MANUAL-GUÍA
SOBRE IMPACTOS DEL REGLAMENTO (UE) DE PROTECCIÓN DE DATOS EN LOS ENTES LOCALES

Rafael Jiménez Asensio.
Consultor "Estudio Sector Público SLPU": Coordinación y redacción del documento-base.

Ascen Moro.
Responsable de la Unidad de Gestión del Conocimiento y Calidad del Ayuntamiento de Sant Feliu de Llobregat.

Federació de Municipis de Catalunya

Han colaborado en la elaboración de la Guía: **Josep Betriu**, letrado; **Irati Labaka Garmendia**, Estudio Sector Público; **Albert Guilera**, letrado; **Estela Ribes Caballer**, politóloga; **Alba Sánchez**, letrada.

ACM Associació Catalana de Municipis

Edita

Federació de Municipis de Catalunya
Via Laietana 33, 6è 1a. 08003 Barcelona

Associació Catalana de Municipis
Carrer de València, 231, 08007 Barcelona

Coordinación general
Juan Ignacio Soto Valle
Marc Pifarré i Estrada

Dirección académica
Rafael Jiménez Asensio

Autores
Rafael Jiménez Asensio
Ascen Moro

Colaboradores
Josep Betriu
Irati Labaka Garmendia
Albert Guilera
Estela Ribes Caballer
Alba Sánchez

Equipo técnico
Laura Gálvez
Mercè Canals
Elisabet Pérez

Diseño y maquetación
www.lacuinagrafica.com

ISBN 78-84-87286-61-2

ÍNDICE

LA NECESIDAD DE REGULACIÓN EN MATERIA DE DATOS PERSONALES:

“Hay una cosa cierta al menos y es que también en este caso lo que se impone es la palabra regulación frente a una mercantilización y una desregulación del mundo sin equivalente alguno en la historia de la humanidad”

(Luc Ferry, La revolución transhumanista. Cómo la tecnologíaa y la uberización del mundo van a transformar nuestras vidas, Alianza Editorial, 2017, p. 154)

¿LLEGA TAL VEZ TARDE?:

“No es de extrañar que Alphabet (Google) ya no hurgue en nuestros correos electrónicos personales para mostrarnos anuncios personalizados: ya sabe todo de cada uno de nosotros y puede prescindir de más información (…) Es decir, en la medida en que el entorno normativo se vuelva más problemático y/o el mercado publicitario se desacelere (…) la compañía tendría un modelo de negocio muy robusto: vender ‘servicios inteligentes’ (IA), tanto a ciudadanos como a gobiernos”

(Evgeny Morozov, Capitalismo “Big Tech” ¿Welfare o neofeudalismo digital? Enclave, 2018 pp. 23-24)

LAS TAREAS PENDIENTES

“Como los malos estudiantes, la mayoría de empresas españolas (y no digo nada de la Administración) no han hecho los deberes y ahora se acuerdan de Santa Bárbara, o de Santo Dato, cuando ya se escuchan los primeros truenos”.

(Borja Adsuara Varela. Protección de Datos: Quedan solo cuatro meses para ponerse al día, Retina, enero 2018)

PRESENTACIÓN

La finalidad de la presente Guía es ofrecer a los operadores del mundo local, tanto políticos como empleados públicos, así como también a la ciudadanía que se relaciona con ese nivel de gobierno, una suerte de manual básico sobre cuáles son las novedades más importantes del Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en lo sucesivo RGPD), en lo que pueden estimarse como los impactos más relevantes que afectaran a los entes locales catalanes y, asimismo, a las entidades de su sector público vinculadas, dependientes o adscritas. En cualquier caso, dado el ámbito de aplicación del RGPD, lo que aquí sigue puede ser aplicado no solo a los entes locales catalanes, sino a cualquier gobierno local y, con las modulaciones que procedan, también a otras Administraciones Públicas territoriales o entes de su sector público.

El enfoque de este breve trabajo es predominantemente explicativo. Se pretende que el lector no informado o escasamente documentado sobre esta nueva realidad normativa, comprenda el alcance de este marco regulador y sobre cuáles serán sus efectos aplicativos a partir del 25 de mayo de 2018. El tratamiento de este tema se hace mediante un análisis sistemático del RGPD donde se intercalan algunos documentos de interés (preferentemente de las autoridades de control o del grupo de trabajo del Artículo 29), así como se exponen algunas ideas-fuerza y otras recomendaciones u opiniones, que el tiempo habrá de contrastar.

Por tanto, antes de precisar su contenido conviene adelantar lo que la Guía no es. No es, en primer lugar, una Guía para especialistas o personas que trabajan en el ámbito de la protección de datos, aunque algunas de las cuestiones que en este texto se tratan puedan asimismo interesarles o servirles, en su caso, de orientación o información adicional. Tampoco es, en segundo lugar, una guía meramente aplicativa (un enfoque que es el seguido por el "Decálogo para la adecuación al Reglamento General de Protección de Datos (RGPD) en las Administraciones Públicas" publicado recientemente por la FEMP (aunque el enlace, tras algún tiempo activo se ha desactivado recientemente) o por el documento recientemente publicado por la AEPD titulado "Protección de Datos y Administración Local" y, particularmente, por otros diferentes e importantes documentos elaborados, ya sea conjunta o individualmente, tanto por la ACPD o adpCat (Autoridad Catalana de Protección de Datos), como por la AEPD (Agencia Española de Protección de Datos) o la AVPD (Agencia Vasca de Protección de Datos), contenidosen el anexo documental a este Manual-Guía y algunos de los cuales se citan en este texto.

Ello en ningún caso supone que no sea de utilidad su uso o consulta, pues también se incorporarán algunos consejos puntuales sobre cómo aplicar determinados aspectos de la nueva regulación por los entes locales, incorporándose diferentes cuadros para determinar qué medidas y protocolos adoptar en la implantación de aspectos relevantes del nuevo marco normativo, tales como el Registro de las Actividades de Tratamiento, la Seguridad en los tratamientos, el Análisis de Riesgos, la Evaluación de Impacto o el proceso de designación de la figura del delegado de protección de datos, por traer a colación cinco ejemplos de indudable trascendencia para el funcionamiento del nuevo modelo de gestión de datos personales en las Administraciones Locales.

Este Manual-Guía pretende, por consiguiente, ser una herramienta básicamente pedagógica que facilite la introducción a este nuevo modelo institucional y de gestión de datos personales y, asimismo, su cabal comprensión, pues no cabe duda alguna que el RGPD representa un notable **cambio de paradigma** en el modo y manera de comprender y aplicar esta cuestión en el ámbito local de gobierno o en cualquier organización de carácter público.

En todo caso, aunque el presente trabajo solo se ocupa del RGPD, se recogerán también de forma adicional y con fines meramente informativos (y un carácter obviamente provisional) algunas referencias puntuales al texto del Proyecto de Ley Orgánica de Protección de Datos (PLOPD) de carácter personal, actualmente en tramitación en las Cortes Generales. Cuando este texto se apruebe definitivamente y sea publicado en el "BOE" habrá, sin duda, que volver a redefinir algunos aspectos puntuales de esta Guía.

Pero no cabe llamarse a engaño. Dada la naturaleza del instrumento normativo elegido (Reglamento de la Unión Europea), la posición esta vez de la LOPD será, a diferencia de la anterior, mucho más vicarial o complementaria. Ciertamente, el RGPD llama en más de cincuenta supuestos a que "sus normas sean especificadas o restringidas por el Derecho de los Estados miembros", pero el RGPD con carácter general tiene primacía aplicativa y entra en una serie de detalles en la regulación que la propia LOPD solo podrá reenviar a lo establecido en el Reglamento.

Por consiguiente, frente a la situación anterior, **el operador** político, directivo o técnico **deberá actuar a partir de este nuevo marco con un binomio normativo que habrá de consultar en paralelo: RGPD y LOPD** (así como reglamentos que la desarrollen). Así, no cabe extrañarse de que este último texto (el actual PLOPD) lleve a cabo remisiones constantes a artículos del propio RGPD. El régimen jurídico de protección de datos personales descansará, así, sobre dos "pantallas normativas" que se deben visualizar conjuntamente: RGPD y LOPD. No habrá, ni se la espera, norma que sintetice esa regulación.

El contenido de la presente guía es muy sencillo de explicar.

La parte central es una suerte de manual explicativo de lo que son los rasgos principales de la nueva normativa y de sus hipotéticos impactos sobre los gobiernos locales. Esta parte se estructura en tres grandes ejes:

- El primero analiza **la transformación radical que se ha producido en el modelo de protección de datos de carácter personal.**

- El segundo se ocupa **de las cuestiones generales** que trata el Reglamento: especialmente**, principios y derechos;** con un enfoque predominante hacia la ciudadanía, pero también a la Administración que ha de tratar estos datos.

- Y el tercero pone el foco de atención en los elementos centrales del **nuevo modelo institucional y de gestión de protección de datos personales** y su aplicación sobre los gobiernos locales.

No se tratarán en esta guía, al menos directamente, aquellos aspectos que, en principio, inciden menos directamente sobre la actuación de los gobiernos locales. Por ejemplo, no se aborda un tratamiento específico del Capítulo V (transferencias de datos personales a terceros países u organizaciones internacionales) o del Capítulo VII (Cooperación y coherencia), entre otros temas, sin perjuicio de que todas estas previsiones normativas se deben tener completamente en cuenta en el tratamiento de datos personales por el sector público, más aún en un entorno de globalización de los datos y de cruce permanente de información.

Cabe agradecer, en este sentido, las aportaciones o sugerencias que al contenido inicial ha llevado a cabo mi buen amigo Iñaki Vicuña, director del CENDOJ (Consejo General del Poder Judicial) y, en su día, también director de la Agencia Vasca de Protección de Datos, así como Ascen Moro del Ayuntamiento de Sant Feliu de Llobregat. En todo caso, los errores u omisiones solo se pueden imputar a quien ha estado encargado de redactar el documento-base.

La Guía contiene asimismo un análisis de caso o buena práctica. **Se trata de exponer lo que ha sido y será la gestión de protección de datos de carácter personal en el Ayuntamiento de Sant Feliu de Llobregat** *(La seguridad integral y el nuevo modelo organizativo. Los retos de adecuación al RGPD)*. **Esta parte ha sido elaborada por la persona responsable en tal materia en el citado Ayuntamiento**. Sin duda, **Sant Feliu de Llobregat es uno de los municipios catalanes con un desarrollo digital y de seguridad de datos más relevante**, hasta el punto de que su modelo de gestión ha sido objeto de análisis en algunos libros y premiado en diferentes foros de gestión pública e innovación. De ahí su importancia de tratarlo en esta guía. Lo que ha hecho y lo que se proponga hacer puede ser tomado como senda por otras organizaciones locales.

Y, en fin, la guía, que es un trabajo colectivo de un equipo que se enuncia al principio, se cierra con un breve dossier de documentación muy selectivo, donde se pretenden recoger una serie de referencias jurisprudenciales, doctrinales y documentales, que puedan ayudar al operador, sea político o técnico, para saber más o completar algunas de las cuestiones que sucintamente se tratan en el presente texto.

NOTA: *En esta guía las referencias al RGPD se hacen al texto oficial editado en castellano. Hay una versión traducida al catalán (sin carácter oficial) realizada por la Autoritat Catalana de Protecció de Dades: http://apdcat.gencat.cat/ca/documentacio/RGPD/textos_normatius/*

Asimismo, algunas referencias a documentos publicados por la AEPD, especialmente el último ("Protección de Datos y Administración Local"), en cuanto que no tienen versión oficial traducida al catalán, se ha preferido mantener la redacción inicial en castellano. Ver el documento citado en: http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2018/notas_prensa/news/2018_04_03-ides-idphp.php

1. LÍNEAS-FUERZA DEL NUEVO MARCO NORMATIVO DE LA UE EN MATERIA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

¿Por qué una nueva regulación europea?

La necesidad objetiva de la nueva regulación europea en materia de protección de datos de carácter personal surge del propio contexto tecnológico y de su evolución en las dos últimas décadas. En efecto, en los años transcurridos desde 1995 (fecha de aprobación de la Directiva) a 2016 (fecha de entrada en vigor del Reglamento) la digitalización y la revolución tecnológica, así como la globalización de los propios datos, ha generando nuevos e importantes retos para la protección de los datos personales y, en particular, para los derechos y libertades de los ciudadanos. Y nada sabemos con certeza, aunque lo intuyamos, sobre qué pasará en un futuro inmediato. Innumerables incógnitas, incertidumbres y no menos perplejidades rodean el desarrollo de la automatización, de la inteligencia artificial y del Big Data (por no hablar de los ordenadores computacionales, que anuncian el fin de la privacidad) a escala aún desconocida.

La aceleración de los procesos tecnológicos y su impacto sobre los datos personales es, hoy en día, una realidad incontestable, que irá creciendo cada vez más, por lo que esta nueva regulación no solo se dicta para afrontar los retos del presente, sino en especial los grandes desafíos del futuro en materia de protección de datos y de garantía de los derechos y libertades de los ciudadanos, ámbitos que en estos momentos están siendo objeto de una erosión nunca conocida hasta la fecha. El riesgo que se corre es que llegue tarde o que pronto se quede corta, sobre todo por las dificultades de adaptación que el marco regulador europeo presenta.

La manipulación de datos personales con fines absolutamente espurios (recuérdese el reciente caso Cambridge Analytica) afecta principalmente a las grandes compañías tecnológicas, pero advierte claramente de una tendencia ya fuertemente arraigada de mal uso de los datos personales por las grandes compañías tecnológicas (en régimen de casi monopolio global) y empresas de intermediación. En este acelerado contexto, el papel del sector público y, particularmente, de la Administración Local, adquiere un rol de gran importancia para preservar los derechos y libertades de la ciudadanía. La protección de los datos personales que maneja cotidianamente cualquier nivel de gobierno se transforma en un reto de alto valor democrático.

La idea está perfectamente expresada en el Considerando 6 del RGPD: *"La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales"*

¿Cuáles son los motivos por los que se ha derogado la Directiva de 1995 y se ha aprobado el Reglamento de 2016?

La derogación de la Directiva 96/45/CE y su sustitución por el RGPD no es una operación normativa menor. El cambio de instrumento regulador obedece a razones de contexto y a la necesidad objetiva de establecer un Reglamento que, como es sabido, tiene un alcance general, es obligatorio en todos sus elementos y directamente aplicable.

Su entrada en vigor se produjo a los veinte días de su publicación en el DOUE, pero su plena aplicabilidad es a partir del 25 de mayo de 2018 (artículo 99 RGPD).

En los Considerandos 9 a 13 del RGPD se explicitan cuáles han sido los motivos que han justificado el cambio de instrumento normativo. Entre los que caben citar los siguientes:

- La aplicación de la Directiva 1995 ha sido fragmentaria y desigual, mientras que los riesgos para la protección de datos son cada vez mayores.

- Se quiere garantizar un nivel uniforme y elevado de protección de datos personales, y que sea además equivalente en todos los Estados miembros. La aplicación de las normas de protección de datos se pretende que sea coherente y homogénea.

- La protección efectiva de los datos personales exige reforzar las obligaciones de quienes los tratan, reconocer poderes equivalentes para supervisar y garantizar su cumplimiento, así como que las infracciones se castiguen con sanciones equivalentes.

- Hay base jurídica para esta regulación en el artículo 16. 2 del TFUE. Aunque el derecho fundamental ya estaba recogido (luego trasladado al propio TFUE) en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea.

- Era, por tanto, necesario regular esta materia por un Reglamento que proporcionara seguridad jurídica y transparencia.

El nuevo marco normativo del RGPD como cambio de paradigma

Este punto requiere un desarrollo algo más detenido. En efecto, la nota distintiva del actual marco normativo (RGPD-futura LOPD) frente al vigente hasta ahora (Directiva-LOPD) reside en transitar **desde un modelo reactivo a un modelo proactivo o centrado en el "enfoque de riesgos".**

En cierta medida se puede afirmar que se traslada a la protección de datos de carácter personal (aunque con algunas limitaciones, según se verá) la política de compliance, en la que **la dimensión preventiva o anticipadora es una de las claves de bóveda del modelo que se pretende construir**.

Como se ha venido reconociendo, también por la AEPD, en verdad se ha producido un **auténtico cambio de paradigma** en el modo y manera de gestionar los datos personales con innegables consecuencias.

En esta lógica encuentran pleno sentido diferentes instrumentos o instituciones que se articulan dentro de lo que se podría denominar como **un nuevo modelo institucional y de gestión de las protección de datos en las organizaciones públicas,** que descansa principalmente sobre los siguientes ejes de nueva configuración:

1. Nuevo rol o nuevo marco de responsabilidades del responsable y del encargado de tratamiento de datos
2. Registro de las actividades de tratamiento.
3. Obligaciones específicas vinculadas con la seguridad (*breach data)*
4. Análisis de riesgos en el tratamiento.
5. Evaluación de impacto de las operaciones de tratamiento.
6. Implantación de la figura del delegado de protección de datos (preceptiva en las administraciones públicas)
7. Códigos de conducta y mecanismos de certificación
8. Refuerzo del papel de las autoridades de control (adpCAT/AEPD/AVPD)

No acaban aquí los elementos de esa nueva arquitectura del modelo institucional y de gestión de protección de datos, pero tales aspectos se abordarán puntualmente en otros pasajes de esta guía.

En cualquier caso, este nuevo enfoque tiene ya algunos impactos evidentes. Por ejemplo:

- Decae la obligación de notificar a las autoridades de control la existencia de ficheros automatizados.
- Pierde sentido, al menos con carácter general, la diferenciación entre niveles de protección alto, medio y bajo, establecidos en la normativa en vigor (Ver lo expuesto más adelante: "Medidas de Seguridad").

IDEA-FUERZA:

Ante la constante evolución tecnológica y los procesos de transformación digital que sufren las actividades de tratamiento de datos personales, la reforma de la regulación de protección de datos supone un cambio del modelo tradicional para afrontar las medidas que garantizan la protección de datos personales hacia un nuevo modelo más dinámico, enfocado en la gestión continua de los riesgos potenciales asociados al tratamiento desde su diseño"

(AEPD, Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD)

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2018/notas_prensa/news/2018_02_28-ides-idphp.php

2. CUESTIONES GENERALES DEL RGPD. ALGUNAS NOVEDADES SOBRE PRINCIPIOS Y DERECHOS

Introducción. Algunas claves para la comprensión del RGPD

En un manual-guía sobre el impacto del RGPD en las entidades locales no puede faltar un tratamiento, aunque sea epidérmico, de lo que aquí de denomina como "Cuestiones Generales", con especial atención a las novedades sobre "principios" y "derechos", algunas de ellas con particular incidencia en el quehacer cotidiano de las Administraciones locales cuando traten datos personales.

En todo caso, la Administración Local se caracteriza por su proximidad a la ciudadanía. Y no cabe descartar que, también en esta materia de protección de datos personales, las autoridades locales y sus agentes deban llevar a cabo una labor de difusión y sensibilización entre la ciudadanía, complementaria a la realizada por las autoridades de control, sobre cuáles son los derechos nuevos que las personas físicas tienen, también en relación con el tratamiento de datos personales que se lleven a cabo por las organizaciones públicas. La perspectiva del ciudadano es importante también en este caso, en especial en Administraciones Públicas prestadoras de servicios.

Así, **no puede olvidarse nunca que el RGPD tiene por objeto la protección de las personas físicas en lo que respecta a sus derechos fundamentales y libertades públicas en su**

conjunto, no solo (aunque también) se refiere al derecho a la protección de sus datos personales, sino especialmente a que a través de la lesión de este último se pueden menoscabar profundamente el ejercicio y disfrute del resto de derechos y libertades. En este punto la realidad cotidiana nos muestra que esta afectación general es cada día más real y profunda. Bajo ese punto de vista no es indiferente afirmar que **la protección de datos personales es, hoy en día, una batalla por el Estado democrático y por el sistema de derechos fundamentales asentados durante más de dos siglos en los países occidentales**.

Algunas claves para la comprensión de este segundo apartado se encuentran en los propios Considerandos del RGPD. Veamos sucintamente determinadas referencias y, en todo caso, se puede acudir a la lectura íntegra de los mismos para una comprensión cabal de la regulación que se examina.

- ***¿A qué se aplican los principios de la protección de datos?*** (Considerando 26):
    - "Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable". También a los datos "seudonimizados".
    - Pero no a la información anónima, entendida como aquella "que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable o deje de serlo" (Ver: artículo 2.2, a qué tratamientos no se aplica el RGPD)
- ***Principios*** (Considerando 39):
    - "Todo tratamiento de datos debe ser lícito y leal".
    - El principio de transparencia "exige que toda información y comunicación relativa al tratamiento de datos sea fácilmente accesible y fácil de entender y que se utilice un lenguaje sencillo y claro".
    - Los fines del tratamiento deben ser explícitos y legítimos y determinarse en el momento de su recogida.
    - Se debe garantizar que se limiten a un mínimo estricto el plazo de conservación de los datos (incorporar plazos para su supresión o revisión periódica").
- ***Nuevo régimen jurídico del consentimiento*** (Considerandos 32, 40 a 44):
    - "El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada e inequívoca".
    - Así, a partir del RGPD, debe quedar claro que el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. (Considerando 32).
    - Consentimiento o base jurídica legítima: "Para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho". Se trata de un aspecto clave, especialmente en el sector público.
    - Cuando el tratamiento se lleva a cabo con el consentimiento del interesado: "El responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento (véase las exigencias en el Considerando 42).
    - Asimismo, es importante tener en cuenta las garantías del consentimiento exigidas cuando el tratamiento lo lleva a cabo una autoridad pública (Considerando 43)
- ***Derecho al olvido*** (Considerandos 65 y 66): "Los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen y un 'derecho al olvido'".

