal (artículo 15 RGPD)

-derecho de **rectificación** como el derecho que tiene el interesado a rectificar sus datos cuando sean inexactos (artículo 16 RGPD).

- El responsable del tratamiento tendrá la obligación de **borrar** los datos cuando no sean ya necesarios, o ya no se tenga el consentimiento o la base de legitimación, cuando se trataron ilegalmente, cuando el interesado se oponga) (artículo 17 del RGPD).

-En los casos en los que se tratan datos sin el consentimiento del interesado, éste puede **oponerse** en cualquier momento y señalar los motivos relacionados con su situación particular para que dejen de tratarse (artículo 21 del RGPD,) a que los datos personales que le conciernan sean objeto de un tratamiento

-Uno de los nuevos derechos es el derecho a la **portabilidad** de los datos, **pero el mismo no aplica propiamente a las Administraciones Públicas** . Se trata del "derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado" (art. 20. 1º RGPD). Este derecho se aplicará cuando el tratamiento esté basado en el consentimiento o en la ejecución de un contrato y el tratamiento se efectúe por medios automatizados (art. 20. 1º RGPD).[31]

Otro de los nuevos derechos del RGPD es la **limitación de tratamiento** (art. 18 RGPD). Se trata del derecho a que cuando se solicite, los "datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.

2. ¿Qué obligaciones implican para quienes tratan datos personales?

Si la entidad local o sus entes dependientes tratan datos de interesados como responsables –o como encargados-, es una obligación poder dar respuesta al ejercicio de los derechos. Y lo cierto es que **estos derechos afectan y mucho a la gestión interna de toda organización que trate datos y obligan a tomar decisiones de organización de la información que quede dispuesta a posibilitarlos.**

[31] Hay que tener presente las FAQ del Grupo del artículo 29 al respecto (http://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/3122.pdf) y lo afirmado por la Agencia siguiendo aquéllas.

Es imposible hacer efectivo el acceso si no se gestiona bien la información. De hecho, la posibilidad de ejercer estos derechos expresa un funcionamiento inadecuado de los procedimientos y gestión (por ejemplo, por no haber cancelado datos).

En el caso de la portabilidad, obliga a adoptar decisiones materiales de infraestructura tecnológica y de gestión.

Además, como se recuerda en el Considerando 59 "Deben arbitrarse fórmulas para facilitar al interesado el ejercicio de sus derechos […] El responsable del tratamiento también debe proporcionar medios para que las solicitudes se presenten por medios electrónicos". El artículo 13 no impone una obligación general de ejercicio electrónico de derecho (sólo "si procede"). Pero hay que estar a la regulación concreta de cada derecho y al desarrollo nacional.

De particular importancia en la gestión son derechos como la limitación del tratamiento y en especial la portabilidad.

Es bien posible que alguien pregunte la información que se tiene sobre él, y al conocerla pretenda que se rectifique o se suprima, o se oponga al tratamiento lícito de esta información, o quiera llevársela a otra parte. No obstante, pese a que estos derechos son afines, e incluso su ejercicio natural esté encadenado, se trata de derechos autónomos o independientes.

Estos derechos quedan desarrollados y regulados en el RGPD. Por cuanto a su régimen general cabe tener en cuenta que:

- El ejercicio es gratuito, no obstante, si las solicitudes son manifiestamente infundadas o excesivas (carácter repetitivo) el responsable podrá cobrar un canon proporcional a los costes administrativos soportados o negarse a actuar.

- Debe darse respuesta en el plazo general de un mes. No obstante, se puede prorrogar otros dos meses más, teniendo en cuenta la complejidad y número de solicitudes. Si el responsable no da curso a la solicitud, informará y a más tardar en un mes, de las razones de su no actuación y la posibilidad de reclamar ante una Autoridad de Control.

- El responsable está obligado a informar sobre los medios para ejercitar estos derechos. Estos medios deben ser accesibles y no se puede denegar este derecho por el solo motivo de que optes por otro medio. Así pues, hay elección de medio por afectado, no se le puede imponer un procedimiento determinado como el uso de un concreto impreso (art. 12 LOPD). No obstante, cabría darse la posibilidad de que el medio elegido diferente al electrónico podría generar costes que se trasladasen a afectado.