¿Cuál es el objeto del RGPD?

El objeto último es la protección de los derechos fundamentales de las personas físicas y toda la afectación que a estos derechos y libertades **se pueda producir por el tratamiento de datos personales.** La garantía y protección de los datos personales evita, así, que el resto de derechos y libertades de la persona física se vean "manchados" o "negados" por el **efecto irradiación de los datos personales**. La seguridad de los datos por parte de la autoridad pública u organismo es consustancial, pero instrumental, para cumplir esos objetivos.

El artículo 1 RGPD condensa su objeto en los siguientes puntos:

- Establecer normas relativas a:
    - La protección de las personas físicas en lo que respecta al tratamiento de los datos personales.
    - La libre circulación de tales datos

Proteger los derechos fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.

PERSONAS FALLECIDAS:
También se ha de tener en cuenta que, tal como expone el Considerando 27, el RGPD "no se aplica a la protección de datos personales de personas fallecidas", siendo los Estados miembros competentes para establecer normas relativas al tratamiento de los datos personales de estas. Véase al respecto el artículo 3 ("Datos de las personas fallecidas") y la disposición adicional séptima ("Acceso a contenidos de personas fallecidas") del PLOPD

¿Se aplica el RGPD íntegramente a los gobiernos locales y a sus entidades del sector público?

El RGPD es desde el 25 de mayo de 2018 norma directamente aplicable en su integridad a la administración local y a las entidades de su sector público (con alguna excepción puntual que se tratará: DPD en determinadas sociedades mercantiles de capital público, al menos en la formulación actual del PLOPD).

También se han de tener en cuenta, en un contexto globalizado y de datos abiertos, las normas que regulan las transferencias de datos personales a terceros países u organismos internacionales (Capítulo V). Esta regulación no se trata en la presente guía, pero debe ser siempre y en todo caso tenida en cuenta.

IDEA-FUERZA:
"Aunque pudiera parecer que las transferencias internacionales son poco habituales en el ámbito de los entes de la Administración Local, el uso cada vez más frecuente de tecnologías de la información y la comunicación o la generalización de servicios 'en nube' (cloud computing) supone que aumenten las posibilidades de que se trasfieran estos datos fuera del Espacio Económico Europeo dentro de los contratos de servicios informáticos".
(Ver, asimismo, artículos 45 y 46 que permiten realizar dichas transferencias internacionales sin necesidad de solicitar autorización previa a la autoridad de control)

Guía para la adaptación del Reglamento General de Protección de Datos, de las Administraciones Locales, FEMP, Grupo de Trabajo para la Implantación del nuevo RGPD en las Administraciones Locales.

Las administraciones locales deberían haber adaptado sus protocolos, procedimientos y organización a las importantes medidas que se contienen en el RGPD antes de la fecha indicada

ÁMBITOS DE AFECTACIÓN DE TRATAMIENTOS EN LA ADMINISTRACIÓN LOCAL:

- Padrón municipal
- Subvenciones
- Smart Cities

Fuente: AEPD, "Protección de Datos y Administración Local", 2018

El nuevo concepto de "protección de datos" y otras definiciones

El concepto de "dato personal" se recoge en el artículo 4, 1) RGPD en los siguientes términos:

"Datos personales": toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

Otras definiciones que, por su incidencia en la actividad local, se recomienda la consulta de su alcance en el artículo 4 RGPD:

- Tratamiento
- Limitación del tratamiento
- Elaboración de perfiles
- Seudonimización
- Responsable del tratamiento
- Encargado del tratamiento
- Destinatario
- Violación de la seguridad de los datos personales
- Datos biométricos

Datos biométricos: "Tendrán la consideración de datos sensibles solo cuando sean utilizados para identificar unívocamente a una persona" (AEDP, *Protección de Datos y Administración Local*)

En particular, por la importancia que tiene en el nuevo régimen jurídico de la protección de datos personales, es importante la definición de "Consentimiento del interesado" recogida en el artículo 4, 11) RGPD:

"Consentimiento del interesado": toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;

¿"Interesado" o "afectado"? La AEPD recomienda utilizar la expresión de "afectado" y no la de "interesado", para no incurrir en confusión con la terminología establecida en la Ley 39/2015, de 1 de octubre, de procedimiento administrativo común de las Administraciones Públicas *(Protección de Datos y Administración Local)*

¿Cuáles son los principios que se deben tener en cuenta en todo tratamiento de datos personales?

Los principios de protección de datos se recogen en el Capítulo II RGPD y algunos de ellos se desarrollan en el PLOPD (inexactitud de los datos, deber de confidencialidad, consentimiento afectado y de menores, etc.).

Los principios se pueden sistematizar partiendo de la regulación que recoge el propio artículo 5 RGPD:

- Licitud, lealtad y transparencia
- Limitación de la finalidad
- Minimización de los datos
- Exactitud
- Limitación del plazo de conservación
- Integridad y confidencialidad

Sin duda, por su novedad o por su incidencia en la actividad local cabe destacar, entre otros, tres de tales principios:

Limitación de la finalidad: Los datos personales serán recogidos "con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines"

UN EJEMPLO:

Según recoge la Guía para la adaptación al RGPD de la Administración Local (FEMP), un posible supuesto de aplicación del principio de limitación de la finalidad de los datos sería el siguiente:

"¿Podría comunicarse por parte de un Ayuntamiento los datos de menores en situación de riesgo a una Mancomunidad que presta servicios sociales?"

Al margen de otras consideraciones generales que allí se realizan, se concluye del siguiente modo:

"En todo caso, será preciso tener especialmente en cuenta que el RGPD regula el principio de limitación de la finalidad, es decir, que los datos no podrán ser utilizados para fines incompatibles con los fines iniciales. Por ello, la utilización de los datos para cualquier otra finalidad distinta de la relacionada con el ejercicio de las competencias en materia de atención a menores que tiene atribuida legalmente, precisaría de otra legitimación específica a la luz de las normas de protección de datos de carácter personal" (pp. 56-57)

Minimización de los datos: Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

ALGÚN EJEMPLO:

Según recoge la Guía para la adaptación al RGPD de la Administración Local (FEMP), algunos posibles supuestos de aplicación del principio de minimización de datos serían:

- "La incorporación, tanto en la firma de los documentos electrónicos o en papel como en la marca de agua, del dato relativo al DNI del funcionario firmante, podría constituir un tratamiento excesivo y, en consecuencia, contrario al principio de minimización de datos del artículo 5 del RGPD" (p. 50)

- "Con carácter general, las grabaciones indiscriminadas de voz y de conversaciones del público en general que acceden a los edificios de un Ayuntamiento a través de sistemas de videovigilancia, no cumpliría el principio de minimización de datos, considerándose una medida intrusiva" (p. 52)

Limitación del plazo de conservación: "Los datos personales serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado".

BASE JURÍDICA

Licitud del tratamiento (artículo 6 RGPD: Consultar): El tratamiento solo será lícito si cumple (entre otras) alguna de estas condiciones:

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

- El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte

- **El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable de tratamiento.**

- Tratamiento para otros fines distintos de aquel para el que se recogieron los datos personales (ALERTA): artículo 6.4 RGPD.

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

IDEA-FUERZA:

Como se expone en el Considerando 26, "los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable". Por tanto, deben seguirse fielmente en toda operación de tratamiento de datos personales que lleven a cabo el responsable o el encargado del tratamiento.

CATEGORÍAS DE DATOS PERSONALES OBJETO DE TRATAMIENTO POR LA ADMINISTRACIÓN LOCAL:

- De carácter identificativo (nombre, apellidos, teléfono, DNI, imagen)

- De carácter tributario

- Académicos y profesionales (selección, bolsas, Recursos Humanos)

- Ejercicio de potestad sancionadora

- Categorías especiales de datos

- Smart cities

Ver: AEDP, *Protección de Datos y Administración Local*.

El PLOPD contiene algunas previsiones que conviene tener presentes:

- **Disposición adicional novena**. Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos.
- **Disposición adicional decimoquinta**. Disposiciones específicas aplicables a los tratamientos de los registros de personal del sector público.

¿Cuál es la nueva configuración del "consentimiento" en el RGPD?

Ya se ha visto la definición de consentimiento del interesado. Cuando no hay "base legal" o base jurídica específica, la Administración Pública debe solicitar inexcusablemente el consentimiento expreso e inequívoco del interesado. El artículo 6 PLOPD reenvía a la regulación del RGPD, salvo algunas precisiones (consentimiento cuando haya pluralidad de finalidades en un tratamiento). Hay una regulación particular sobre el consentimiento del niño (artículo 8 RGPD) o del menor de edad (artículo 7 PLOPD). Particular importancia tiene para la Administración Local lo establecido en el artículo 6.1 c) RGPD y artículo 8 LOPD, sobre tratamiento de datos amparados por la Ley (base jurídica legal).

En todo caso, se deben tener en cuenta asimismo las disposiciones adicionales decimotercera y transitoria sexta del PLOPD, que se recogen al final de este epígrafe.

En este nuevo ámbito de regulación cabe resaltar lo establecido en el artículo 7 RGPD relativo a lo que se denomina como Condiciones para el consentimiento. Veamos algunas de las más relevantes:

Condiciones para el consentimiento (selección):

- Si el tratamiento se basa en el consentimiento del interesado: "El responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales" (carga de la prueba del responsable)

- Si el consentimiento se da en un contexto de declaración escrita que se refiera también a otros asuntos, el "consentimiento se prestará de tal forma que se distinga claramente de los demás asuntos de forma ineludible y de fácil acceso y utilizando un lenguaje claro y sencillo".

- "El interesado tendrá derecho a retirar su consentimiento en cualquier momento (…) Será tan fácil retirar el consentimiento como darlo".

PROYECTO DE LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

El PLOPD recoge, asimismo, algunas disposiciones que, directa o indirectamente, pueden afectar al consentimiento.

Así, **la disposición adicional décima ("Potestad de verificación de las Administraciones Públicas")** recoge lo siguiente:

"Cuando se formulen solicitudes por medios electrónicos en las que el interesado declare datos personales que obren en poder de las Administraciones Públicas, el órgano destinatario de la solicitud podrá efectuar en el ejercicio de sus competencias las verificaciones necesarias para comprobar la exactitud de los datos".

Por su parte, en **la "disposición adicional decimotercera ("Comunicaciones de datos por los sujetos enumerados en el artículo 77.1")**, parece advertirse un debilitamiento de las exigencias del consentimiento según el RGPD cuando actúan entidades del sector público en determinadas circunstancias:

"Los responsables enumerados en el artículo 77.1 de esta Ley orgánica podrán comunicar los datos de carácter personal que les sean solicitados por sujetos de derecho privado cuando cuenten con el consentimiento de los afectados o aprecien que concurre en los solicitantes un interés legítimo que prevalezca sobre los derechos o intereses de los afectados conforme a lo establecido en el artículo 6 1 f) del Reglamento (UE) 2016/679".

Y, finalmente, **la disposición transitoria sexta ("Consentimientos otorgados con anterioridad a la aplicación del Reglamento (UE) 2016/679")**, expone:

"Cuando el tratamiento se base en un consentimiento otorgado con anterioridad a la aplicación del Reglamento (UE) 2016/679, no será necesario recabar nuevamente dicho consentimiento si la forma en que se otorgó se ajusta a las condiciones del Reglamento (UE) 2016/679".

UNA POSIBLE APLICACIÓN:

Por parte de alguna opinión doctrinal se ha puesto de relieve que el inciso segundo del apartado 2 del artículo 28 de la Ley 39/2015, de 1 de octubre, quedaría desplazado por el RGPD cuando afirma que "se presumirá que la consulta u obtención es autorizada por los interesados salvo que conste en el procedimiento su oposición expresa o la ley especial aplicable requiera consentimiento expreso". El problema, ciertamente, radica en que en este caso se prevé un consentimiento tácito o presunto que no se adecua, en principio, a las exigencias del RGPD.

Ver: Concepción Campos Acuña, "Los 7 imprescindibles en protección de datos para el ámbito local", El Consultor de los Ayuntamientos y Juzgados, enero 2018 https://bit.ly/2EftpAb

Cabe considerar que si prospera la actual redacción de la DA 10 del PLOPD, las Administraciones Públicas tendrán la potestad de verificar en todo caso, y sin necesidad de consentimiento, los datos que los usuarios manifiesten en las solicitudes mediante una declaración responsable. Esto supone una mejora considerable en la aplicación práctica de la simplificación de procedimientos y cumplimiento normativo de no pedir datos ni documentos a la ciudadanía que ya obren en poder de otras Administraciones Públicas. Otra cosa es que, obviamente, se requiere informar debidamente a la ciudadanía (en los términos recogidos en el RGPD) de este hecho. Habrá que esperar a cómo queda esta materia definitivamente regulada en la futura LOPD y cómo se cohonestan las previsiones del RGPD con esa finalidad de simplificación administrativa.

En todo caso, **la tesis de la AEPD es que la redacción actual del artículo 28.2 de la Ley 39/2015, podría encontrar fundamento en el artículo 6.1 e) RGPD, en concreto** "cuando el tratamiento sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento" (Ver: *Protección de Datos y Administración Local,* p. 13).

En el caso de la interoperabilidad de los registros electrónicos de las Administraciones públicas, el tratamiento podría ampararse en el cumplimiento de una obligación legal aplicable al responsable del tratamiento o, asimismo, en que ese tratamiento es necesario para el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6, 1 c) o 6,1 e) RGPD)

Los tratamientos de "categorías especiales"

En los Considerandos se hace alguna mención específica a la noción "datos sensibles", pero el RGPD en su artículo 9 se refiere a la noción de "categorías especiales de datos personales", en los siguientes términos:

Categorías especiales de datos personales:

9.1 RGPD: "Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física".

PARA SABER MÁS:

En el tratamiento de categorías especiales de datos y las excepciones aplicables a la Administración Local, ver: AEDP, *Protección de Datos y Administración Local*, p. 14

¿Qué derechos garantiza el RGPD al "interesado" o "afectado"?

El RGPD contiene una nueva regulación de los derechos de las personas en materia de protección de datos. Los viejos derechos ARCO se mantienen o se modulan, pero se incorporan otros con perfiles nuevos, especialmente como se verá a continuación el derecho de información a los afectados.

Esta importante regulación está recogida en el Capítulo III ("Derechos del interesado"), artículos 12 a 22. El PLOPD también prevé una regulación de tales derechos, pero salvo en los que afectan a la transparencia e información al afectado (artículo 11), derecho de acceso (artículo 13) y derecho de rectificación (artículo 14), que completan lo previsto en el Reglamento, en lo demás se lleva a cabo un simple reenvío a lo establecido en el RGPD.

Por tanto, teniendo en cuenta los fines del RGPD, las Administraciones Locales en los procesos de tratamiento de datos tienen que adoptar medidas de carácter técnico, organizativo y de seguridad encaminadas a no afectar a ninguno de los derechos allí recogidos.

El dato siempre es de la persona, la gestión del dato cuando la ejerce una autoridad u organismo público es administrativa, pero enmarcada en el conjunto de principios, limitaciones y derechos establecidos por el RGPD.

DERECHOS DEL INTERESADO O AFECTADO:

- Transparencia de la información (artículos 12-13-14)
- Derecho de acceso (artículo 14)
- Derecho de rectificación (artículo 16)
- Derecho de supresión o "derecho al olvido" (artículo 17)
- Derecho a la limitación del tratamiento (artículo 18)
- Derecho a la portabilidad de los datos (artículo 20)
- Derecho de oposición y a no ser objeto de decisiones individuales automatizadas (artículos 21-22)

SI ES USTED CIUDADANO, CONOZCA SUS NUEVOS DERECHOS EN RELACIÓN CON LOS DATOS

NUEVOS DERECHOS	ARTÍCULOS RGPD
Derecho a recibir información clara y comprensible	(Artículos 12-14)
Derecho a solicitar acceso a los datos personales que una organización tenga sobre usted	(Artículo 15)
Derecho a solicitar a un proveedor de servicios que transmita sus datos personales a otro o se los provea	(Artículo 20)
Derecho al olvido	(Artículo 17)
Consentimiento expreso (Ya no caben extensas condiciones jurídicas que usted nunca lee)	(Artículos 4.11 y 7)
Si sus datos se pierden o son robados: Derecho a ser informado sin dilación indebida	(Artículos 33-34)
Mayor protección en línea para los menores	(Artículo 8)

[Fuente: Comisión Europea, enero 2018 (data protection-factsheet-citizens_es)]

IDEA-FUERZA SOBRE LOS DERECHOS EN EL RGPD:

- **Fortalecimiento de los derechos de las personas**: el Reglamento introduce nuevos requisitos de transparencia; derechos reforzados de información, acceso y eliminación («derecho al olvido»); el silencio o la falta de actividad dejarán de considerarse como un consentimiento válido, ya que se requiere una clara acción afirmativa para expresar dicho consentimiento; y la protección de los niños en línea. *(Fuente: Comunicación de la Comisión al Parlamento. Europeo y al Consejo. Mayor protección, nuevas oportunidades: Orientaciones de la Comisión sobre la aplicación directa del Reglamento general de protección de datos a partir del 25 de mayo de 2018 Bruselas 20-1-2018 COM (2018) 43 final)*

¿Cuál es el nuevo marco normativo de la información y cómo afecta a las entidades locales?

Bajo el enunciado de "Transparencia y modalidades", los artículos 12 a 14 del RGPD contienen una nueva regulación de la información y de las comunicaciones que se debe proveer a las personas físicas cuando se traten sus datos. Un desarrollo de tales previsiones se recoge en el artículo 11 del PLOPD.

El RGPD prevé, así, **la transparencia como principio** (que debe ser especialmente tenido en cuenta por la Administración Pública en el ejercicio de sus funciones de tratamiento de datos) **y como derecho de las personas físicas en relación con sus datos de carácter personal**.

Las novedades más significativas de este nuevo marco normativo van encaminadas a reforzar notablemente la obligación de información en todo proceso de tratamiento de datos, lo que obligará a las Administraciones Locales a tener en cuenta estas nuevas exigencias.

Algunos rasgos de este derecho a ser informado son:

- El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda la información relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.

- El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos y asimismo le proveerá de la información relativa a su solicitud en el plazo de un mes o, excepcionalmente, en dos cuando se invoque complejidad o un número elevado de solicitudes. Si no da curso a su solicitud, la información será realizada sin dilación o como máximo en un mes, con una posible prórroga de dos meses.

- La información solicitada será gratuita, salvo excepciones tasadas (artículo 12.5)

- Entre la información que se debe facilitar cuando los datos se obtengan del interesado, se encuentra la siguiente:

  - Identidad y datos de contacto del responsable
  - Los datos de contacto del delegado de protección de datos
  - Los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento
  - El plazo en el que se conservarán los datos personales
  - La existencia del derecho a solicitar del responsable del tratamiento el acceso a los datos personales, su rectificación o supresión, la limitación del tratamiento, la oposición o la portabilidad de los datos.

- Cuando los datos no se hayan obtenido del interesado a la información anterior se le añade, "la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público".

Las autoridades de control de protección de datos han elaborado conjuntamente una *Guia per al cumpliment del deure d'informar a l'RGPD*, que puede consultarse en su versión en lengua catalana en: http://apdcat.gencat.cat/ca/documentacio/RGPD/altres_documents_dinteres/

¿QUÉ CAMBIA EL RGPD SOBRE EL DEBER DE INFORMACIÓN EJERCIDO POR LAS ADMINISTRACIONES PÚBLICAS?

Información que cabe facilitar actualmente (LO 15/1999)	**NUEVO: Información adicional que se debe añadir por aplicación del RGPD**
La existencia del fichero o tratamiento	Los datos de contacto del delegado de protección de datos
El carácter obligatorio o no de la respuesta, así como sus consecuencias	La base jurídica o legitimación del tratamiento
La posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición	La previsión de transferencias a terceros países y la existencia de una decisión de adecuación o de garantías adecuadas y los medios para obtener una copia
La identidad y los datos de contacto del responsable de tratamiento	El plazo o los criterios de conservación de la información
	El derecho a solicitar la limitación del tratamiento y la portabilidad de los datos
	(*) El artículo 14.2 b) no se aplica a las autoridades y organismos públicos

RECOMENDACIÓN DE LAS AUTORIDADES DE CONTROL SOBRE LAS OBLIGACIONES DE INFORMACIÓN DEL RGPD:

"En consecuencia, los procedimientos, modelos o formularios diseñados de conformidad con la LOPD se han de revisar y adaptar antes de la fecha de plena aplicación del RGPD, para incorporar allí los nuevos requisitos"

"Se recomienda revisar y aplicar esta adaptación sin que quepa esperar a la fecha de plena aplicación del RGPD"

INFORMACIÓN POR CAPAS:

Es preciso delimitar el derecho a la información en una **"información por capas"**, información básica (primer nivel) y una información adicional (segundo nivel):

Presentar información básica en un 1r nivel:

• de forma resumida,

• en el mismo momento y

• en el mismo medio de recogida

Remitir a información adicional en un 2º nivel:

• de forma detallada,

• en un medio más adecuado para su presentación, comprensión y archivo

RECOMENDACIÓN AEDP: TRACTAMENT PER CAPES

En lo que afecta al "Cumplimiento del principio de transparencia: derecho a la información en la recogida de datos personales, con la finalidad de facilitar ese cumplimiento la AEPD recomienda adoptar un modelo de información por capas o niveles. Una buena información sobre cómo llevar a cabo ese tratamiento por capas se recoge en el Cuadro de la página 28 del documento *Protección de Datos y Administración Local*. Ver cuadro en la página siguiente

EJEMPLO TRATAMIENTO POR CAPAS (AEPD, *Guía de Protección de Datos y Administración Local*, abril 2018)

EPÍGRAFE	INFORMACIÓN BÁSICA (1ª Capa resumida)	INFORMACIÓN ADICIONAL (2ª Capa detallada)
Responsable del tratamiento	Identidad del responsable del tratamiento	1.- Datos de contacto 2.- Identidad/Datos contacto representante 3.- Datos contacto DPD
Finalidad del tratamiento	Descripción sencilla de los fines del tratamiento, incluso elaboración perfiles	1.- Descripción ampliada fines del tratamiento 2.- Plazos y criterios de conservación de los datos 3.- Decisiones automatizadas, perfiles y lógicas ampliadas
Legitimación del tratamiento	Base jurídica del tratamiento	1.- Detalle base jurídica, en los casos de obligación legal, interés público o interés legítimo 2.- Obligación o no de facilitar datos y consecuencias de no hacerlo
Destinatarios de cesiones o transferencias	Previsión o no de cesiones Previsión de transferencias o no a terceros países	Destinatarios o categorías de destinatarios Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables
Derechos de las personas interesadas (o afectadas)	Referencia al ejercicio de derechos	1.- Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición de su tratamiento 2.- Derecho a retirar el consentimiento prestado 3.- Derecho a reclamar ante la autoridad de control
Procedencia de los datos	Fuentes de los datos cuando no proceden del interesado (o afectado)	1.- Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público. 2.- Categorías de datos que se traten

Derecho de acceso

El derecho de acceso del interesado se manifiesta en el derecho a obtener del responsable del tratamiento confirmación de si se están tratando datos personales, así como en tal caso el derecho de acceso a los datos y a la información recogida en el artículo 15.1 RGPD.

ACLARACIÓN SOBRE EL DERECHO DE ACCESO RGPD:

"Debe distinguirse del derecho de acceso de los interesados a los expedientes administrativos que regula la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, así como del derecho de acceso regulado en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno" [así como del mismo derecho de acceso a la información pública regulado en la Ley 19/2014, de 29 de diciembre, del Parlament de Catalunya, sobre transparencia, acceso a la información pública y buen gobierno"]

Guía para la adaptación del Reglamento General de Protección de Datos de las Administraciones Locales, FEMP, p. 24

Derecho de rectificación y supresión ("Derecho al olvido")

El interesado tiene derecho a pedir la **rectificación** de los datos personales inexactos o que no sean veraces, así como a que se completen los datos personales que estén incompletos. Esta rectificación la llevará a cabo el responsable del tratamiento, y no podrá sufrir dilaciones indebidas.

No hay novedades relevantes en lo que afecta a la rectificación de los datos, pero sí al denominado **derecho al olvido o la supresión de datos personales**, que es, sin duda, uno de los elementos nuevos de la regulación.

El responsable del tratamiento está obligado a suprimir los datos personales siempre que concurran alguna de las circunstancias establecidas en el artículo 17.1 RGPD.

En efecto, el RGPD ha sumado el "**derecho al olvido**" o derecho de supresión a los clásicos derechos ARCO -acceso, rectificación, cancelación y oposición- , que no es otra cosa que "un derecho de cancelación actualizado". Tanto el considerando 65 como el artículo 17 del RGPD exponen que los interesados tienen derecho al olvido si la retención de sus datos impide lo dispuesto por el propio RGPD o por la normativa del Estado miembro. Asimismo, afirma que los interesados "deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos" o "si los interesados han retirado su consentimiento" o si se oponen al tratamiento. También indica que deberán ser suprimidos los datos personales tratados ilícitamente.

Si los datos se hacen públicos, el responsable de tratamiento deberá adoptar medidas razonables para informar a los responsables que estén tratando dichos datos, así como para suprimir cualquier enlace, copia, o réplica de los mismos, teniendo en cuenta la tecnología disponible y el coste de su aplicación.

Derecho a la limitación del tratamiento

Asimismo, el RGPD recoge expresamente el derecho a la limitación del tratamiento (artículo 18), siempre que no concurra alguna causa legalmente prevista. Ese derecho no es absoluto, y se podrá llevar a cabo cuando se dé alguna de las siguientes condiciones:

- Se podrá limitar el tratamiento de los datos del interesado cuando este haya impugnado su exactitud, durante el plazo que el responsable los verifique.
- Si el tratamiento es ilícito, el interesado podrá pedir la limitación del uso de los datos en vez de su supresión.
- Cuando el responsable ya no necesite hacer uso de esos datos, pero el interesado los necesite para interponer o defender reclamaciones.
- Cuando el interesado se haya opuesto al tratamiento de sus datos por motivos relacionados con su situación particular, mientras se verifica si los motivos han de tenerse en cuenta.

Derecho a la portabilidad de los datos

El derecho a la **portabilidad de los datos** supone el "derecho del interesado a recibir su información en un formato estructurado y de uso común, para su trasmisión a otro responsable o, incluso la obligación del anterior responsable de hacerlo directamente", esto último será posible cuando sea técnicamente viable.

- **Mayor control sobre los datos personales para los particulares.** El Reglamento establece un **nuevo derecho a la portabilidad de los datos** que permite a los ciudadanos solicitar que una empresa u organización le devuelva los datos personales que le facilitó por consentimiento o contrato; también permitirá que dichos datos personales se transmitan directamente a otra empresa u organización, cuando sea técnicamente posible. *(Fuente: Comunicación de la Comisión al Parlamento. Europeo y al Consejo. Mayor protección, nuevas oportunidades: Orientaciones de la Comisión sobre la aplicación directa del Reglamento general de protección de datos a partir del 25 de mayo de 2018 Bruselas 20-1-2018 COM (2018) 43 final)*

Esquema de Ideas-Fuerza:

- El artículo 20 RGPD crea un nuevo derecho a la portabilidad de los datos estrechamente relacionado con el derecho de acceso aunque diferente de este en muchos aspectos.
- El propósito de este nuevo derecho es capacitar al interesado y darle más control sobre los datos personales que le conciernen.
- El derecho a la portabilidad de los datos es también una herramienta importante que respaldará la libre circulación de datos personales en la UE y facilitará el cambio entre distintos proveedores de servicios y, por tanto, promoverá el desarrollo de nuevos servicios en el contexto de la estrategia para el mercado digital.
- Una práctica recomendable es que los responsables del tratamiento comiencen a desarrollar los medios que contribuyan a responder a las solicitudes de portabilidad.

PARA SABER MÁS:

Grupo de Trabajo sobre Protección de Datos del Artículo 29: Directrices sobre el derecho a la portabilidad de los datos, 16/ES, WP 242 rev. 01 (Adoptadas el 13

de diciembre de 2016. Revisadas por última vez y adoptadas el 5 de abril de 2017)

http://apdcat.gencat.cat/ca/documentacio/RGPD/altres_documents_dinteres/altres_documents_del_grup_de_larticle_29/

Derecho de oposición y decisiones individuales automatizadas

El interesado podrá, siempre que no concurra alguna de las excepciones previstas en el Reglamento, **oponerse** a que sus datos sean objeto de tratamiento. Esta oposición se podrá presentar en cualquier momento, y se podrá basar en motivos relacionados con la situación particular del interesado. Si se presenta la oposición, el responsable del tratamiento deberá dejar de tratar los datos personales.

Limitaciones

Los derechos mencionados no son absolutos, sino que se pueden encontrar limitados por varios factores.

Es el responsable o el encargado del tratamiento, **a través de medidas legislativas,** el que puede limitar dichos derechos, siempre y cuando las medidas adoptadas sean necesarias y proporcionadas y respete lo previsto en la normativa para ello, asimismo la limitación deberá siempre respetar en lo esencial los derechos y libertades fundamentales.

El artículo 23 del RGPD dispone los casos en los que se acepta la limitación de los derechos del interesado, atendiendo, siempre, a la necesidad de salvaguardar, entre otros, la defensa, la prevención, investigación o enjuiciamiento de infracciones penales, la seguridad pública, la protección del interesado o de los derechos y libertades de otros.

3. NUEVO SISTEMA INSTITUCIONAL Y DE GESTIÓN DE PROTECCIÓN DE DATOS EN LA ADMINISTRACIÓN PÚBLICA

Introducción

El nuevo modelo de Protección de Datos que se prevé en el RGPD se asienta sobre la **responsabilidad proactiva**, lo que tiene especiales consecuencias a la hora de articular el sistema institucional y de gestión de protección de datos en las Administraciones locales.

Se pone, por tanto, el acento en el análisis de riesgos y en la evaluación de impacto que conlleva determinados tratamientos de datos personales; es decir, **el foco se sitúa en la anticipación y en la prevención, una suerte de garantía y aplicación de la política de cumplimiento (*compliance*) también en las organizaciones públicas**.

Ni que decir tiene que **este enfoque de riesgos y preventivo implica un cambio de cultura organizativa frontal en lo que al tratamiento de datos respecta.** Al menos impone una forma distinta de trabajar en todos los procesos, procedimientos y proyectos que impliquen tratar datos de forma masiva, que entrañen alto riesgo y aquellos otros que se encuadran en "categorías especiales" (datos sensibles).

Y es aquí donde se hallan los principales problemas para transitar correctamente de un modelo de protección de datos "reactivo" a otro "proactivo". La formación se torna ineludible y las políticas de sensibilización que deben llevar a cabo las autoridades de control (apdCAT/AEPD/AVPD), junto con las administraciones públicas, son una herramienta o palanca de cambio o transformación imprescindible para ir introduciendo paulatinamente la **nueva cultura de gestión en la protección de datos personales.**

El tránsito será lento, también en el sector público. Se ha comenzado tarde y habrá que ajustar paulatinamente los distintos elementos de esa nueva arquitectura institucional y de gestión que deberá funcionar en un plazo razonable de forma armónica, sobre todo si se quiere que los datos personales y los derechos fundamentales de las personas físicas no sufran menoscabo alguno.

De hecho, ese nuevo sistema de gestión debiera estar ya listo para funcionar con anterioridad al 25 de mayo de 2018, pero su puesta en marcha en el sector público se dilatará en el tiempo, al menos en algunos casos. En cualquier caso, no hay excusa, puesto que el RGPD se aprobó con un largo periodo que difería su aplicabilidad precisamente para garantizar su efectividad y llevar a cabo tal proceso de adaptación.

Y, para articular razonablemente, las diferentes piezas que gravitan en torno a la construcción de ese nuevo modelo institucional y de gestión de la protección de datos personales en el sector público, se deben tener presentes, aparte de los principios y derechos antes recogidos, una serie de elementos organizativos e institucionales que tienden a configurar un nuevo **Sistema de Gestión de la Protección de Datos en el Sector Público que se configura de los siguientes elementos básicos**:

Elementos básicos del sistema de gestión de protección de datos	*Ubicación sistemática en el RGPD*
Responsables/ Encargados del tratamiento	Capítulo IV RGPD (artículos 24-29)
Registro de las Actividades de tratamiento	Artículo 30 RGPD
Seguridad de los datos personales	Artículos 32-34 RGPD
Análisis de Riesgos	Proceso previo, en su caso, a la evaluación de impacto
Evaluación de impacto relativa a la protección de datos	Artículos 35-36
Delegado de protección de datos	Artículos 37-39
Códigos de conducta	Artículos 40-41
Mecanismos de certificación	Artículos 42-43
Autoridades de Control (AEPD/ACPD)	Artículos 51-59 (especialmente) Título VII PLOPD
Régimen de sanciones	Capítulo VIII RGPD Título IX PLOPD

El objeto, por tanto, de esta tercera parte de la Guía no es otro que analizar brevemente y de forma descriptiva estos elementos que configuran la arquitectura básica del Sistema Institucional y de Gestión de la Protección de Datos en las organizaciones públicas, con la finalidad de que este análisis sirva como medio de activar la puesta en marcha de todas esas piezas de este complejo engranaje a la mayor brevedad por parte de las Administraciones locales y de sus entidades del sector público institucional.

Responsables de tratamiento y encargados de tratamiento: sus peculiaridades aplicativas en el ámbito del gobierno local.

Responsable de tratamiento

El Considerando 78 RGPD comienza del siguiente modo: "La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento".

La puesta en marcha de esas medidas técnicas y organizativas apropiadas es una responsabilidad de una figura clave en el modelo de protección de datos, también en el sector público: el responsable del tratamiento. Junto a esta figura también se encuentra otra que es la del "encargado del tratamiento", ambas deben estar en condiciones de cumplir sus obligaciones en materia de protección de datos. Y, además, implantar los principios de protección de datos desde el diseño y por defecto, tal como se verá.

Dos Considerandos son importantes en esta materia. Y conviene reproducirlos para poder extraer sus consecuencias efectivas:

CONSIDERANDO 79:

"***La protección de los derechos y libertades de los interesados, así como la responsabilidad de los responsables y encargados del tratamiento***, también en lo que respecta a la supervisión por parte de las autoridades de control y a las medidas adoptadas por ellas, ***requieren una atribución clara de las responsabilidades en virtud del presente Reglamento***, incluidos los casos en los que un responsable determine los fines y medios del tratamiento de forma conjunta con otros responsables, o en los que el tratamiento se lleve a cabo por cuenta de un responsable".

CONSIDERANDO 81:

"**Para garantizar el cumplimiento de las disposiciones del presente Reglamento respecto del tratamiento que lleve a cabo el encargado por cuenta del responsable, este, al encomendar actividades de tratamiento a un encargado, debe recurrir únicamente a encargados que ofrezcan suficientes garantías**, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento. La adhesión del encargado a un código de conducta aprobado o a un mecanismo de certificación aprobado puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable. **El tratamiento por un encargado debe regirse por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros que vincule al encargado con el responsable**, que fije el objeto y la duración del tratamiento, la naturaleza y fines del tratamiento, el tipo de datos personales y las categorías de interesados, habida cuenta de las funciones y responsabilidades específicas del encargado en el contexto del tratamiento que ha de llevarse a cabo y del riesgo para los derechos y libertades del interesado (…) Una vez finalizado el tratamiento por cuenta del responsable, el encargado debe, a elección de aquel, devolver o suprimir los datos personales, salvo que el Derecho de la Unión o de los Estados miembros aplicable al encargado del tratamiento obligue a conservar los datos."

La figura del responsable de tratamiento viene definida en el artículo 4.7 RGPD en los siguientes términos:

"'RESPONSABLE DE TRATAMIENTO' O 'RESPONSABLE': La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros determine los fines y medios del tratamiento (…)"

La regulación específica de la figura del responsable de tratamiento se halla en los artículos 24 a 27 RGPD, si bien el Reglamento está plagado de referencias permanentes a esta figura, que se transforma así en pieza clave para garantizar el perfecto cumplimiento de las obligaciones derivadas de la norma europea o del Derecho interno de los Estados miembros, así como en garante último de que se adoptarán las medidas técnicas y organizativas apropiadas para su adecuación a tal normativa.

Esta idea se refleja perfectamente en el artículo 24 RGPD, cuyo apartado 1 expone, por ejemplo, lo siguiente:

"Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario."

Tal como expresa el artículo 24.3 RGPD la adhesión a códigos de conducta o mecanismos de certificación "podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento".

El artículo 25 RGPD, por su parte, recoge una de las ideas sustantivas del nuevo modelo centrado específicamente en la gestión de riesgos, algo que se tratará en el epígrafe de esta guía relativo al Análisis de Riesgos, pero conviene reproducir, por su importancia implícita, los apartados 1 y 2 del citado precepto. Como puede advertirse la protección de datos desde el diseño y por defecto es responsabilidad exclusiva del propio responsable del tratamiento, que deberá asimismo aplicar las medidas técnicas y organizativas apropiadas teniendo en cuenta lo establecido en el primer inciso de ese mismo precepto.

ARTÍCULO 25.1 Y 2 RGPD: PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento***, medidas técnicas y organizativas apropiadas***, como la seudonimización, concebidas ***para*** aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y ***proteger los derechos de los interesados.***

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

El artículo 26 regula la figura del corresponsable y el régimen aplicable.

El PLOPD establece una minuciosa regulación en su Título V del responsable y encargado del tratamiento. Sin perjuicio de cómo quede finalmente esa regulación en el texto que definitivamente se apruebe, algunos de los puntos que allí se tratan en relación con el papel del responsable son los siguientes:

- Con el fin de concretar las medidas técnicas y organizativas que los responsables y encargados han de adoptar, se determinan una serie de supuestos en los que se podrían producir "mayores riesgos", lo que puede ayudar a definir en qué casos se pueden adoptar tales medidas (artículo 28.2 PLOPD)

- El artículo 31 PLOPD regula el registro de actividades de tratamiento y, entre otras cosas, la necesidad de comunicar por parte del responsable o del encargado del tratamiento al delegado de protección de datos "cualquier adición, modificación o exclusión del contenido del registro"

- También en este mismo artículo 31.2 PLOPD se establece la obligación de que las Administraciones Locales y sus entidades del sector público (recogidas en el ámbito de aplicación del artículo 77.1 PLOPD) hagan público un inventario de actividades de tratamiento.

- Se establece la obligación del responsable del tratamiento de "bloquear los datos cuando proceda a su rectificación o supresión", la determinación de a disposición de qué autoridad quedan tales datos, así como que "los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior" (artículo 32, 1 a 3). El apartado 4 prevé un régimen de excepciones que pueden definirse por las autoridades de control en los términos allí previstos.

En el ámbito local de gobierno la figura del responsable de tratamiento será el alcalde o alcaldesa, salvo que tal atribución haya podido ser delegada en un miembro de su equipo de Gobierno o, asimismo, en la persona titular de un órgano directivo en los municipios de gran población. En el municipio de régimen especial de Barcelona, estas responsabilidades podrían ser asimismo delegadas en la estructura gerencial o directiva.

UNA PROPUESTA:

En todo caso, atendiendo a la importancia estratégica o nuclear que tiene la figura del responsable en la aplicación efectiva del nuevo modelo de gestión del RGPD, cabría plantearse la oportunidad de elaborar, al menos en determinadas entidades locales de ciertas dimensiones, un reglamento municipal o provincial de protección de datos que, con un evidente carácter organizativo, determinara no solo el papel del responsable o responsables en la estructura municipal en materia de protección de datos, sino también sus relaciones con la figura del encargado o encargados de tratamiento, así como en relación con el delegado de protección de datos (y la definición concreta de esa figura en la organización), pudiendo igualmente regular otros aspectos específicos de tal materia (seguridad, registro de actividades, análisis de riesgos, evaluación de impacto, etc.).

También cabría plantearse si toda esta información y la organización no se pueden seguir reflejando en el documento de seguridad, dado que se podría considerar vigente en cuanto que no contradice lo previsto en el RGPD. En cualquier caso, el cambio de paradigma es tan profundo (al menos en sus finalidades y arquitectura institucional) que tal vez requiera plantearse (siquiera sea como mera hipótesis) un reflejo normativo, como antes se indicaba.

PARA SABER MÁS

Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento, AEPC, apdCAT, AVPD, 2018.

http://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf

Encargado de protección de datos

Ya se ha visto cómo el Considerando 97 delimita a rasgos generales cuál es el papel y perfil que debe tener esta figura. Su regulación en el RGPD se encuentra recogida en los artículo 28 y 29, principalmente en el primero que resulta fundamental para concretar los criterios generales expuestos en el Considerando 97 sobre cuál es el régimen aplicable a la figura del encargado de tratamiento.

Dada la finalidad del RGPD de protección de los datos de carácter personal y, concretamente, de los derechos fundamentales de las personas físicas que se puedan ver afectados por tales datos, la norma europea introduce algunas novedades importantes en la regulación del encargado del tratamiento, con el objetivo de apuntalar el cumplimiento estricto del propio Reglamento, puesto que en las Administraciones Locales tales datos en unas ocasiones serán tratados por encargados "internos", pero en no pocas de ellas por encargados "externos", mediante procedimientos de contratación pública, encomiendas de gestión, convenios u otros instrumentos jurídicos.

De ahí que la regulación de esta figura se prevea con cierto detalle. Y de ahí también cómo las autoridades de control (AEPD/apdCAT/AVPD) han elaborado, según se verá de inmediato, un documento de notable interés sobre el encargado del tratamiento y, asimismo, sobre el papel del responsable de tratamiento en relación con aquel.

PARA SABER MÁS:

"Directrices para la elaboración de contratos entre responsables y encargados de tratamiento".

La versión en catalán de este documento ha sido difundida por la ACPD con el título *Guia sobre l'encarregat del tractament al RGPD*; http://apdcat.gencat.cat/ca/documentacio/RGPD/altres_documents_dinteres/guia_sobre_lencarregat_del_tractament_al_rgpd/

La regulación sustantiva de esa figura se lleva a cabo en el artículo 28 RGPD, del que se pueden destacar los siguientes aspectos:

- El apartado 1 expone lo siguiente: "Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, éste **elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas**, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado."

- En el apartado 2 se regula que el encargado del tratamiento no podrá recurrir a otro encargado sin la autorización previa por escrito, específica o general, del responsable. Debiendo informar de todo cambio.

- **El tratamiento por el encargado se regirá por un contrato o acto jurídico,** que deberá estipular, en particular, una serie de exigencias que se detallan en el artículo 28.3 RGPD.

- Cuando un encargado recurra a otro para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se le impondrán, también por contrato o acto jurídico, las mismas obligaciones de protección de datos estipuladas en el contrato o acto jurídico existentes entre el responsable y encargado principal (artículo 28.4)

- La adhesión a códigos de conducta o mecanismos de certificación podrá utilizarse como elemento para demostrar que se cumplen las garantías establecidas en este artículo 28.1 a 4.