-Es muy importante para el responsable –o en su caso el encargado- genere un sistema de prueba, puesto que la "prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulado por el afectado recaerá sobre el responsable" (art. 12. 4º LOPD)

- Son derechos personalísimos que se ejercen por el titular. Ahora bien, se pueden ejercer directamente o por medio de tu representante legal o voluntario. Si el responsable tiene dudas sobre la identidad, puede solicitar información adicional para confirmar la misma como la fotocopia del DNI o pasaporte u otro documento válido. También se puede usar la firma electrónica en vez del DNI. En el caso de representantes, la representación conferida o el documento o instrumento electrónico que acredite la representación. El derecho puede denegarse por no poder verificar razonablemente la identidad del solicitante. Hay especialidades respecto de menores e incapaces[32]

La petición va dirigida al **responsable** que posea o trate los datos personales, a través de los mecanismos sobre los que está obligado a informar. Cabe la posibilidad de que por

[32] En los casos de incapacidad o minoría de edad se habrá de acreditar la condición de representante legal. En principio el menor que tenga la edad para consentir el tratamiento de datos (14 años) ejercerá por sí los derechos y los titulares de la patria potestad ejercerán los derechos de los menores de 14 años (art. 12 LOPD). Ahora bien, se trata de una cuestión compleja que puede llevar a que los padres o tutores tengan interés legítimo para solicitar información y datos por sus deberes y obligaciones (patria potestad, alimentos, etc.) y, por ello, puedan solicitar y acceder a información del menor mayor de 14 años, e incluso del mayor de edad.

cuenta del responsable, sea el **encargado** el que atienda tu solicitud, si ambos lo han establecido en el contrato o acto jurídico que les vincule (art. 12 LOPD)

La **comunicación para el ejercicio de derechos** incluirá, además de la identificación oportuna: la petición en que se concreta la solicitud; la dirección a efectos de notificaciones, fecha y tu firma y documentos acreditativos de la petición que realices, si fuesen necesario.

En la **respuesta** a quien ejerza el derecho es obligatorio informar sobre la posibilidad de invocar la tutela de la autoridad de control en caso de denegación que ahora, además, debe incluir la información sobre la posibilidad de acceso a la jurisdicción. Cabe señalar asimismo que ante el procedimiento del artículo 37 LOPD de reclamación voluntaria al DPD previa a la AGPD, debe informarse de esta posibilidad de acudir al DPD.

Para el caso de recibir cualquier petición o ejercicio de derechos procede sin duda comunicarlo al DPD

3. ¿Cuándo no es obligatorio dar respuesta a estos derechos?

Estos derechos serán exigibles salvo que hubiera una excepción legal (art. 23 RGPD). En todo caso, hay que señalar que estas excepciones a los derechos pueden darse en el ámbito de la investigación (art. 89 RGPD). Así por ejemplo, no procede la información y transparencia obligatoria (art. 14.5º b) RGPD) cuando ello "resulte imposible o suponga un esfuerzo desproporcionado". En todo caso, hay limitaciones específicas previstas por el RGPD (Art. 23 en general) que deben contenerse en regulaciones legales expresas. Las mismas pueden darse especialmente en el ámbito de seguridad o investigación, por ejemplo.

4. ¿Cuándo suprimo, borro y bloqueo datos? ¿A quién debo comunicarlo?

Por cuanto a la supresión, debe señalarse que se trata de una **cuestión bien compleja la procedencia de la supresión de los datos y su efectivo borrado o "destrucción"** (art. 32 LOPD). Cuando proceda la supresión de los datos –también respecto de los datos rectificados- debe darse el "bloqueo" de los datos, esto es, "la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización".

Así pues, **los datos se mantienen, pero bloqueados (y con especiales medidas de seguridad)** y quedan fuera del flujo de datos de la organización y únicamente, sólo, "para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y sólo por el plazo de prescripción de las mismas." Así pues, cuando procede suprimir los datos, no se borran o destruyen, sino que se mantienen bloqueados para atender posibles responsabilidades jurídicas de cada tipo de relación contractual, de consumo,

administrativa, etc. Así, durante el plazo de prescripción de posibles responsabilidades, una vez pasado este plazo, procederá la destrucción.

Por cuanto al bloqueo el artículo 32.4º LOPD añade que cuando "la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que **implique un esfuerzo desproporcionado**, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo."

Asimismo, el apartado 5º remite a las autoridades de datos para establecer posibles "**excepciones a la obligación de bloqueo** […cuando éste] pudiera generar un riesgo elevado […o] un coste desproporcionado". Cabe añadir que como excepción no se dará el bloqueo respecto de la videovigilancia (art. 22 LOPD) y de los sistemas de denuncias internas (art. 24 LOPD).

Debe recordarse que el derecho a suprimir datos es diferente del derecho de los interesados a revocar o retirar su consentimiento.

En el caso de la supresión, es importante la regulación del artículo 17. 2º RGPD, por cuanto **si procede la supresión hay que informar a otros que traten datos de que se han suprimido**: "teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos."

De hecho hay que tener en cuenta el artículo 19 para rectificación, supresión y limitación de tratamiento:

"El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16 [rectificación], al artículo 17, apartado 1 [supresión], y al artículo 18 [limitación] a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita."

Se trata de una novedad del RGPD relevante que habrá que implantar prácticamente y en cada supuesto y que puede implicar importantes acciones para quienes traten datos, especialmente en el ámbito de plataformas y prestadores de servicios de la sociedad de la información.