- Se prevé una referencia a las cláusulas contractuales tipo y a la facultad de adoptarlas por la Comisión o por la autoridad de control.

- Se contiene asimismo la exigencia de que el contrato u otro acto jurídico sea siempre por escrito (formato electrónico, actualmente).

- Y, finalmente, se incorpora una importante cláusula de desplazamiento de la responsabilidad en determinados supuestos (artículo 28.10).

El PLOPD contiene en su artículo 33 una regulación de la figura del encargado del tratamiento, cuyas notas más relevantes, sin perjuicio de cómo quede finalmente en el texto de la Ley Orgánica que se apruebe, son las siguientes:

- El acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos, si se cumple lo establecido en la normativa de aplicación.

- Tendrá la consideración de responsable del tratamiento y no la de encargado quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 RGPD. Se exceptúan de esta regla los encargos efectuados en el marco de la legislación de contratación del sector público.

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

- El responsable del tratamiento determinará si, cuando finalice la prestación de los servicios del encargado, los datos de carácter personal deben ser destruidos, devueltos al responsable o entregados, en su caso, a un nuevo encargado. Se establece alguna excepción.

- El encargado del tratamiento podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

- **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 Reglamento (UE) 2016/679.

DISPOSICIÓN TRANSITORIA QUINTA PLOPD. CONTRATOS DE ENCARGADOS DEL TRATAMIENTO

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 transcurridos cuatro años desde la citada fecha.

En caso de que los contratos previesen su prórroga al término de su vencimiento, ya fuera por mutuo acuerdo entre las partes o en ausencia de denuncia por cualquiera de ellas, deberá producirse su adaptación con anterioridad al momento en que estuviera prevista dicha prórroga.

Y, finalmente, para tener una idea más cabal del papel y de las novedades que implica la figura del encargado del tratamiento, así como de sus relaciones con el responsable del tratamiento, debe consultarse el importante Documento de Directrices para la elaboración de contratos entre responsables y encargados del tratamiento, editado en catalán por la apdCAT con el título ya indicado, que es el que se utilizará como referencia en este texto.

IDEAS-FUERZA de la "Guía sobre el encargado del tratamiento en el RGPD"; http://apdcat.gencat.cat/ca/documentacio/RGPD/altres_documents_dinteres/guia_sobre_lencarregat_del_tractament_al_rgpd/

¿QUÉ ES UN ENCARGADO DEL TRATAMIENTO Y CUÁL ES SU FUNCIÓN PRINCIPAL?

- El encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u organismo que presta al responsable un servicio que conlleva el tratamiento de datos personales por cuenta de éste.
- Aunque la definición puede parecer clara, en la práctica se dan multitud de situaciones en las que puede ser difícil delimitar cuándo nos encontramos ante un encargado y en qué casos ante un responsable del tratamiento. Para facilitar esta distinción, debemos tener en cuenta que corresponde al responsable decidir sobre la finalidad y los usos de la información, mientras que el encargado del tratamiento debe cumplir las instrucciones de quien le encomienda un determinado servicio, en relación con el tratamiento de los datos personales a los que tiene acceso como consecuencia de la prestación de este servicio.

¿QUÉ NIVEL DE DECISIÓN PUEDE ASUMIR UN ENCARGADO DEL TRATAMIENTO?

- El encargado del tratamiento puede adoptar cualquier decisión organizativa y operacional necesaria para prestar el servicio que tiene contratado. En ningún caso puede variar los fines y los usos de los datos, ni puede utilizarlas para sus propias finalidades.
- Las decisiones que adopta deben respetar las instrucciones del responsable del tratamiento.

¿EL RESPONSABLE DEL TRATAMIENTO PUEDE ELEGIR CUALQUIER ENCARGADO DEL TRATAMIENTO?

- El responsable del tratamiento debe elegir un encargado del tratamiento que ofrezca garantías suficientes respecto de la implantación y el mantenimiento de las medidas técnicas y organizativas apropiadas, de acuerdo con lo establecido en el RGPD, y que garantice la protección de los derechos de las personas afectadas. Por lo tanto, hay un deber de diligencia a la hora de escoger el encargado.

¿CÓMO REGULAR LAS RELACIONES ENTRE EL RESPONSABLE Y EL ENCARGADO DEL TRATAMIENTO?

- - La regulación de la relación entre el responsable y el encargado del tratamiento debe establecerse a través de un contrato o de un acto jurídico similar que los vincule. El contrato o acto jurídico debe constar por escrito, incluido en formato electrónico.
- La posibilidad de regular esta relación a través de un acto jurídico unilateral del responsable del tratamiento es una de las novedades previstas en el RGPD. En cualquier caso, debe ser un acto jurídico que establezca y defina la posición del encargado del tratamiento, siempre que dicho acto vincule jurídicamente el encargado del tratamiento. Este sería el caso, por ejemplo, de una resolución administrativa que conste notificada al encargado del tratamiento.

QUIÉN ES RESPONSABLE DE LOS TRATAMIENTOS REALIZADOS POR EL ENCARGADO DEL TRATAMIENTO?

- El responsable del tratamiento no pierde esta consideración ningún caso. Por lo tanto, sigue siendo responsable de que los datos personales se traten correctamente y de la garantía de los derechos de las personas afectadas.
- El responsable tiene una obligación de especial diligencia en la elección y la supervisión del encargado

SI SE EXTERNALIZAN LAS FUNCIONES DEL DELEGADO DE PROTECCIÓN DE DATOS A UN TERCERO, ESTE TIENE LA CONSIDERACION DE ENCARGADO DEL TRATAMIENTO?

- Sí, el RGPD prevé que el delegado de protección de datos debe poder acceder a los datos que se traten. Por lo tanto, se deberá formalizar un encargo del tratamiento.

¿CUAL ES EL CONTENIDO MÍNIMO DE UN ACUERDO O ACTO DE ENCARGO DEL TRATAMIENTO? (VER LA DESCRIPCIÓN DE CADA PUNTO EN LA GUÍA)

- Las instrucciones del responsable del tratamiento.
- El deber de confidencialidad
- Las medidas de seguridad
- El régimen de la subcontratación
- Los derechos de los interesados
- Colaboración en el cumplimiento de las obligaciones del responsable
- El destino de los datos al finalizar la prestación
- La colaboraciones para demostrar el cumplimiento

ENCARGADO DE TRATAMIENTO: EJEMPLOS CUANDO UN AYUNTAMIENTO ENCARGA A UN TERCERO EL TRATAMIENTO DE DATOS.

- Elaboración de nóminas de personal
- Destrucción de documentación
- Control de cámaras de videovigilancia
- Gestión de cobro de impuestos
- Mantenimiento de equipos informáticos
- Fuente: AEPD, *Protección de Datos y Administración Local*

Registro de las actividades de tratamiento

Se trata, sin duda, de una de las novedades más significativas del RGPD, que enlaza directamente con la filosofía que impregna el nuevo modelo de gestión de datos personales.

La creación o mantenimiento de un registro de actividades de tratamiento es una obligación que deben llevar a cabo necesariamente los responsables del tratamiento (o sus representantes) y los encargados del tratamiento (o sus representantes). Y sustituye la antigua obligación de notificar los ficheros y tratamientos a las autoridades de control (AEPD, adpCAT o AVPD). No es un registro de ficheros, sino de tratamientos.

HERRAMIENTAS. CÓMO IMPLANTAR EL REGISTRO DE ACTIVIDADES: Un buen modelo de registro de actividades de tratamiento, a partir del "ciclo de vida de los datos", puede hallarse en: *Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD*, pp. 36-39

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php

El marco regulatorio viene establecido por el artículo 30 RGPD. Aunque cabe tener en cuenta lo que al respecto establezca la futura LOPD (artículo 31 PLOPD).

Las Administraciones Públicas y sus entidades del sector público institucional (con excepción de las sociedades mercantiles públicas) "harán público un inventario de sus actividades de tratamiento accesible por medios electrónicos" (artículo 31.2 PLOPD).

Hay que tener en cuenta que estos registros de actividades de tratamiento del responsable o del encargado tienen distinta intensidad en cuanto a su contenido, tal como establecen los apartados 1 (Responsable) o 2 (Encargado) del artículo 30 RGPD:

Responsables de tratamiento	***Encargados de tratamiento***
Nombre y datos de contacto del responsable o de su representante	Nombre y datos de contacto del encargado o de su representante
Nombre y datos de contacto del DPD	Nombre y datos de contacto del DPD
Fines del tratamiento	Categorías de tratamientos
Categorías interesados y de datos personales	
Categorías destinatarios comunicaciones, incluidos destinatarios terceros países	
Transferencias internacionales tercer país	Transferencias internacionales tercer país
Plazos previstos supresión categorías datos	
Medidas técnicas y organizativas de seguridad: descripción general	Medidas técnicas y organizativas de seguridad: descripción general

El artículo 30.5 RGPD expone lo siguiente:

> "Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10".

No obstante, este precepto se ha de interpretar de conformidad con lo establecido en el Considerando 13 "in fine". Su aplicabilidad como excepción a las Administraciones locales se ha de enmarcar en tales exigencias. Por los datos que se tratan en el ámbito local, al menos en algunos casos, la excepción entendida como inaplicación parece que no operaría en este caso.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO ADMINISTRACIÓN LOCAL: ALGUNOS EJEMPLOS:

- Impuesto vehículos: "Por ejemplo, si los datos que se utilizan para el cobro del impuesto de vehículos se usan para informar sobre una campaña informativa sobre contaminación producida por los citados vehículos, existirán dos tratamientos de esos datos: uno respecto al cobro del impuesto y otro referente a la citada campaña" (pp. 15-16)

- Registro de actividades del Padrón municipal y de Seguridad, ver: pp. 17-18

Fuente: AEPD, Protección de Datos y Administración Local

Seguridad de los datos personales

En el RGPD la seguridad se vincula estrechamente con la protección de datos personales y con la salvaguarda de los derechos y libertades de las personas físicas. Este es un enfoque de seguridad diferente, pues tiende a formar parte de ese Sistema de Gestión de Datos Personales que deben activar todas las organizaciones públicas.

Las novedades que introduce el RGPD en este ámbito también son importantes, sobre todo por la naturaleza proactiva de los tratamientos y la necesidad de tener el enfoque de riesgos estrechamente vinculado con los sistemas de seguridad. Ello imprime un concepto de seguridad "dinámico" o "instantáneo", que depende del responsable del tratamiento.

El marco regulatorio es muy preciso: Artículos 32 y 33 del RGPD. Ver asimismo la Disposición Adicional primera del PLOPD. En esta última referencia se emplaza a una modificación del Esquema Nacional de Seguridad para adaptarlo a las exigencias del RGPD, lo que implicará la modificación o adaptación 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.

Disposición adicional primera PLOPD:

"El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos de carácter personal para evitar su pérdida, alteración o acceso no autorizado, adaptando criterios de determinación del riesgo en el tratamiento de los datos en el artículo 32 del Reglamento (UE) 2016/679"

En función de una serie de variables que se enuncian en el artículo 32.1 RGPD, "el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo", que incluya, entre otras cuestiones:

- Seudonimización y cifrado de datos personales.
- Garantía de confidencialidad, integridad, disponibilidad y resiliencia de los sistemas.
- Capacidad de restaurar la disponibilidad y acceso rápidamente en casos de incidentes.
- Verificación, evaluación y valoración con carácter regular de la eficacia de las medidas técnicas y organizativas (*) (**).

(*) Cuando se evalúe la adecuación del nivel de seguridad se tendrán en cuenta los riesgos (algo que se trata en el siguiente epígrafe).

(**) La adhesión a códigos de conducta y mecanismos de certificación pueden servir como medios de cumplimiento de los requisitos establecidos.

IMPORTANTE PARA LA ADMINISTRACIÓN PÚBLICA Y ENTIDADES VINCULADAS, ASÍ COMO PARA LOS EMPLEADOS PÚBLICOS :

"El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable (…)" (Artículo 32.4 RGPD).

IDEAS-FUERZA SOBRE MEDIDAS DE SEGURIDAD SEGÚN AEPD:

- "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" (p. 20).
- "En ningún caso el RGPD se debe entender como la eliminación automática de tales medidas de seguridad ya existentes" (p. 20).
- "La seudonimización contribuye a reducir riesgos"

(AEPD, Protección de Datos y Administración Local)

***DATA BREACH:* VIOLACIONES DEL SISTEMA DE SEGURIDAD**

Se trata también de una importante novedad del RGPD. Se regula en los artículos 33 y 34, ofreciendo un doble régimen jurídico de notificación o comunicación inmediata ("sin dilación indebida") por parte del responsable del tratamiento a la autoridad de control y a los interesados, respectivamente, en los casos de violación de seguridad que comporten pérdida, alteración o destrucción de datos.

Hay, por tanto, una obligación institucional doble y está detrás de esta regulación un derecho de la persona física a ser informado de las violaciones del sistema de seguridad que afecten a sus datos personales. El encargado lo debe poner de inmediato en conocimiento del responsable.

RÉGIMEN DE NOTIFICACIONES Y COMUNICACIONES:

A la autoridad de control. Requisitos:

- A más tardar 72 horas después de que se haya tenido constancia de la violación.
- No es necesaria cuando sea improbable un riesgo para los derechos y libertades de la persona.
- La notificación debe recoger una serie de exigencias establecidas en el artículo 33.3 RGPD.
- La autoridad de control verifica el cumplimiento de lo previsto en el artículo 33 RGPD.

A los interesados. Requisitos:

- Se comunica la violación de los datos personales "cuando sea probable que entrañe un alto riesgo para los derechos y libertades".
- La comunicación describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad, así como deberá cumplir determinadas exigencias (artículo 34.2 RGPD).
- Supuestos en que no es necesaria (artículo 34.3 RGPD).
- La autoridad de control puede exigir al responsable de tratamiento que lleve a cabo esta comunicación cuando no lo haya hecho.

PARA SABER MÁS:

ARTICLE 29 DATA PROTECTION WORKING PARTY 17/EN, WP 250

Guidelines on Personal data breach notification under Regulation 2016/679

Adopted on 3 October 2017

Análisis de Riesgos

El enfoque predominantemente "proactivo" del Sistema de Gestión de Datos Personales que se deriva del RGPD impone al responsable y encargado del tratamiento la exigencia de **llevar a cabo con carácter previo un Análisis de Riesgos,** al menos para descartar que se pueda requerir la necesidad de realizar una "evaluación de impacto relativa a la protección de datos" que se analiza en el siguiente epígrafe de esta guía.

Esta cuestión está asimismo entrelazada con el sistema de seguridad que se implante, pues **el análisis de riesgos debe formar parte de la propia evaluación del nivel de seguridad.**

Y ello lo pone de relieve el artículo 32.2 RGPD de forma diáfana:

> "Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de protección de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos".

El análisis de riesgos está por tanto imbricado con la seguridad y también con la prevención o anticipación, forma parte "existencial" por tanto del nuevo Sistema de Gestión de Datos Personales también en el sector público.

Pero ahora nos interesa el Análisis de Riesgo como fase previa a la evaluación. Y para ello cabe remitirse a un documento que elaboró en su día la AEPD sobre esta cuestión.

PARA SABER MÁS Y COMPRENDER MEJOR QUÉ ES UN ANÁLISIS DE RIESGOS:

Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD (GARTDP, en lo sucesivo)

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php

El modelo del RGPD basado en un enfoque de riesgos se despliega con un carácter preventivo con una finalidad muy precisa: garantizar los derechos y libertades de los interesados desde la definición de una actividad de tratamiento.

PROTECCIÓN DE DATOS POR DISEÑO Y POR DEFECTO:

El artículo 25 RGPD, tal como se ha dicho, prevé una importante regulación de lo que se enuncia como "Protección de datos desde el diseño y por defecto". Y toma como referencia dos dimensiones:

- ***Privacy by design. Garantizar la protección de la privacidad desde el inicio o diseño*** (los datos deben protegerse cuando se diseñe un proceso nuevo): Artículo 25.1 RGPD ("(…) el responsable del tratamiento aplicará tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas (…) para aplicar de forma efectiva los principios de protección de datos".

- ***Privacy by default. Garantizar la protección de la privacidad en todo momento o por defecto.*** (los datos deben estar siempre protegidos por defecto). Artículo 25.2 RGPD: "El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento".

LÍNEAS FUERZA DE LA GARTDP (AEPD) SOBRE ANÁLISIS DE RIESGOS:

- **FINALIDAD:** El diseño adecuado de las actividades de tratamiento es un aspecto clave para poder garantizar los derechos y libertades de los interesados.

- **CUÁNDO**: La fase de diseño de un tratamiento define el flujo de los datos personales y es el momento idóneo para definir las medidas de control y seguridad para garantizar los derechos y libertades.

- **QUÉ ES LA GESTIÓN DE RIESGOS:** "Es el conjunto de actividades y tareas que permiten controlar la incertidumbre relativa a una amenaza mediante una secuencia de actividades que incluyen la identificación y evaluación del riesgo, así como las medidas para su reducción o mitigación".

- **CUÁLES SON LAS ETAPAS DE LA GESTIÓN DE RIESGOS:** Es un sistema de monitorización continua que se pueden dividir en tres etapas:
  - IDENTIFICAR las amenazas
  - EVALUAR los riesgos
  - TRATAR los riesgos

- **QUÉ ES UNA AMENAZA:** "Es cualquier factor de riesgo con potencial para provocar un daño o perjuicio a los interesados sobre cuyos datos de carácter personal se realiza un tratamiento".

- **QUÉ ES UN RIESGO:** "Un riesgo se puede definir como la combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas".

- **TRATAR LOS RIESGOS:** "El objetivo de tratar los riesgos es disminuir su nivel de exposición con medidas de control que permitan reducir la probabilidad y/o impacto de que estos se materialicen.

- **DEFINICIÓN DE LA ACTIVIDAD:** Es el paso que requiere tener claros cuáles son las finalidades del tratamiento, así como definir adecuadamente las actividades de tratamiento, documentando los análisis y dejando constancia de la trazabilidad de estos. Se deben tener siempre presentes en este tipo de operaciones los principios del artículo 5 RGPD.

IDEA-FUERZA: El RGPD busca aprovechar las ventajas que ofrece la gestión de riesgos introduciendo una nueva visión donde ***el foco de atención no se centra en las amenazas a la seguridad de la organización, sino que centra su atención en las amenazas sobre los derechos y libertades de los interesados*** (esto es, ciudadanos, clientes, usuarios servicios, etc.). Por tanto, la evaluación de los riesgos debe ser el resultado de una reflexión sobre las implicaciones que los tratamientos de datos de carácter personal tienen en relación con los "interesados"

PARA SABER MÁS Y PARA APLICAR MEJOR LA GESTIÓN DE ANÁLISIS DE RIESGOS: Es de imprescindible consulta la citada Guía Práctica de Análisis de Riesgos en los Tratamientos de Datos Personales sujetos al RGPD elaborada por la AEPD

Para determinar si un tratamiento conlleva escaso riesgo, la AEPD ha elaborado la herramienta Facilita destinada a aquellas organizaciones y procesos que implican escaso nivel de riesgo en el tratamiento de los datos personales, partiendo de la premisa de que todo tratamiento conlleva un determinado nivel de riesgo.

https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/herramientas_ayuda/index-ides-idphp.php

Evaluación de Impacto sobre la Protección de Datos

Conviene tener claro desde el inicio que **una Evaluación de Impacto sobre la Protección de Datos (EIPD) no se requiere siempre.**

Por eso es importante llevar a cabo con carácter previo ese Análisis de Riesgos (aunque en algunos casos, como se verá, no es necesaria esta fase si la EIPD es obligatoria).

El Análisis de Riesgos puede conducir perfectamente a que no existe riesgo alguno en el tratamiento o los riesgos que conlleva son de orden menor (fácilmente controlables), adoptando las medidas técnicas y organizativas necesarias para preservar la seguridad de los datos personales y su no afectación a los derechos y libertades de las personas físicas. En ese caso no hay que pasar a la EIPD.

RECOMENDACIÓN: La GARTDP de la AEPD

Indica que "si como resultado del análisis previo se considera que no es necesario llevar a cabo una EIPD, se deben documentar adecuadamente los motivos por los cuales se ha llegado a esa conclusión", dejando constancia de que "se ha llevado a cabo ese análisis (responsabilidad proactiva)"

CARÁCTER DE LAS EIPD:

"Las EIPD están orientadas a asegurar preventivamente que, cuando las operaciones de tratamiento puedan comportar riesgos espacialmente relevantes (alto riesgo), se tomen las medidas para reducir, dentro de lo posible, el riesgo de dañar o perjudicar a las personas, o afectar negativamente sus derechos y libertades, impidiendo o limitando su ejercicio o contenido"

Guía Práctica sobre la Evaluación de Impacto relativa a la Protección de Datos 2.0 (GPEI, en lo sucesivo;, Barcelona, enero, 2018.

http://apdcat.gencat.cat/ca/documentacio/RGPD/altres_documents_dinteres/Guia-sobre-la-evaluacion-de-impacto-relativa-a-la-proteccion-de-datos-en-el-RGPD/

EIPD EN TRATAMIENTOS DE ALTO RIESGO:

CONSIDERANDO 84 RGPD:

"***A fin de mejorar el cumplimiento del presente Reglamento*** en aquellos casos en los que sea probable que las ***operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas***, debe incumbir al responsable del tratamiento la ***realización de una evaluación de impacto relativa a la protección de datos, que evalúe, en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo***. El resultado de la evaluación debe tenerse en cuenta cuando se decidan las medidas adecuadas que deban tomarse con el fin de demostrar que el tratamiento de los datos personales es conforme con el presente Reglamento. Si una evaluación de impacto relativa a la protección de datos muestra que las operaciones de tratamiento entrañan un alto riesgo que el responsable no puede mitigar con medidas adecuadas en términos de tecnología disponible y costes de aplicación, debe consultarse a la autoridad de control antes del tratamiento".

¿CUÁNDO LLEVAR A CABO UNA EIPD?

CONSIDERANDO 89 "in fine" RGPD

Estos tipos de operaciones de tratamiento pueden ser, en particular, las que implican el uso de nuevas tecnologías, o son de una nueva clase y el responsable del tratamiento no ha realizado previamente una evaluación de impacto relativa a la protección de datos, o si resultan necesarias visto el tiempo transcurrido desde el tratamiento inicial.

El Considerando 90, por su parte, detalla qué son "operaciones a gran escala" y en qué otras operaciones (a raíz, por ejemplo, del tratamiento de "datos de categorías especiales") se requiere EIPD.

REGULACIÓN DE LA EIPD EN EL RGPD

El marco regulatorio de la EIPD está recogido en el importante artículo 35 RGPD. Y en el artículo 36 RGPD se recoge el trámite de "consulta previa" estrechamente relacionado con los tratamientos de alto riesgo.

El artículo 35.1 RGPD establece una regla general que conviene tener siempre presente: **"**Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares".

Por su parte, el artículo 35.3 determina en qué casos la EIPD es necesaria en los tratamientos:

- Evaluación sistemática y exhaustiva de aspectos personales en un tratamiento automatizado (elaboración de perfiles) sobre cuya base se tomen decisiones que produzcan efectos jurídicos. En este sentido cabría preguntarse hasta qué punto es posible aprovechar las ventajas que proporciona la Administración electrónica, ser proactivos y utilizar el intercambio de datos personales entre administraciones públicas para ofrecer, por "anticipación", determinados servicios o prestaciones a la ciudadanía. Una vez más, en estos casos, hay que tener en cuenta todo lo dicho anteriormente.

- Tratamiento a gran escala de "categorías especiales de datos"

- Observación sistemática a gran escala de una zona de acceso público

La EIPD debe incluir, como mínimo, las exigencias recogidas en el artículo 35.7 del RGPD (Ver más adelante)

Otras cuestiones:

- Para llevar a cabo la EIPD el responsable contará siempre con el asesoramiento de la figura del delegado de datos personales (artículo 35.2).

- Hay que tener en cuenta en esta materia las facultades de las autoridades de control (artículo 35, apartados 4, 5 y 6)

- El cumplimiento de códigos de conducta se tendrán debidamente en cuenta al evaluar las repercusiones de las operaciones realizadas por los responsables o encargados (artículo 35.8 RGPD).

RÉGIMEN DE LA CONSULTA PREVIA: Regulación artículo 36 RGPD.

- Ante quién se formula: Autoridad de control.

- En qué casos: Cuando la EIPD muestre que el tratamiento entraña alto riesgo

- Papel de la autoridad de control: artículo 36, apartados 2 y 3. Ver asimismo apartado 4.

PARA SABER MÁS; UN MATERIAL DE CONSULTA IMPRESCINDIBLE:

La Autoridad Catalana de Protección Datos ha publicado recientemente una interesante y completa *Guía Práctica sobre la Evaluación de Impacto relativa a la Protección de Datos 2.0* (GPEI, en lo sucesivo), Barcelona, enero, 2018.

http://apdcat.gencat.cat/ca/documentacio/RGPD/altres_documents_dinteres/Guia-sobre-la-evaluacion-de-impacto-relativa-a-la-proteccion-de-datos-en-el-RGPD/

ALGUNAS ADVERTENCIAS PRELIMINARES SEGÚN LA AEPD SOBRE TRATAMIENTOS ANTERIORES A LA ENTRADA EN VIGOR DEL RGPD:

Guía Práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD (GEIPD)

1. "El RGPD prevé que las Evaluaciones de Impacto se lleven a cabo "antes del tratamiento" en los casos en que sea probable que exista un alto riesgo para los derechos y libertades de los afectados. Ello implica que el mandato del Reglamento no se extiende a las operaciones de tratamiento que ya estén en curso en el momento en que comience a ser de aplicación.

2. Sin embargo, sí debiera realizarse una Evaluación cuando en una operación iniciada con anterioridad a la aplicación del Reglamento se hayan producido cambios en los riesgos que el tratamiento implica en relación con el momento en que el tratamiento se pudo en marcha.

3. Este cambio en los riesgos puede derivar, por ejemplo, del hecho de que se hayan empezado a aplicar nuevas tecnologías a ese tratamiento, de que los datos se estén usando para finalidades distintas o adicionales a las que se decidieron en su momento, o de que se estén recogiendo datos distintos o diferentes",

ALGUNAS LÍNEAS FUERZA CONTENIDAS EN LA GEIPD (AEPD) Y EN LA GPEI (apdCAT):

- **ALERTA PERMANENTE:** "El continuo avance de la tecnología y la evolución de los tratamientos propician la aparición continua de nuevos riesgo que deben ser gestionados: el RGPD exige que los responsable del tratamiento implementen medidas de control"

- **EIPD**: "La EIPD es una herramienta de carácter preventivo". Se debe reducir el nivel de riesgo a través de determinadas medidas de control "hasta un nivel considerado aceptable".

- **¿CUÁNDO SE DEBE HACER UNA EIPD?:** Supuestos de "riesgos elevados". La EIPD está muy vinculada a dos conceptos: "alto riesgo" y tratamiento "a gran escala"

- **PRIVACIDAD:** La EIPD está alineada con el principio de privacidad y debe cumplir además con los principios de necesidad y proporcionalidad.

- **QUÉ DEBE INCLUIR UNA EIPD:**

    - Una descripción sistemática de las actividades de tratamiento previstas

    - Una evaluación de la necesidad y proporcionalidad del tratamiento respecto a su necesidad

    - Una evaluación de los riesgos

    - Las medidas para afrontar esos riesgos (garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales).

    - Fases:

        - Describir el ciclo de vida de los datos

        - Analizar la necesidad y proporcionalidad de los datos

        - Gestión de riesgos: Identificar amenazas y riesgos; evaluar riesgos; y tratar riesgos.

        - Plan de acción y conclusiones. Si procede, consulta previa.

- **CÓMO DEBE ENTENDERSE LA EIPD:** Debe entenderse como un proceso de mejora continua, "de forma que esta se revise siempre que se modifique o actualice cualquier aspecto relevante de las actividades de tratamiento".

- **QUIÉN DEBE REALIZAR LA EIPD:** El responsable del tratamiento. Pero:

    - No obstante, "es importante destacar que la responsabilidad del 'responsable' no implica que el área indicada para cada fase de la EIPD sea obligatoriamente quien deba ejecutar las tareas asociadas, pudiendo apoyarse en otras áreas, expertos, recursos externos, etc.".

    - La obligación del hacer una EIPD corresponde al responsable del tratamiento, con el apoyo y la colaboración del encargado del tratamiento y con el DPD.

    - "Adicionalmente, el personal encargado de la seguridad, el área de tecnología, asesoría jurídica o incluso diferentes responsables de distintas áreas implicadas en el tratamiento pueden ser requeridas durante el proceso de evaluación".

RECOMENDACIÓN GPEI (apdCAT):

"La documentación relacionada con las evaluaciones de impacto debe estar a disposición de las autoridades de supervisión, es decir, no solo el informe final, sino también el conjunto de trabajos que se han utilizado para hacer la evaluación y que sustentan las decisiones tomadas" (p. 15)

- **¿CUÁL ES EL PAPEL DEL DELEGADO DE PROTECCIÓN DE DATOS EN LA EIPD?** El papel del Delegado de Protección de Datos en la EIPD es muy relevante. A saber:

    - Proporciona asesoramiento necesario al responsable del tratamiento para el adecuado desarrollo de la ejecución de la EIDP.

    - "Supone un valor añadido en el desarrollo de la EIPD aportando garantías para los derechos y libertades de los interesados".

    - "Puede haber sido el mismo delegado de protección de datos quién haya definido cómo se debe ejecutar las EIPD en la organización (por ejemplo, mediante la elaboración de una guía interna de evaluación o adoptando una guía externa que sirva de marco de evaluación); y asimismo, quien ejecute la evaluación" (GPEI)

    - El DPD debe verificar la adecuada ejecución de la EIPD

- **METODOLOGÍA** (Ver GEIPD, pp. 10-36):

    - Contexto del tratamiento: Conocer ciclo de vida y flujo de los datos

    - Gestión de riesgos:

        - Identificar

        - Evaluar

        - Tratar

    - Comunicación y consulta a la autoridad de control

    - Supervisión y revisión de la implantación: papel del DPD.

ORIENTACIONES PARA LA EJECUCIÓN DE LA EIPD SEGÚN LA GPEI (ACPD):

- **Aspectos preparatorios de la ejecución de la EIPD:** Método de evaluación, interlocutores, equipo de evaluación, etc.

- **Análisis de la necesidad de hacer la EIPD:** ¿Qué datos se tratarán y de quién? (elaborar lista exhaustiva); volumen de personas afectadas por el tratamiento y si este es "a gran escala"; ¿Qué se prevé hacer con los datos?

- **Descripción sistemática de las operaciones de tratamiento** (descripción funcional según el ciclo de los datos)

- **Objetivos y finalidades del tratamiento:** evaluación necesidad y proporcionalidad de las operaciones de tratamiento.

- **Gestión de riesgos:** aspectos generales. Identificación de potenciales escenarios de riesgo (PER)

- **Informe de evaluación:** Conclusiones y Recomendaciones para mitigar los riesgos de las operaciones de tratamiento.

IDEA FUERZA:

La gestión de riesgos que prevé el RGPD va más allá de evaluar la exposición al riesgo de los sistemas de información o de los datos o de los riesgos para la organización (GPEI/ACPD, p. 61).

IDENTIFICACIÓN DE SITUACIONES DE RIESGO SEGÚN RGPD GPEI/ACPD (p. 61):

- Se priva a los interesados de sus derechos y libertades, que incluye cuando se impide su ejercicio normal y libre.
- Se provocan daños y perjuicios físicos, materiales o inmateriales a las personas interesadas.
- Se revelan categorías especiales de datos personales, o relativas a condenas e infracciones penales, durante el tratamiento.
- Se crean o se utilizan perfiles personales.
- Se tratan los datos personales de colectivos especialmente vulnerables
- Se trata una gran cantidad de datos personales o datos que afectan a un gran número de personas

CUATRO CUESTIONES CLAVE EN UNA EIPD (GEIPD, AEDP):

1. En ningún caso se puede proceder a llevar a cabo un tratamiento sI el riesgo es elevado.

2. En aquellos casos en que se presta un servicio como encargado de tratamiento se recomienda realizar un análisis de riesgos sobre la tipología del servicio prestado.

3. Siempre que exista una variación relevante en el contexto de las actividades de tratamiento que pueda suponer un incremento del riesgo asociado al mismo, deberá realizarse una actualización de la EIPD.

4. Si el responsable del tratamiento está adherido a algún código de conducta donde se incluya metodología propia, se podrá utilizar la misma para la realización de las EIPD.

PARA SABER MÁS:

GT29 WP 248; Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento entraña probablemente un alto riesgo a efectos del Reglamento (UE) 2016/279

http://apdcat.gencat.cat/ca/documentacio/RGPD/altres_documents_dinteres/altres_documents_del_grup_de_larticle_29/

IDEA-FUERZA FINAL:

Una EIPD es un proceso utilizado para reforzar y demostrar el cumplimiento (GPEI/adpCAT, p. 7)

SMART CITIES: UN EJEMPLO DE EIDP SEGÚN LA AEPD

- « Antes de la puesta en producción de un proyecto Smart City es necesario hacer un análisis previo del mismo valorando el volumen de la información que se pretende procesar y el número y tipo de fuentes desde la que se pretende obtener dicha información o incluso el tiempo durante el que se pretende conservar esta información"

- Por tanto, en estos casos, "será necesaria la realización de una evaluación de impacto relativa a la protección de datos o incluso una consulta previa a la autoridad de protección de datos" (p. 24)

AEPD, *Protección de datos y Administración Local, 2018.*

El delegado de protección de dato

La figura del delegado de protección de dato (DPD) es nueva, aunque tiene algunos precedentes que ahora no es necesario citar.

Se inserta, como una pieza más e importante, en el nuevo Sistema Institucional y de Gestión de Datos Personales que se enmarca en esa política "proactiva", anticipatoria o preventiva por la que aboga el RGPD.

Para las Administraciones Locales la nota más importante es la obligatoriedad que establece el RGPD: todas ellas deben disponer de un DPD.

Realmente, esta exigencia, como tantas otras que se contienen en el RGPD, iba más dirigidas a las Administraciones Públicas de gran tamaño y a otras sectoriales donde los riesgos, el uso masivo y las categorías especiales en el tratamiento de datos personales son la moneda corriente. Pero la obligación normativa está ahí y, por tanto, ha de cumplirse.

Hay que insertar la figura del DPD en ese cambio de modelo de gestión de datos personales al que se viene haciendo referencia. Y **hay que verlo como ventana de oportunidad,** pues el DPD **debería ayudar a ese proceso de transformación organizativa y al cambio en los tratamientos que el RGPD exige**.

Esa transformación o tránsito de una cultura "reactiva" a otra "proactiva" no es fácil, menos aún en un sector público en el que el endurecimiento del régimen sancionador del RGPD se ve hasta cierto punto descafeinado, al descansar principalmente sobre "multas administrativas".

En ese contexto, **el DPD debe ser una palanca de transformación que haga posible la implantación de la cultura proactiva también** en las instituciones públicas y, por lo que ahora interesa, **en la Administración Local**.

Pero, además, el DPD es importante que tenga conocimientos especializados y cualificación pertinente, pues **es el punto de apoyo principal del responsable y encargado del tratamiento, al efecto de cumplir debidamente las obligaciones del RGPD.** Debería actuar, por tanto, como "cortafuegos" que impidiera incumplimientos. **Especialmente importante es su papel en los procesos de evaluación de impacto.**

Es en el considerando 97 donde se dibujan las líneas maestras de esa nueva figura del DPD, que luego serán desarrolladas por los artículos 37 a 39 del RGPD, así como a través de referencias incidentales (algunas que ya se han visto) a lo largo del resto del articulado.

CONSIDERANDO 97 RGPD:

"Al supervisar la observancia interna del presente Reglamento, ***el responsable o el encargado del tratamiento debe contar con la ayuda de una persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos si el tratamiento lo realiza una autoridad pública,*** a excepción de los tribunales u otras autoridades judiciales independientes en el ejercicio de su función judicial (…) ***Tales delegados de protección de datos, sean o no empleados del responsable del tratamiento, deben estar en condiciones de desempeñar sus funciones y cometidos de manera independiente."***

Cuatro son, por tanto, las ideas-fuerza que cabe resaltar del DPD según este Considerando 97:

1.- El DPD es un **colaborador necesario**, aunque también supervisor, del responsable o encargado del tratamiento en el sector público.

2.- Debe ser DPD una persona que acredite **conocimientos especializados del Derecho y de la práctica de protección de datos**.

3.- El DPD puede ser **empleado público o ser provisto de forma externa**.

4.- El DPD **ejerce sus funciones y cometidos "de manera independiente"**

Antes de adentrarnos en el análisis de la regulación normativa y en algunos aspectos operativos o prácticos que plantea a corto plazo esta figura, es conveniente delimitar su alcance en el ámbito de lo que hasta ahora indeterminadamente llamamos "sector público"

¿Qué cabe entender por "autoridad y organismo público" según el RGPD?

El RGPD utiliza ***la expresión "autoridad y organismo público"*** a la hora de atribuir la exigencia de crear necesariamente la figura del DPD.

¿Y qué cabe entender por "autoridad y organismo público" según el RGPD?

Esta es una noción que, como expuso el Grupo de Trabajo del Artículo 29 en el documento que seguidamente se cita (Directrices sobre los delegados de protección de datos), **reenvía al Derecho interno de los Estados miembros**.

Y, por tanto, tendría que ser la futura LOPD la que precise su perímetro. De momento, la redacción que se ha dado al artículo 34 PLOPD es sencillamente frustrante, pues seguimos sin saber con certeza qué entidades del sector público son las que están obligadas a disponer de esta figura del DPD.

Para resolver el problema (al menos hasta que la LOPD se apruebe definitivamente) se puede intentar acudir al artículo 77 PLOPD, donde se regula cuál es el "Régimen aplicable a determinadas categorías de responsables o encargados

del tratamiento" que, por una razón de paralelismo, cabría estimar que son las entidades que sí tienen obligación de disponer de un DPD. Por lo que afecta al ámbito local de gobierno, el perímetro de aplicación de tal régimen singular se proyecta sobre las siguientes entidades:

- Los entes que integran la Administración Local (ayuntamientos, veguerías o diputaciones, áreas metropolitanas, comarcas, mancomunidades y entidades municipales descentralizadas)

- Los organismos públicos y entidades de Derecho Público vinculadas o dependientes de la Administración Local (organismos autónomos y entidades públicas empresariales)

- Las fundaciones del sector público adscritas a entes locales.

- Los consorcios adscritos a un ente local.

Si se puede trasladar este esquema institucional a las entidades que están obligadas a disponer de un DPD, ello supondría que las sociedades mercantiles no tendrían esa obligación "ex RGPD", pero que sí podría exigírseles en los mismo términos que a las empresas del sector privado cuando concurrieran las circunstancias previstas en el citado RGPD.

Pero no parece tener mucho sentido que se incluya a las fundaciones y no a las sociedades mercantiles de capital público. Algunas de ellas llevan a cabo precisamente tratamiento de datos de forma extensa e intensa (piénsese, por ejemplo, en todas aquellas sociedades mercantiles de capital público que prestan servicios informáticos de apoyo a la entidad matriz).

PARA SABER MÁS:

Directrices sobre los delegados de protección de datos (DPD), adoptadas el 13 de diciembre de 2016. Revisadas por última vez y adoptadas el 5 de abril de 2017, Grupo de Trabajo sobre la protección de Datos del Artículo 29. 16/ES WP 243, rev. 1
http://apdcat.gencat.cat/ca/documentacio/RGPD/altres_documents_dinteres/altres_documents_del_grup_de_larticle_29/

La regulación de esta figura se recoge principalmente en los artículos 37 a 39 RGPD.

El artículo 37, dedicado a **"la designación"** del DPD, prevé los siguientes extremos:

- **DESIGNACIÓN PRECEPTIVA:** ¿Cuándo ha de designarse según el RGPD por el responsable del tratamiento preceptivamente un DPD? (artículo 37.1 RGPD) El caso de las autoridades y organismos públicos ya ha sido analizado. Lo que no impide que cualquier organización lo pueda designar voluntariamente o si así lo exige la legislación de un Estado miembro (artículo 37.4 RGPD)
- **¿CUÁNTOS DPD?:** Pretende dar respuesta a si cabe nombrar uno o varios DPD (por grupo de empresas o autoridad u organismo público, atendiendo a "su estructura organizativa y su tamaño" (artículo 37.2 y 3 RGPD)
- **ACREDITACIÓN COMPETENCIAS PROFESIONALES:** Las exigencias profesionales y conocimientos que debe acreditar quien sea designado DPD, vinculadas a las funciones de la figura (artículo 37.5 en relación con artículo 39 RGPD)
- **¿INTERNO O EXTERNO?** El DPD podrá formar parte de la plantilla o ser un externo a la organización (contratación de servicios) (artículo 37.6 RGPD)
- **PUBLICIDAD DEL DPD:** El responsable o encargado publicarán (presumiblemente en la Web o Portal de Transparencia) los datos de contacto del DPD y los comunicarán a la apdCAT.

Por su parte, el artículo 38 tiene como objeto **"la posición"** del DPD en relación con el responsable o encargado del tratamiento:

- **COLABORADOR NECESARIO**: Se prevé una garantía de participación del DPD en "todas las cuestiones relativas a la protección de datos personales" (artículo 38.1 RGPD).
- **RECURSOS:** Se le deben facilitar al DPD los recursos necesarios para el desempeño de sus funciones y para el mantenimiento de sus conocimientos especializados (formación) (artículo 38.2 RGPD)
- **ESTATUTO INDEPENDENCIA:** Garantía de que no recibirá ninguna instrucción en lo que respecta al desempeño de sus funciones, no pudiendo ser destituido ni sancionado por su desempeño, y rindiendo cuentas al más alto nivel jerárquico de la organización (artículo 38.3 RGPD)
- **PUNTO DE CONTACTO:** Los interesados podrán ponerse en contacto con el DPD en todo lo relativo a sus datos personales y al ejercicio de sus derechos (artículo 38.4 RGPD).
- **CONFIDENCIALIDAD:** El DPD está obligado a mantener el secreto o confidencialidad por el desempeño de sus funciones (artículo 38.5 RGPD)
- **DPD "A TIEMPO PARCIAL"**: El DPD podrá desempeñar otras funciones siempre que no den lugar a conflictos de interés (artículo 38.6 RGPD)

Y, en fin, el artículo 39 RGPD define cuáles son, como mínimo, las funciones del DPD, vinculándolas todas ellas especialmente a "los riesgos asociados a las operaciones de tratamiento"(artículo 39.2 RGPD) . A saber:

FUNCIONES DEL DPD SEGÚN EL RGPD:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados sobre las obligaciones del RGPD y del Derecho interno.
- Supervisar el cumplimiento del presente RGPD, promover su implantación en la organización e impulsar la formación.
- Ofrecer asesoramiento sobre la EIPD y supervisar su aplicación.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control.

Por su parte, ha de ser la futura LOPD la que complete algunos de los perfiles de este régimen jurídico de la figura del DPD definida por el RGPD.

El PLOPD contiene, por ejemplo, las siguientes previsiones (artículos 34 a 37):

- Obligación de comunicar a la adpCAT en el plazo de 10 días las designaciones, nombramientos y ceses de los DPD
- La adpCAT mantendrá una lista actualizada de DPD que será accesible por medios electrónicos.
- Por Real Decreto se establecerá el procedimiento de interconexión de las listas creadas por las autoridades de control (adpCAT/ACPD/AVPD).
- La acreditación de los "requisitos" exigidos por el RGPD podrá realizarse, entre otros medios, a través de mecanismos voluntarios de certificación
- La remoción del DPD se podrá realizar si incurriera en dolo o negligencia grave en el ejercicio de sus funciones, previo expediente disciplinario tramitado al efecto (sector público).
- El DPD tendrá acceso a todos los datos personales y procesos de tratamiento.
- Cualquier vulneración relevante en materia de protección de datos será comunicada por el DPD al responsable o encargado del tratamiento.
- Con carácter previo a la interposición de una reclamación antes la autoridad de control por parte del interesado, este "podrá dirigirse al DPD de la entidad contra la que se reclame". En este caso, el DPD "comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación".
- Si el afectado presenta la reclamación ante la adpCAT, esta podrá remitir la reclamación al DPD a fin de que responda en el plazo de un mes. En caso de son respuesta, continuará el procedimiento.

ALGUNAS DIRECTRICES DE LAS AUTORIDADES DE CONTROL SOBRE LA FIGURA DEL DELEGADO DE PROTECCIÓN DE DATOS:
El Delegado de Protección de Datos en las Administraciones Públicas
http://www.agpd.es/portalwebAGPD/temas/reglamento/index-ides-idphp.php

PARA SABER MÁS:
Rafael Jiménez Asensio, "*La figura del Delegado de Protección de Datos en las organizaciones públicas*", La Mirada Institucional
https://rafaeljimenezasensio.com/2018/03/20/la-figura-del-delegado-de-proteccion-de-datos-en-las-organizaciones-publicas-1/
Víctor Almonacid, "*El Delegado de Protección de Datos en la Administración Local*"
https://nosoloaytos.wordpress.com/2018/03/28/el-delegado-de-proteccion-de-datos-en-la-administracion-local-dpo/#more-13764
Concepción Campos Acuña, "*Los 7 imprescindibles en protección de datos para el ámbito local*", El Consultor de los Ayuntamientos y Juzgados, enero 2018

IDEAS-FUERZA Y PROBLEMAS APLICATIVOS DE LA IMPANTACIÓN DE LA FIGURA DEL DPD EN LAS ADMINISTRACIONES LOCALES

¿CUÁNTOS DPD DEBE HABER EN LAS AAPP?:
- Uno al menos, en las Administraciones Públicas de cierto tamaño pueden ser dos o más, según sectores. Nada impide, sin embargo, que sea un solo DPD con una unidad o departamento y actuando de forma descentralizada.

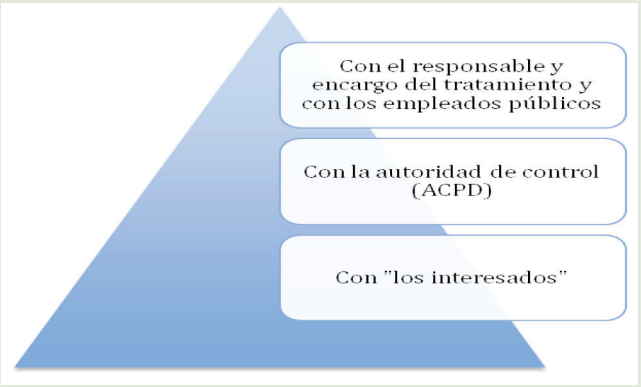
¿LOS GOBIERNOS LOCALES DE PEQUEÑO O MEDIANO TAMAÑO DEBEN TENER DPD?
- Necesariamente, pero esa función se puede prestar por las diputaciones, comarcas o, en su caso, a través de mancomunidades o por medio de convenios entre entes locales (horizontales o verticales).

¿PUEDEN SER DPD ÓRGANOS COLEGIADOS?
- El GT-ART-29 lo desaconseja; la accesibilidad requiere personalización.

¿DEBE SER EL DPD FUNCIONARIO O EMPLEADO PÚBLICO?
- Preferentemente sí, siempre que realice funciones de autoridad (funcionario), pero cabe la externalización de los servicios, aunque no de aquellas funciones que directa o indirectamente ejerzan potestades públicas. Las funciones del RGPD pueden ejercerse por un externo (empresa o profesional), las que asigna el PLOPD pueden plantear más dudas.

¿CABE QUE EL DPD DESARROLLE SUS FUNCIONES A TIEMPO PARCIAL? Sí, siempre que no se vea incurso en conflictos de interés.

POSICIÓN DEL DPD Y FUNCIONES: LA RELACIÓN TRIANGULAR DEL DPD



FUNCIONES DEL DPD:

- RGPD fija funciones mínimas. Derivan de su relación "triangular"

- Atención especial a los riesgos en las operaciones de tratamiento

- Las funciones esenciales son:

  - Asesorar responsable y encargado de tratamiento

  - Asesorar, orientar sobre análisis de riesgo y ejecutar, incluso, los EIPD

  - Supervisar cumplimiento RGPD

  - Cooperar con la autoridad de control

  - Actuar como punto de contacto

  - Conocer de las reclamaciones previas protección de datos y por remisión de la autoridad de control (PLOPD)

CUALIDADES PROFESIONALES QUE DEBE ACREDITAR EL DPD:

- "Cualidades profesionales y conocimientos especializados":

  - Conocimientos y experiencia de Derecho Público (Directrices: procedimientos administrativos)

  - Conocimientos y experiencia de protección de datos

  - Buen manejo del RGPD y de todos los instrumentos allí recogidos

- Qué ámbito profesional es el más idóneo para el desarrollo de esas funciones

  - No hay reserva profesional. Pero el PLOPD le da un sesgo jurídico acusado: resolver reclamaciones (puede subsanarse con personal técnico adscrito)

  - Las Directrices añaden también integridad y ética (inciden mucho en cómo evitar conflictos de intereses).

ESTATUTO JURIDICO Y POSICIÓN DEL DPD:

- Independencia: no recibe instrucción alguna. No tiene dependencia jerárquica.

- Participación temprana en los procesos de tratamiento de datos.

- Presencia en los órganos que adaptan decisiones (problema con externos)

- Proveer de los recursos necesarios si es interno (local, medios personales y tecnológicos)

- Facilitarle formación para el mantenimiento de sus conocimientos

- "Tiempo suficiente" para el ejercicio de sus funciones

- A mayor complejidad del tratamiento más recursos

- Rendición de cuentas al máximo nivel (externos)

- Blindaje frente a sanciones (PLOPD) y remociones

- Mantener secreto y confidencialidad

UBICACIÓN ORGÁNICA DEL DPD:

- ¿Cómo encuadrarlo en la estructura?

- Descartar su encuadre como alto cargo.

- Unidad situada en Alcaldía o en la Presidencia. Motivos.

- Cubierta preferentemente por funcionario A1. No necesariamente jurista.

- Figura incardinada en el modelo de seguridad informática.

ALGUNOS PROBLEMAS DE RRHH EN RELACIÓN AL DPD: LISTADO DE CUESTIONES ABIERTAS.

- Crear un puesto de trabajo "ad hoc" o acumular las funciones a otro existente.

- Incorporar a plantilla presupuestaria y a la RPT, en su caso

- ¿Cómo cubrir ese puesto de trabajo?

  - Selección "ex novo" desaconsejable. Razones,

  - Cubrirlo con funcionarios interinos, desaconsejable también.

  - ¿Se puede designar personal laboral? Plantea dificultades (PLOPD)

- La primera tensión: discrecionalidad y profesionalidad. Debe primar esta última: criterios de competencia profesional.

- Provisión puesto DPD. Modalidades

  - Libre designación. Desaconsejada, no se ajusta RGPD.

  - Concurso de méritos, no mide competencia profesional efectiva

  - Concurso específico, puede ser el más idóneo

  - ¿Cabe la comisión de servicios y otras formas de provisión?

- La segunda tensión: temporalidad versus permanencia. Decisión estratégica: puesto de estructura permanente, pero cubierto por períodos. No hay (casi) profesionales de ese perfil. Importancia estratégica.

  - Decisión compleja en un primer momento, aunque RGPD parece dar carácter estructural a la figura, ello no impediría rotación.

  - Dificultades, marco jurídico rígido.

  - Se podría explorar la figura de la DPP como alternativa. Problemas: normativización.

ÁRBOL DE DECISIONES EN RELACIÓN CON EL DPD EN LAS ADMINISTRACIONES LOCALES:

1.- Internalizar o externalizar la figura. Valorar "pros" y "contras". Prestar servicios por otra Administración (definición del convenio). Prestar servicios externos (definición pliegos).

2.- Uno o varios DPD.

3.- Cómo y dónde encuadrarla en la estructura organizativa. No dependencia.

4.- Dotarla de medios: ¿estructura personal?

5.- A tiempo completo o parcial

6.- ¿Qué régimen jurídico aplicamos?

7.- ¿Qué sistema de provisión?

8.- ¿Cómo salvaguardar su independencia?

ALGUNAS CONCLUSIONES:

- Figura singular y de complejo encaje. Prueba ensayo/error

- Irá creciendo en protagonismo conforme avance la revolución tecnológica

- Banco de pruebas para explorar la incorporación de nuevos perfiles

- La exigencia de inscripción se difiere a la aprobación de la LOPD. Se gana tiempo.

- Factor tiempo: Nos hemos despertado muy tarde y sin las herramientas necesarias

Códigos de conducta y mecanismos de certificación

Se trata de **dos instrumentos que entroncan perfectamente con el enfoque "proactivo" que imprime el RGPD**. Tienen, por tanto, una orientación preventiva o anticipatoria.

Asimismo **son herramientas de carácter voluntario**, pero que en el caso de los códigos de conducta, una vez asumidos por quienes se adhieran a los mismos tendrán carácter vinculante.

En cualquier caso, sin perjuicio de lo que se dirá, cabe presumir que la adhesión a tales códigos puede implicar la atenuación en sus caso de las responsabilidades derivadas por un tratamiento de datos incorrecto. Aunque, en el supuesto de los mecanismos de certificación, expresamente se recoge la idea de que la certificación no limitará la responsabilidad del responsable o del encargado (artículo 43.4 RGPD). De ahí que se hablara al inicio de esta guía de una

política de compliance atenuada trasladada a la protección de datos.

CÓDIGOS, CERTIFICACIÓN Y POLÍTICA DE CUMPLIMIENTO

Esta impresión inicial puede desvanecerse si se analizan estas herramientas en el marco del conjunto de previsiones del RGPD.

En efecto, los rasgos del sistema preventivo y de cumplimiento son evidentes en ciertos pasajes del RGPD. Tal como prevén los artículos 24.3 y 28.5 RGPD, la adhesión a códigos de conducta o mecanismos de certificación "pueden ser utilizados como elementos para demostrar el cumplimiento" o la existencia de una serie de garantías, respectivamente, por parte del responsable o del encargado del tratamiento.

Asimismo, la adhesión a un código de conducta o a un mecanismo de certificación "podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos" (en materia de seguridad) en el artículo 32.1 RGPD (artículo 32.3 RGPD).

También el cumplimiento de los códigos de conducta "se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por los responsables o encargados", en particular cuando se lleve a cabo una EIPD.

IDEA-FUERZA:

Por consiguiente, **disponer de códigos de conducta y mecanismos de certificación es** no solo adoptar una visión preventiva en línea con la finalidad del RGPD, sino especialmente ***dotarse de una política de cumplimiento que salvaguarda la función del responsable o encargado del tratamien***to de cualquier organización, también de la Administración Local.

REGULACIÓN CÓDIGOS DE CONDUCTA

En el RGPD:

El RGPD regula en los artículos 40 a 43 los códigos de conducta y los mecanismos de certificación. A pesar de su carácter de libre adhesión, cabe constatar que algunas de tales previsiones no se aplican a "las autoridades y organismos públicos".

El artículo 40.1 RGPD prevé una labor de promoción de los códigos de conducta que será llevada a cabo, por lo que ahora interesa, por la adpCAT (o el resto de autoridades de control), en la que se tendrán en cuenta las características específicas de los distintos sectores de tratamiento.

IDEA-FUERZA:

Los códigos de conducta están destinados a contribuir a la correcta aplicación del RGPD (artículo 40.1)

Por su parte, el artículo 40.2 se refiere a que "las asociaciones y otros organismos representativos de categorías de responsables o encargados de tratamiento podrán elaborar códigos de conducta". Como podrían ser, por ejemplo, las asociaciones o federaciones de municipios o entes locales, en su caso.

Y se establece un contenido orientativo de lo que pueden recoger tales códigos. Por ejemplo (Ver artículo 42.2 RGPD):

- La recogida de datos personales
- La información proporcionada al público y a los interesados
- El ejercicio de los derechos del interesado
- Las medidas y procedimientos para garantizar la seguridad del tratamiento
- La notificación y comunicación de las violaciones de la seguridad de los datos, respectivamente, a la autoridad de control y a los interesados

Es importante, asimismo, tener en cuenta que tales asociaciones que promuevan esos códigos de conducta (por ejemplo, FMC, ACM, FEMP o EUDEL) deben presentar el **proyecto de código ante la autoridad de control** (adpCAT o la autoridad que corresponda: AEPD o AVPD) **para que por parte de esta se dictamine si es conforme al RGPD y proceda a aprobar tal código** "si considera suficiente las garantías adecuadas ofrecidas". Por parte de la autoridad de control se registrará y publicará tal código (artículo 40.5 y 6 RGPD).

ACLARACIÓN (Exclusión autoridades y organismos públicos):

Cabe tener en cuenta que el artículo 41 RGPD ("Supervisión de los códigos de conducta aprobados"), así como por conexión el artículo 40. 4 RGPD, no se aplicarán al tratamiento realizado por autoridades y organismos públicos (artículo 41.6 RGPD)

En el PLOPD

La regulación (provisional) de los códigos de conducta en el PLOPD se contiene en su artículo 38 y tiene, por lo que a la Administración Local interesa, los siguientes rasgos:

- Los códigos de conducta serán vinculantes por quienes se adhieran a los mismos.
- Podrán promoverse por asociaciones y organismos, pero también por los responsables o encargados a los que se refiere el artículo 77.1 LOPD. Por tanto, por cualquier ente local, organismo público, consorcio o fundación.
- Los códigos serán aprobados por las autoridades de control (adpCAT/AEPD/AVPD)
- Las autoridades de control someterán los proyec-

tos de código de conducta al mecanismo de coherencia establecido en el artículo 63 RGPD, en relación con lo previsto en el artículo 40.7 RPD.

- La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán un registro conjunto de los códigos de conducta aprobados.

- Por Real Decreto se establecerá el contenido del registro y las especialidades del procedimiento de aprobación de los códigos de conducta.

REGULACIÓN MECANISMOS DE CERTIFICACIÓN

En el RGPD

Los artículos 42 y 43 RGPD regulan los mecanismos y organismos de certificación.

En el artículo 42.1 también se recoge una labor de "promoción" que debe ser ejercida entre otros por los Estados miembros y las autoridades de control con la finalidad de crear mecanismos de certificación en materia de protección de datos y sellos y marcas de protección de datos. El objetivo de tales instrumentos es siempre "demostrar el cumplimiento de lo dispuestos en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados"

IDEA-FUERZA:

Los mecanismos de certificación (sellos o marcas) tienen como finalidad principal demostrar que, por parte de los responsables y encargados del tratamiento, se cumple el RGPD. Tienden, por tanto, a salvaguardar la actuación de responsables y encargados. De ahí la importancia de dotarse de ellos.

Las líneas básicas de esa regulación son las siguientes:

- La certificación será voluntaria y estará disponible a través de un proceso transparente (artículo 42.3 RGPD).

- La certificación no limitará las responsabilidad del responsable o encargado del tratamiento en cuanto al cumplimiento del presente Reglamento (artículo 42.4 RGPD)

- Será expedida por los organismos de certificación regulados en el artículo 43 RGPD o por la autoridad de control competente (adpCAT), sobre la base de criterios aprobados por dicha autoridad en los términos establecidos en el artículo 42 RGPD.

- Obligación de los responsables y encargados del tratamiento de proveer toda la información necesaria para llevar a cabo el procedimiento de certificación.

- La certificación será expedida al responsable o encargado del tratamiento por un período máximo de tres años, renovables en las condiciones expuestas (artículo 42.6 RGPD)

En el PLOPD

El artículo 39 PLOPD confiere la competencia para llevar a cabo la acreditación de las instituciones de certificación a la Entidad Nacional de Acreditación (ENAC), que será la que comunique a las autoridades de control respectivas (adpCAT) las concesiones, denegaciones o revocaciones de las acreditaciones, así como su motivación.

Se ha de tener asimismo en cuenta la disposición transitoria segunda del PLOPD en relación con los códigos tipo inscritos en las autoridades de protección de datos de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre: Adaptación de su contenido al artículo 40 RGPD en el plazo de un año.

UNA BUENA PRÁCTICA:

Esquema de Certificación de Delegados de Protección de Datos de la Agencia Española de Protección de Datos (Esquema AEPD-DPD)

http://www.agpd.es/portalwebAGPD/temas/certificacion/index-ides-idphp.php

Autoridades de control independientes: Idea general

No cabe duda que la correcta implantación del RGPD, también en los distintos niveles de gobierno (y, en particular, en la Administración Local) requiere de esa pieza institucional imprescindible que son las autoridades de control.

No es objeto de esta guía, por sus especiales características, analizar el papel y funciones de tales autoridades de control, a las que el RGPD y el PLOPD dedican un buen espacio regulador.

En estas páginas solo interesa destacar cuál es la finalidad de tales autoridades de control, en especial de la adpCAT (aunque también sus relaciones con la AEPD y con la AVPD), y poner de relieve algunos de sus elementos más relevantes, pues se trata sin duda, del mecanismo de cierre para que el nuevo Sistema Institucional y de Gestión de Protección de Datos de las Administraciones Locales funcione adecuadamente.

Bajo este punto de vista es oportuno resaltar que la finalidad principal de las autoridades de control no es otra que la protección de las personas físicas con respecto al tratamiento de datos de carácter personal.

Esta es una idea que se recoge perfectamente en el Considerando 117 y en otros sucesivos (por ejemplo, en el Considerando 123 donde se añade a la finalidad anterior la de "facilitar la libre circulación de los datos personales en el

mercado interior"). En el ejercicio de esas funciones "deben supervisar la aplicación de las disposiciones adoptadas de conformidad con el presente Reglamento y contribuir a su aplicación coherente en toda la Unión".

CONSIDERANDO 117 RGPD

El establecimiento en los Estados miembros de autoridades de control capacitadas para desempeñar sus funciones y ejercer sus competencias con plena independencia constituye un elemento esencial de la protección de las personas físicas con respecto al tratamiento de datos de carácter personal. Los Estados miembros deben tener la posibilidad de establecer más de una autoridad de control, a fin de reflejar su estructura constitucional, organizativa y administrativa.

No interesa abordar aquí las cuestiones relativas a la posición institucional de estas autoridades de control ni tampoco a la existencia de varias autoridades de control o a la designación, en este caso, de una autoridad de control que ejerza como "punto de contacto único" (Considerando 117). Pero sí puede ser oportuno resaltar que los amplios cometidos funcionales que el RGPD encomienda a tales autoridades de control implicarán necesariamente un refuerzo de recursos financieros y humanos, que no parece ser muy viable en época de contención fiscal.

REGULACIÓN DE LAS AUTORIDADES DE CONTROL EN EL RGPD

La regulación de las autoridades de control en el RGPD está contenida en su Capítulo VI. Este capítulo se estructura en diferentes secciones que abordan, entre otros, los siguientes ámbitos materiales:

- Designación de una o varias autoridades por Estado (actualmente en España existen tres: AEPD, adpCAT y AVPD (artículo 51 RGPD)
- Estatuto de independencia de tales autoridades (ajenos a toda influencia externa, ya sea directa o indirecta y no admitirán ninguna instrucción) (artículo 52 RGPD)
- Condiciones aplicables a los miembros de las autoridades de control y normas relativas al establecimiento de la autoridad de control. (artículos 53 y 54 RGPD)
- Competencias de la autoridad principal de control (artículos 55 y 56 RGPD)
- Funciones es el aspecto más importante a nuestros efectos y se trata de forma singularizada (artículo 57 RGPD)
- Poderes, que se desdoblan en poderes de investigación, correctivos o de autorización y consultivos (artículo 58 RGPD).
- Informe de actividad (artículo 59 RGPD)

ALGUNAS FUNCIONES DE LAS AUTORIDADES DE CONTROL EN RELACIÓN CON LOS GOBIERNOS LOCALES:

- Controlar la aplicación del presente Reglamento y hacerlo aplicar.

- Asesorar a las instituciones sobre las medidas administrativas a adoptar para la protección de los derechos y libertades con respecto a los tratamiento de datos.

- Promover la sensibilización de los responsable y encargados del tratamiento sobre sus obligaciones derivadas del presente Reglamento.

- Tratar las reclamaciones presentadas.

- Llevar a cabo investigaciones sobre aplicación del presente Reglamento.

- Adoptar cláusulas contractuales tipo

- Elaborar lista relativa al requisito de evaluación de impacto.

- Ofrecer asesoramiento sobre operaciones de tratamiento.

- Alentar la elaboración de códigos de conducta, dictaminar y aprobarlos.

- Fomentar la creación de mecanismos de certificación de la protección de datos y aprobar los criterios de certificación.

- El desempeño de las funciones de la autoridad de control será gratuito para el interesado y para el delegado de protección de datos; salvo las excepciones tasadas en la norma (artículo 57.4 RGPD)

ALGUNOS "PODERES CORRECTIVOS" DE LAS AUTORIDADES DE CONTROL SEGÚN EL RGPD

- Sancionar a todo responsable o encargado del tratamiento con una advertencia.

- Sancionar a todo responsable o encargado del tratamiento con un apercibimiento

- Ordenar al responsable o encargado del tratamiento que atienda las solicitudes de ejercicio de los derechos del interesado en virtud del RGPD

- Ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten al RGPD

- Ordenar al responsable de tratamiento que comunique las violaciones de la seguridad de los datos personales.

- Imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición.

- Ordenar la rectificación o supresión de datos personales o la limitación de tratamiento.

- Retirar una certificación

- Imponer una multa administrativa (ver régimen singular entidades sector público)

REGULACIÓN DE LAS AUTORIDADES DE CONTROL EN EL PLOPD

El Título VII del PLOPD regula exhaustivamente las autoridades de protección de datos.

No puede ser objeto de esta guía un análisis detenido de tales previsiones, máxime el carácter provisional que ellas tienen al encontrarse en plena tramitación de enmiendas el citado proyecto de ley.

Por tanto, solo se dará noticia puntual de algunos de los puntos de esa propuesta normativa a efectos de pura información y obviamente de aquellos que puedan afectar con mayor intensidad a las entidades locales.

Algunos aspectos de interés de esa regulación a efectos de la presente guía serían los siguientes:

- En el capítulo relativo a la Agencia de Española de Protección de Datos, conviene resaltar lo siguiente:
    - En el ámbito de las potestades de investigación y planes de auditoria preventiva hay que tener en cuenta lo dispuesto en el artículo 51 sobre ámbito de la investigación y personal competente para llevarla a cabo.
    - Igualmente es importante el deber de colaboración de las Administraciones Públicas establecido en el artículo 52.
    - Las potestades de regulación a través de "Circulares de la Agencia Española de Protección de Datos"
    - O las funciones relacionadas con la acción exterior.
- En el capítulo relativo a las autoridades autonómicas de protección de datos, se contienen algunas previsiones importantes en el ámbito local. Por ejemplo, dos de ellas vinculadas con el ejercicio que a tales autoridades de control se les reconoce de las funciones establecidas en los artículos 57 y 58 RGPD, cuando se refieran a:
    - Tratamientos de los que sean responsable las entidades integrantes del sector público de la correspondiente Comunidad Autónoma de las entidades locales incluidas en su ámbito territorial o quienes presten servicios a través de cualquier forma de gestión directa o indirecta.
    - Tratamientos llevados a cabo por personas físicas o jurídicas para el ejercicio de las funciones públicas en materias que sean competencia de la correspondiente Administración Autonómico o Local.
- Cabe presumir igualmente que la normativa reguladora de las autoridades de control de las Comunidades Autónomas (adpCAT y AVPD) deberán adaptarse a lo establecido en el RGPD.

Régimen de responsabilidades y sanciones: Idea general. Aplicación al sector público

Uno de los pilares de esta nueva regulación era dotar a la normativa (y, en particular, a las autoridades de control) de "poderes coercitivos más contundentes" con el fin de proteger los derechos y libertades de las personas físicas como consecuencia de los tratamientos de datos personales. Detrás de todo ello está, sin duda, el avance imparable de la revolución tecnológica y el poder cuasi absoluto de las empresas de ese mismo ámbito que despliegan su actividad con el manejo y cruce de toda la información recuperada a través de los motores de búsqueda, de las redes sociales o de los correos electrónicos. Es algo muy conocido.

Con esta finalidad de fortalecer la aplicabilidad del nuevo marco normativo en esta materia, no quedaba otra opción que hacer el necesario hincapié en el poder sancionador. Y esto es algo que se recoge en los Considerandos 149 y siguientes del RGPD. Veamos un ejemplo.

CONSIDERANDO 148 RGPD

A fin de reforzar la aplicación de las normas del presente Reglamento, cualquier infracción de este debe ser castigada con sanciones, incluidas multas administrativas, con carácter adicional a medidas adecuadas impuestas por la autoridad de control en virtud del presente Reglamento, o en sustitución de estas. En caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento. Debe no obstante prestarse especial atención a la naturaleza, gravedad y duración de la infracción, a su carácter intencional, a las medidas tomadas para paliar los daños y perjuicios sufridos, al grado de responsabilidad o a cualquier infracción anterior pertinente, a la forma en que la autoridad de control haya tenido conocimiento de la infracción, al cumplimiento de medidas ordenadas contra el responsable o encargado, a la adhesión a códigos de conducta y a cualquier otra circunstancia agravante o atenuante. La imposición de sanciones, incluidas las multas administrativas, debe estar sujeta a garantías procesales suficientes conforme a los principios generales del Derecho de la Unión y de la Carta, entre ellas el derecho a la tutela judicial efectiva y a un proceso con todas las garantías.

En todo caso, como anuncia el título del presente epígrafe, la pretensión de estas líneas es solo dar una idea general de esta problemática, entre otras cosas porque su aplicabilidad a las entidades del sector público se ve mediatizada por la regulación que se prevé en el PLOPD, donde –a pesar del cambio cualitativo que implica el RGPD- en el ámbito sancionador se sigue el viejo patrón de la LOPD de 1999, con algunos matices.

REGULACIÓN EN EL RGPD

El Capítulo VIII del RGPD se enuncia del siguiente modo: "Recursos, responsabilidad y sanciones". De esa regulación nos interesa particularmente todo aquello que tiene que ver con la responsabilidad y el régimen de sanciones. Pero muy sucintamente este capítulo aborda los siguientes temas:

- Prevé el derecho que tiene todo interesado de presentar una reclamación ante la autoridad de control si considera que el tratamiento de datos personales aplicado infringe el presente Reglamento (artículo 77)

- Prevé, asimismo, el derecho a la tutela judicial efectiva en un doble sentido: contra una autoridad de control; y contra un responsable o encargado del tratamiento (artículos 78-79)

- Se regula la representación de los interesados (artículo 80) y la suspensión de los procedimientos (artículo 81)

- Se contiene una importante regulación relativa al derecho de indemnización y responsabilidad (artículo 82), de la que conviene destacar algunos extremos.

- Hay que tener en cuenta que este Capítulo VIII, sobre todo su artículo 83, reenvía a determinados "poderes" (con implicaciones obviamente sancionadoras) que ejercen las autoridades de control según el artículo 58 (por ejemplo, advertencias o apercibimientos).

- El artículo 83 establece lo que denomina como "Condiciones generales para la imposición de multas administrativas". Un precepto fundamental a partir del cual la legislación de los Estados miembros adaptará su régimen sancionador o lo impondrá en aquellos casos que no lo tuviera. Particularmente importante por lo que se dirá es el artículo 83.7 RGPD. Este precepto requiere asimismo una cita expresa.

DERECHO A INDEMNIZACIÓN Y RESPONSABILIDAD: EXTRACTOS (ARTÍCULO 82 RGPC)

1. Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.
2. Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el presente Reglamento. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del presente Reglamento dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable.

CONDICIONES GENERALES PARA LA IMPOSICIÓN DE MULTAS ADMINISTRATIVAS: EXTRACTOS (ARTÍCULO 83)

"1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.
2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta: (…)
3. Si un responsable o un encargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones del presente Reglamento, la cuantía total de la multa administrativa no será superior a la cuantía prevista para las infracciones más graves.
4. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía: (…)
5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía: (…)"

LA PREVISIÓN PUNTUAL PARA LAS AUTORIDADES Y ORGANISMOS PÚBLICOS: ARTÍCULO 83.7 RGPD

7. Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, ***cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro.***

PROPUESTA DE REGULACIÓN EN EL PLOPD

El Título IX del PLOPD trata del Régimen sancionador. Y muy brevemente nos interesa hacer mención a algunos de esos artículos, pero especialmente a la previsión recogida en el artículo 77 PLOPD, porque –de aprobarse en estos términos la futura LOPD- colocaría a las entidades del sector público en una posición casi similar a la que se encuentra actualmente la Administración Pública en el marco normativo vigente anterior al RGPD.

En términos generales, la citada regulación que se propone contiene los siguientes elementos:

- Sujetos responsables (artículo 70 PLOPD), donde entre otros se prevén los responsables y los encargados de los tratamientos, así como se afirma que al delegado de protección de datos no le será de aplicación el régimen sancionador previsto en este título.

- Se tipifican las infracciones muy graves, graves y leves (respectivamente, artículos 72, 73 y 74)

- Se regula la interrupción de la prescripción (artículo 75) y el régimen de prescripción de las sanciones (artículo 78)

- También se recoge una regulación cobre sanciones y medidas coercitivas.

- Y, finalmente, el artículo 77 del PLOPD establece un "régimen aplicable a determinadas categoría de responsables o encargados del tratamiento", con amparo en el artículo 83.7 RGPD. Y, dada su importancia para la Administración Local, es oportuno reproducirlo en su integridad, al margen de cómo quede realmente en la versión final tras su tramitación parlamentaria.

ARTÍCULO 77 PLOPD: Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento.

1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.

b) Los órganos jurisdiccionales.

c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.

d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.

e) Las autoridades administrativas independientes.

f) El Banco de España.

g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.

h) Las fundaciones del sector público.

i) Las Universidades Públicas.

j) Los consorcios.

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 73 a 75 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido. La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos podrá proponer también la iniciación de actuaciones disciplinarias. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, ésta publicará en su página web con la debida separación las resoluciones en que se imponga una sanción a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.

PARA SABER MÁS:

GRUPO DE TRABAJO SOBRE LA PROTECCIÓN DE DATOS DEL ARTÍCULO 29; 17/ES WP 253

Directrices sobre la aplicación y fijación de multas administrativas a efectos del Reglamento 2016/679

Otras cuestiones. Situaciones específicas de tratamiento

Con carácter meramente telegráfico conviene poner de relieve algunas otras disposiciones que el RGPD encuadra como "situaciones específicas de tratamiento".

A tal efecto, se deberán tener en cuenta las siguientes previsiones:

- **Tratamiento y libertad de expresión e información** (artículo 85 RGPD) , lo que implica una obligación a los Estados miembros de conciliar la protección de datos personales con tal derecho fundamental, en particular en lo que se refiere al tratamiento con fines periodísticos y de expresión académica, artística o literaria.

- En el artículo 86 RGPD se regula el **tratamiento y acceso a documentos oficiales**.

- Por su parte en el artículo 87 se prevé una **regulación del número nacional de identificación.**

- El artículo 89 prevé una serie de **garantías aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica y fines estadísticos.**

- El artículo 90 se ocupa de las **obligaciones de secreto**.

- Y, finalmente, el artículo 91 tiene por objeto las "**normas vigentes sobre protección de datos de las iglesias y asociaciones religiosas**".

Particular importancia tiene la previsión del artículo 88, sobre **tratamiento en el ámbito laboral,** que cabe entender plenamente aplicable a las relaciones de empleo en el ámbito del sector público.

ARTÍCULO 88 RGPD: TRATAMIENTO EN EL ÁMBITO LABORAL

1. Los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral.
2. Dichas normas incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo.
3. Cada Estado miembro notificará a la Comisión las disposiciones legales que adopte de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior de las mismas.

En este sentido es de notable importancia la propuesta normativa recogida en la Disposición adicional decimoquinta del PLOPD que tiene por objeto una serie de "disposiciones específicas aplicables a los tratamientos de los registros de personal del sector público".

Disposición adicional decimoquinta. Disposiciones específicas aplicables a los tratamientos de los registros de personal del sector público.

1. Los tratamientos de los registros de personal del sector público se entenderán realizados en el ejercicio de poderes públicos conferidos a sus responsables, de acuerdo con lo previsto en el artículo 6.1.e) del Reglamento (UE) 2016/679.

2. Los registros de personal del sector público podrán tratar datos personales relativos a infracciones y condenas penales e infracciones y sanciones administrativas, limitándose a los datos estrictamente necesarios para el cumplimiento de sus fines. 3. De acuerdo con lo previsto en el artículo 18.2 del Reglamento (UE) 2016/679, y por considerarlo una razón de interés público importante, los datos cuyo tratamiento se haya limitado en virtud del artículo 18.1 del citado reglamento, podrán ser objeto de tratamiento cuando sea necesario para el desarrollo de los procedimientos de personal.

Asimismo, por lo que afecta a la **transparencia publicidad activa y al derecho de acceso a la información pública**, es importante tener en cuenta lo recogido en la disposición adicional segunda del PLOPD que, en materia de protección de datos reenvía a lo dispuesto en los artículos 5.3 y 15 de la Ley 19/2013, a lo establecido en el RGPD y también a lo que regule la LOPD. Esta referencia debe entenderse extensiva a lo establecido en la Ley 19/2014, del Parlamento de Cataluña, de transparencia, acceso a la información pública y buen gobierno.

DOCUMENTACIÓN RECIENTE AEPD: MUY ÚTIL

Listado de cumplimiento normativo para facilitar la adaptación al RGPD

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2018/notas_prensa/news/2018_04_13-ides-idphp.php

Final

Protección de datos e inteligencia artificial

LOS DATOS NO SON EL NUEVO PETRÓLEO DE LA ECONOMÍA

"Uno de los lugares comunes de nuestro tiempo es que los datos son el nuevo petróleo (…) Pero los datos no se parecen al petróleo. El petróleo es un recurso finito; los datos son infinitamente renovables"

(*Franklin Foer, Un mundo sin ideas: La amenaza de las grandes empresas tecnológicas a nuestra identidad*; Paidós, 2017, pp. 182-183)

LA ERA DEL ALGORITMO

"La era del algoritmo marca el momento en que la memoria técnica ha evolucionado para almacenar no solo nuestros datos, sino también algunos patrones del comportamiento más sofisticado, desde el gusto musical hasta nuestros grafos sociales. En muchos casos, ya nos estamos imaginando sincronizados con nuestras máquinas".

(*Ed Finn, La búsqueda del algoritmo. Imaginación en la era de la informática*, Alpha Decay, p. 336)

UNA IDEA PARA EL DEBATE

"¿Y qué significa realmente la retórica en torno a la smart city o ciudad inteligente? Si se lee más de cerca, quiere decir que nuestra infraestructura urbana será entragada a un grupo de empresas tecnológicas (desde luego no muy propensas a la transparencia) que luego la gestionarán como mejor les parezca, lo que hará casi imposible remunicipalizarlas más adelante"

(*Evgeny Morozov, Capitalismo Big Tech*, , Enclave, 2018, P. 269).

LA ÉTICA DEL ALGORITMO

"Puede que llegue el momento, quizás más pronto que tarde, de que la pregunta sobre la ética de los algoritmos deba plantearse con respecto a la inteligencia artificial en evolución o, incluso, deba dirigirse a esa mente-máquina. De momento, aún es esencialmente una pregunta para los seres humanos que escriben los algoritmos"

(*Thimothy Garton Ash, Libertad de palabra. Diez principios para un mundo conectado*, Tusquets Editores, 2017, p. 494).

PARA SABER MÁS:

Un documento muy reciente (9 abril 2018): *A Statementon Artificial Intelligence, Robotics and 'autonomous' systems by the European Group of Ethics and Science in New Technologies:*

http://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf

BUENA PRÁCTICA

LOS NUEVOS RETOS DEL RGPD EN LA GESTIÓN Y TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL:

LA SEGURIDAD INTEGRAL EN EL AYUNTAMIENTO DE SANT FELIU DE LLOBREGAT

1. CONTEXTUALIZACIÓN Y ANTECEDENTES

El objeto de este trabajo es compartir la experiencia del Ayuntamiento de Sant Feliu de Llobregat en su camino para la adaptación de su organización interna a las obligaciones que, en materia de seguridad y protección de datos de carácter personal, la normativa ha ido imponiendo a las administraciones públicas.

El Ayuntamiento de Sant Feliu de Llobregat lleva muchos años adaptando su organización a los requerimientos que sucesivamente ha ido imponiendo a las administraciones públicas la regulación en materia de protección de datos de carácter personal.

Establecidas las bases organizativas de la época para la correcta protección de los datos de carácter personal, una nueva serie de leyes administrativas dieron un giro exponencial a lo que con anterioridad trataba, por un lado, la normativa de protección de datos, y por otro, ciertos estándares recogidos en normas ISO relativas a la seguridad de los sistemas.

Un primer revulsivo en esta materia fue la aprobación de la Ley 11/2007 LAECSP, que recogía en su articulado la necesidad de agudizar la protección de datos en la actividad electrónica de las administraciones públicas. De hecho, este nuevo modelo de Administración pública se ha ido configurando, desde el año 2007, mediante la publicación de normativa a nivel europeo, estatal y autonómico, que reconocen un conjunto de derechos a la ciudadanía e imponen obligaciones a las administraciones públicas en materia de Administración electrónica (leyes 39 y 40/2015, de procedimiento administrativo y régimen jurídico del sector público, y Esquemas Nacionales de Seguridad e Interoperabilidad); de transparencia, acceso a la información pública y buen gobierno (Ley estatal 19/2013 y Ley catalana 19/2014); de simplificación de la actividad administrativa de la Generalitat y de los gobiernos locales de Catalunya (Ley 16/2015); de reutilización de la información (Ley 37/2007, modificada por Ley 18/2015); de contratación electrónica (Ley 9/2017); de protección de datos de carácter personal (Reglamento UE 2016/679 del Parlamento Europeo y del Consejo); entre otros.

Estas normativas inciden en el desempeño de los principios plasmados en el Plan de Administración Electrónica 2016-2020 de la Unión Europea, que tiene como objetivo principal **eliminar los obstáculos digitales** que se oponen al Mercado Único Digital y evitar la fragmentación que se puede generar en el contexto de transformación de las administraciones públicas.

Estos principios se concretan en las siguientes dimensiones:

- **Digital por defecto,** las AAPP ofrecerán servicios digitales como opción preferente.
- **Principio de una sola vez,** garantizando que ciudadanía y empresas suministran la misma información sólo una vez a las AAPP.
- **Inclusión y accesibilidad** de forma predeterminada.
- **Apertura y transparencia,** garantizando que ciudadanía y empresas puedan tener control de acceso y rectificación de sus propios datos; control de los procesos administrativos que les involucran...
- **Transfronterizo de forma predeterminada,** facilitando la movilidad dentro del Mercado Único.
- **Interoperabilidad de forma predeterminada,** libre circulación de datos y de servicios digitales en la UE.
- **Confianza y seguridad,** más allá del cumplimiento normativo de protección de datos, privacidad y seguridad de TI, integrando estos elementos en la fase de diseño

En este sentido, el Ayuntamiento de Sant Feliu de Llobregat tiene un largo recorrido en el desarrollo de acciones encaminadas al desarrollo de la Administración electrónica, aprovechando todas las ventajas que las Tecnologías de la Información y la Comunicación ponen al alcance de las administraciones públicas, y todas aquellas herramientas e instrumentos que la normativa está avalando como infraestructuras fundamentales en esta transformación de las organizaciones.

De todas estas infraestructuras (sede electrónica, carpetas ciudadanas, tablón de anuncios electrónico, perfil de contratante, registro electrónico, firma electrónica, expedientes electrónicos, factura electrónica...), la protección de datos de carácter personal es para el Ayuntamiento de Sant Feliu de Llobregat, una pieza clave y esencial sobre los que pivotan el resto de instrumentos y herramientas necesarias para la transformación digital de las administraciones públicas.

2. LA SEGURIDAD INTEGRAL

Con posterioridad, y en desarrollo de la Ley 11/2007 LAECSP, fueron aprobados los Esquemas Nacionales de Seguridad e Interoperabilidad, regulados por el Real Decreto 3/2010, de 8 de enero, y Real Decreto 4/2010, de 8 de enero, lo que en la práctica requirió que, en paralelo al proyecto principal de desarrollo de la Administración electrónica, el Ayuntamiento comenzara también a llevar a cabo todas las acciones necesarias para adecuar sus sistemas a los preceptos de los esquemas.

En este contexto, el reconocimiento del derecho a comunicarse con las administraciones públicas a través de medios electrónicos comporta una obligación para ellas consistente en la promoción de las condiciones de seguridad necesarias para que estas transacciones se produzcan en un contexto adecuado de libertad e igualdad. En este sentido, hay que proteger los activos, sistemas de información y datos de las posibles amenazas, alrededor de tres actuaciones básicas: prevenir, reaccionar y recuperar.

Así, para garantizar el cumplimiento de la seguridad de los

sistemas de información por parte de las administraciones públicas, la Ley 40/2015 LRJSP, como ya hizo la LAECSP, se remitió al ENS (artículo 156), aprobado por el Real Decreto 3/2010 ENS y que ha sido posteriormente modificado por el Real Decreto 951/2015, de 23 de octubre.

En concreto, el ENS vino a instaurar y concebir la seguridad como un proceso integral y transversal en la organización, en un entorno donde las TIC implican unas nuevas amenazas para la seguridad de las transacciones y de los datos, y en especial en relación con los datos de carácter personal.

Está constituido por los principios básicos y los requisitos mínimos requeridos para una protección adecuada de la información. Los principios básicos del ENS establecen unos puntos de referencia para la toma de decisiones en referencia a las medidas de seguridad a tomar. Entre los principios básicos, se encuentran como principios fundamentales la seguridad como proceso integral; la gestión basada en riesgos o el carácter diferenciado de la seguridad respecto a la gestión de la información.

En ese momento, se tuvo que recalcular la estrategia en materia de seguridad de la información para poder atender a los requisitos mínimos fijados por el ENS que eran y son de obligado cumplimiento en el desarrollo de las políticas de seguridad que debían adoptar las AAPP. Con la aplicación de estas medidas de seguridad, se pretende, en esencia, minimizar el impacto que tendrían los incidentes de seguridad en los sistemas que permiten a la ciudadanía ejercer derechos y cumplir obligaciones.

Cabe destacar que, en el camino hacia el cumplimiento del ENS, hubo que realizar una serie de actuaciones, por lo que nos fue muy útil tomar como punto de partida la planificación que, en su Portal de Administración Electrónica, propone el Ministerio de Hacienda y Administraciones Públicas (a través de diferentes guías).

A grandes rasgos, se pueden concretar las siguientes actuaciones:

- Preparar y aprobar la política de seguridad de la información (CCN-STIC 805).
- Realizar un análisis de riesgos que incluya la valoración de las medidas de seguridad existentes. Preparar y aprobar la Declaración de Aplicabilidad de las medidas del Anexo II ENS (CCN-STIC 804). Implantar, operar y monitorear las medidas de seguridad a través de la gestión continua de la seguridad correspondiente.
- Auditar y verificar la seguridad y el cumplimiento del ENS (CCN-STIC 802 y CCN-STIC 808).
- Informar sobre el estado de la seguridad utilizando las métricas y los indicadores definidos (CCN-STIC 815 y CCN-STIC 824).
- Elaborar un Plan de Adecuación para la mejora de la seguridad (CCN-STIC 806).

La adecuación al ENS tiene por finalidad el establecimiento de un Sistema de Gestión de la Seguridad de la Información (SGSI), tal como se recoge en el Anexo III ENS, que exige la gestión continua de la seguridad en línea con los principios básicos a los que se ha hecho referencia anteriormente.

En el caso del Ayuntamiento de Sant Feliu de Llobregat, y una vez aprobado el Plan de Adecuación, nos encontramos en plena fase de desarrollo del Sistema de Gestión de la Seguridad de la Información, revisando los activos y estableciendo las medidas de seguridad adecuadas, en base a la reciente auditoría realizada y, también, en base a los nuevos requerimientos del RGPD, como se detallará posteriormente.

3. REORGANIZACIÓN DE LA SEGURIDAD EN EL AYUNTAMIENTO

En este escenario, otra de las actuaciones de cambio fue, de manera lógica, una necesaria reestructuración de la organización de la seguridad para garantizar el cumplimiento de la normativa tanto de protección de datos de carácter personal como de seguridad de los sistemas de información.

La organización de la seguridad es uno de los elementos estratégicos para conseguir implantar un Sistema de Gestión de la Seguridad de la Información (SGSI) y corresponde a cada organización definir, a través de su política de seguridad, el modelo organizativo así como detallar las atribuciones de cada responsable y los mecanismos de coordinación y de resolución de conflictos. A este respecto, debe tenerse en cuenta que el ENS establece la necesaria diferenciación entre la responsabilidad de la seguridad de los sistemas de información y la prestación de los servicios.

Así, si el objetivo es tratar la seguridad como un proceso transversal e integral, parece razonable que la organización de la seguridad se plantee también desde una doble perspectiva: la seguridad de los sistemas de información y de los datos que se gestionan, es decir, las responsabilidades derivadas del cumplimiento del ENS y las derivadas del cumplimiento de la normativa sobre protección de datos personales. Además, hay que tener presente que el RGPD establece también la necesidad de adoptar medidas de carácter técnico, organizativo y de seguridad en los procesos de tratamiento de datos.

Existen fórmulas diversas para la organización de la seguridad aunque, en el Ayuntamiento de Sant Feliu de Llobregat, se optó por una organización de la seguridad estructurada en dos órganos colegiados, la Comisión y la Subcomisión de Seguridad, que asumen funciones en materia de seguridad de la información y de protección de datos de carácter personal.

Así, finalmente, por acuerdo de JGL de 7 de junio de 2011, se aprobó la reestructuración de la organización de la seguridad del Ayuntamiento de Sant Feliu de Llobregat, que se concretó en los siguientes órganos colegiados y unipersonales con la distribución de competencias y funciones:

1. Responsable del fichero: Ayuntamiento de Sant Feliu de Llobregat (como ente público), representado por la figura del alcalde. Las funciones encomendadas son las propias de esta figura en la normativa en materia de protección de datos.

2. Comisión de Seguridad: órgano colegiado de carácter institucional, integrado por miembros del equipo de gobierno y del equipo directivo que ostenta funciones de responsable de la seguridad. Se reúne por lo menos dos veces al año.

3. Subcomisión de Seguridad: órgano colegiado responsable operativo, junto con la Oficina de Atención Ciudadana. Se reúne mensualmente y está integrado por un/a técnico/a jurídico/a, el Jefe del Departamento de RRHH, la Responsable de la Oficina de Atención Ciudadana, el Jefe de la Unidad de Informática y la Responsable de la Unidad de Gestión del Conocimiento y Calidad.

4. Dos administradores de Seguridad: Secretario y Sistemas de Información. Son las figuras nombradas por la Comisión de Seguridad para hacer efectivas las medidas de seguridad establecidas en el Reglamento de Medidas de Seguridad. Deben velar por las funciones de seguridad relacionadas con el Sistema Informático y la documentación, la distribución de la información a terceros, previa autorización por parte de la Comisión de Seguridad, y la información sensible. Los administradores de Seguridad deberán informar a la Comisión de Seguridad con una periodicidad mensual, y siempre que haya una incidencia grave o muy grave de seguridad.5. Gestors de fitxers: Direccions de serveis, caps de departaments, i caps d'unitat. Són les persones físiques o jurídiques, autoritats públiques, serveis o altres organismes que, sol o conjuntament amb altres, tracten dades de caràcter personal autoritzats pel Responsable del Fitxer. Assumeixen a l'Ajuntament les funcions típiques per a aquestes figures.

6. Responsable de Atención al Afectado: secretario, junto con la Oficina de Atención Ciudadana.

Tanto la Comisión de Seguridad como la Subcomisión de Seguridad asumen funciones de la LOPD y del ENS.

Por lo tanto, el cumplimiento de LOPD, ENS y ENI en el Ayuntamiento se lleva a cabo por la misma estructura organizativa del Ayuntamiento, mediante la Comisión y la Subcomisión de Seguridad.

En este sentido, visto con perspectiva, el foco que el Ayuntamiento puso en el desarrollo del ENS y en la consecución de un SGSI puede considerarse un gran acierto porque, como se ha demostrado, la evolución de la normativa en materia de protección de datos ha evolucionado hacia la consideración de la seguridad en una doble vertiente y en la necesidad de aplicar medidas de protección no sólo a los datos que se tratan sino también a los sistemas de información que los soportan. Da cierta satisfacción observar cómo el anteproyecto de la nueva LOPD recoge como medidas técnicas a aplicar las establecidas en el ENS, el cual será necesario que se adecue también a esta nueva normativa.

Ahora queda adaptar esta estructura organizativa en materia de seguridad a los nuevos preceptos establecidos en el RGPD para garantizar la seguridad de la información y la protección de datos, incorporando/adaptando los siguientes perfiles mínimos obligatorios: Responsable de tractament (RGPD)

- Responsable de tratamiento (RGPD)
- Responsable de la información (ENS)
- Responsable de seguridad (ENS)
- Delegado/a de Protección de Datos (RGPD)
- Responsable de Sistemas (ENS)
- Responsable de Servicio (ENS y LOPD)

Manteniendo la estructura de la Comisión y de la Subcomisión de Seguridad con funciones, entre otras, de coordinación, control del cumplimiento y establecimiento de las medidas y los procedimientos de seguridad establecidos en el Ayuntamiento.

4. ADECUACIÓN AL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS:

La adaptación al Reglamento General de Protección de Datos, que será aplicable a partir del 25 de mayo de 2018, requiere de la elaboración de una nueva ley orgánica que sustituya a la actual; pero, mientras se culmina este proceso, son de agradecer las guías y los materiales didácticos que se han ido publicando por las diferentes autoridades de control, la FEMP y, por supuesto, esta misma guía donde se destacan aquellos aspectos de la regulación en el RGPD que impactan de manera directa sobre la actividad de las administraciones públicas y, en especial, las entidades locales, como responsables y encargadas del tratamiento de datos personales en el desarrollo de sus actividades. Ya estamos trabajando, en el marco de la organización referenciada, para su consecución.

En este sentido, a finales de 2017, en sesión monográfica conjunta de la Comisión y la Subcomisión de Seguridad, se pusieron de manifiesto las obligaciones derivadas de la aplicación del RGPD para concienciar, tanto en el equipo de gobierno como en el equipo de dirección, de las actuaciones que era necesario llevar a cabo para el cumplimiento normativo en esta materia.

Las tareas que se identificaron como prioritarias a abordar durante el año 2018, para garantizar el correcto cumplimiento del Ayuntamiento en el ámbito de la seguridad de la información y datos de carácter personal, fueron:

- Adaptación al Reglamento General de Protección de Datos
- Realizar una auditoría del ENS
- Revisión de la organización de seguridad para incardinar la figura del delegado/a de Protección de Datos

Respecto a la adaptación al RGPD, algunas de las adecuaciones en las que ya estamos trabajando son las siguientes:

- **Identificar con precisión las finalidades y la base juri-**

dica de los tratamientos, y establecimiento de un Registro de Actividades de Tratamiento. En este sentido, hemos solicitado a la Autoridad Catalana de Protección de Datos copia del contenido de los ficheros inscritos en el Registro de Protección de Datos de Catalunya, a fin de disponer de un punto de partida para la elaboración del Registro de Actividades de Tratamiento. La información sobre la finalidad y la base jurídica de los tratamientos es fundamental para poder establecer en qué casos no será necesario recabar el consentimiento del afectado. De hecho, este punto es de capital importancia para cumplir con el principio de "una sola vez", garantizando que ciudadanía y empresas suministran la misma información sólo una vez a las AAPP. El actual artículo 28 de la LPACAP contempla la presunción del consentimiento salvo oposición expresa, lo que entra en contradicción con lo establecido en el RGPD, que prohíbe expresamente el consentimiento tácito. Tendremos que esperar si prospera el PLOPD que en la DA 10 establece la potestad de verificación de las AAPP cuando se formulan solicitudes por medios electrónicos; esperemos que la redacción final no especifique sólo por medios electrónicos, ya que es cierto que el procedimiento es únicamente electrónico, pero la solicitud, si no es un sujeto obligado, se puede realizar presencial o electrónicamente...

- **Identificar los tratamientos gestionados bajo el principio de consentimiento del interesado,** que deberá estar adaptado a las nuevas exigencias del RGPD; es decir, debe ser informado, libre, específico y otorgado por los interesados mediante una manifestación donde quede demostrada la voluntad de consentir, o mediante una clara acción afirmativa. Como se ha dicho antes, habrá que revisar, pues, aquellos tratamientos en los que se haya utilizado un consentimiento tácito para adaptarlo a la nueva normativa, garantizando en este caso la información de este cambio al afectado para que pueda ejercer sus derechos.

- **Cumplimiento del principio de transparencia,** revisando todos los procedimientos y formularios que tenemos en la sede electrónica para garantizar el derecho de información en la recogida de datos personales, y el ejercicio de los derechos de los afectados, dando respuesta en los plazos establecidos en el RGPD. En este sentido, hemos recogido la recomendación de la AEPD de adoptar un modelo de información por capas:

    1. En un primer nivel, en el formulario de solicitud, presentar la información básica (identificación del responsable, finalidad del tratamiento, ejercicio de derechos, origen de los datos...), que podremos hacer una vez hechas las acciones anteriores, ya que necesitan disponer de toda esta información para poderla ofrecer a la ciudadanía.
    2. En un segundo nivel, la información adicional que implicará la reformulación de la política de privacidad que actualmente tenemos publicada en el portal web del Ayuntamiento.

- **Identificar los contratos que impliquen tratamiento de datos de carácter personal** para adecuar las cláusulas relativas a los encargados de tratamiento.

- **Estamos elaborando también tanto la información de los trámites como los circuitos de los expedientes administrativos electrónicos para atender en tiempo y forma los nuevos derechos de los afectados,** el derecho de acceso, rectificación, supresión ("derecho al olvido"), oposición y limitación a su tratamiento.

- **Elaborar análisis de riesgos para los derechos y libertades de la ciudadanía de todos los tratamientos de datos que se desarrollen, y revisar las medidas de seguridad que se aplican al tratamiento en base a este análisis de riesgos.** Como se ha especificado anteriormente en este documento, el Ayuntamiento de Sant Feliu de Llobregat ha organizado la gestión de la seguridad desde una perspectiva transversal y, por lo tanto, la reciente auditoría del ENS ha contemplado tanto el cumplimiento de los requerimientos establecidos en esta norma técnica como la adopción de las medidas técnicas y organizativas que permitan garantizar el cumplimiento del RGPD. De hecho, como resultado de esta auditoría, se ha visto la necesidad de actualizar los activos del Ayuntamiento y de hacer una valoración del riesgo de los tratamientos con el objetivo de determinar con más claridad y aplicar las medidas de seguridad que corrijan o minimicen los riesgos.

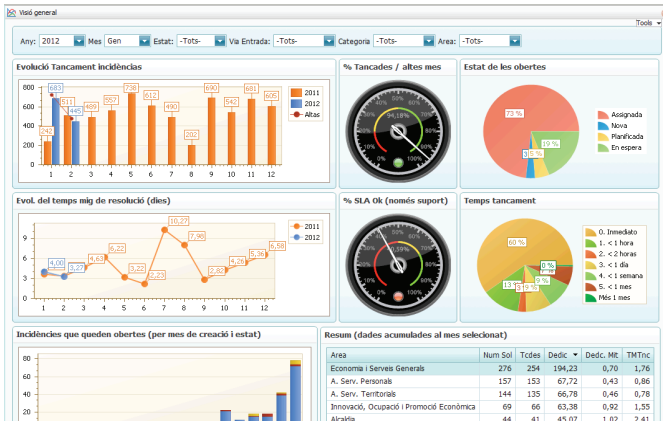
- **Elaborar e implementar el procedimiento de evaluación de impacto en la protección de datos,** en base a la metodología establecida por las autoridades de control. Este es un tema muy importante de cara al desarrollo real de la Administración electrónica como un instrumento para la simplificación y la posibilidad de anticipación de los servicios públicos en beneficio de la ciudadanía. Es evidente que las AAPP disponemos de una cantidad ingente de datos que, bien estructuradas, pueden permitir mejorar los servicios públicos, pasando de una administración reactiva (esperando la solicitud de los interesados), a una administración proactiva, por ejemplo, otorgando subvenciones a aquellas personas que cumplen determinados requisitos sin necesidad de que la ciudadanía lo solicite. Pero hacer esto implicaría el tratamiento de datos personales y hay que realizar previamente esta evaluación de impacto. Lo mismo puede pasar a la hora de desplegar políticas de Smart City, donde, además, el tratamiento y el intercambio de datos se realiza no sólo entre AAPP sino también con operadores económicos.

- **Aprobar la creación del puesto de trabajo de Delegado/a de Protección de Datos (DPD), que se incorporará a la Comisión y la Subcomisión de Seguridad.** En el Pleno de marzo de 2018, se ha aprobado el marco estratégico para la transformación cultural y organizativa del Ayuntamiento de Sant Feliu de Llobregat que incluye, entre otros acuerdos, el desarrollo de una estructura organizativa que incorpore los nuevos requerimientos normativos en materia de contratación, transparencia, control financiero, protección de datos y administración digital, lo que supone modificar el organigrama y el catálogo de puestos de trabajo para, entre otros, incorporar el perfil de delegado/a de protección de datos de carácter personal adscrito a la Dirección de Área de Gobierno Abierto y Servicios Generales. Las funciones serán las establecidas por el propio RGPD, pero también incorporará otras funciones

relacionadas con la reingeniería de procesos, la administración digital, gobierno abierto, etc., que no sean incompatibles con sus funciones propias.

- **Establecer los mecanismos para identificar con rapidez la existencia de violaciones de seguridad de los datos y poder reaccionar ante ellas.** En este caso, la aplicación de las medidas de seguridad estará marcada por los criterios establecidos en el Esquema Nacional de Seguridad, que debe adecuarse también a las previsiones del RGPD. Debemos establecer los procedimientos para comunicar estas violaciones en los plazos establecidos en la APDCat, en caso de riesgo para los derechos y libertades de las personas físicas, y las personas físicas afectadas. En el Ayuntamiento de Sant Feliu de Llobregat, disponemos de un registro de incidencias, que revisamos mensualmente en la Comisión de Seguridad, para aplicar las medidas técnicas necesarias, y estamos elaborando un plan de contingencias que contemple cómo actuar en caso de caída de los sistemas o bien ante una brecha de seguridad.

  En este sentido, nos hemos dotado de un cuadro de mando para controlar las incidencias producidas en materia de seguridad:



- **La adopción del principio de responsabilidad proactiva ("Accountability"),** revisando y manteniendo actualizada permanentemente toda la documentación relacionada (Documento de Seguridad, Política de Seguridad, Manual de funciones y obligaciones, nuevos procedimientos...), para poder demostrar en todo momento a quien lo solicite que cumplimos con el RGPD y que se han establecido los mecanismos y las actuaciones necesarias, lo que se irá adecuando y desplegando progresivamente.

- **Formación en materia de protección de datos.** El Ayuntamiento de Sant Feliu de Llobregat ha incorporado desde hace tiempo esta materia en su Plan Estratégico de Formación, y en la intranet se dispone de un espacio abierto para todos los empleados públicos con información permanente, recomendaciones, plantillas, presentaciones, guías, enlaces de interés, etc.

5. CONCLUSIONES

De todo lo expuesto, se puede observar con claridad que el Ayuntamiento de Sant Feliu de Llobregat está realizando un trabajo de continuidad en la protección de los datos de carácter personal dentro de la organización.

Como expone muy claramente el profesor Rafael Jiménez Asensio en la presente guía, nos encontramos ante un cambio de paradigma en la concepción de la gestión de la protección de datos que requiere el establecimiento de medidas técnicas pero sobre todo organizativas para incorporar la seguridad como un proceso transversal en la actividad de las administraciones públicas. Y es razonable que, ante el reto de la transformación digital, la seguridad ocupe un papel fundamental para generar la confianza de la ciudadanía en el uso de los medios electrónicos pero también para garantizar la transparencia, la rendición de cuentas y, por supuesto, los derechos y libertades de las personas respecto al uso que hacen las administraciones públicas de sus datos personales.

La Administración Digital permite la trazabilidad; controlar los accesos... Pero se requiere establecer las políticas de seguridad, las medidas organizativas y los procedimientos necesarios para que, de forma proactiva, se puedan tomar decisiones con relación a los nuevos tratamientos de la información y reaccionar rápidamente ante las violaciones en materia de seguridad que se puedan producir.

En este sentido, visto con perspectiva, el foco que el Ayuntamiento puso en el desarrollo del ENS y en la consecución de un SGSI puede considerarse un gran acierto porque, como se ha demostrado, la evolución de la normativa en materia de protección de datos ha evolucionado hacia la consideración de la seguridad en una doble vertiente y en la necesidad de aplicar medidas de protección no sólo a los datos que se tratan sino también a los sistemas de información que los soportan.

Sant Feliu de Llobregat, 3 de abril de 2018

DOCUMENTACIÓN ANEXA A LA GUÍA

MATERIALES, INFORMES, ARTÍCULOS Y RESOLUCIONES SOBRE RGPD

REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL 2016/679

Josep Betriu Sangüesa
Alba Sánchez Hostalot

1. Guías, materiales y herramientas sobre el RGPD y su impacto en el sector público

2. Adaptación de la LOPD al RGPD

3. Resoluciones de las Autoridades de Control Españolas.

4. Análisis jurisprudencial sobre la Protección de Datos: Tribunal Supremo, Tribunal Constitucional y Tribunal de Justícia de la Unión Europea.

5. Artículos referentes a la Protección de Datos de carácter personal.

6. Libros de reciente publicación relacionados con el Reglamento General de Protección de Datos.

1. GUÍAS, MATERIALES Y HERRAMIENTAS SOBRE EL RGPD Y SU IMPACTO EN EL SECTOR PÚBLICO

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

GUÍAS DE LA APDCAT

1.1 Guía básica de protección de datos para entes locales de la APDCAT

Esta es una guía elaborada por la Agencia Catalana de Protección de Datos que, aunque es relativa a la normativa precedente al nuevo RGPD, puede ser un punto de partida para ciertos aspectos que requieren de una serie de exigencias a los responsables de los entes locales.

1.2 Guía sobre cumplimiento del deber de informar según la APDCAT

El objeto de esta guía es orientar sobre las mejores prácticas para cumplir la obligación de informar a las personas interesadas, en virtud del principio de transparencia, sobre las circunstancias y las condiciones del tratamiento de datos a efectuar, así como de los derechos que las asisten. Al igual que en otras guías encontraremos una parte introductoria que, una vez superada, encontraremos herramientas útiles.

1.3 Guía práctica - AEvaluación de impacto relativa a la protección de datos.

Desde la APDCAT se redactó esta guía que será útil para poder realizar una evaluación de impacto con garantías. En esta guía se explicarán cuáles son los aspectos preparatorios, el análisis de la necesidad de realizar una evaluación de impacto, la descripción sistemática de las operaciones de tratamiento, y finalmente dispondremos de modelos que poder aplicar.

1.4 Guia sobre el encargado del tratamiento en el Reglament General de Protecció de Datos (RGPD)

La guía elaborada por la Autoridad Catalana de Protección de Datos en colaboración con la Agencia Española de Protección de Datos y la Agencia Vasca de Protección de Datos, persigue identificar los puntos clave a tener en cuenta en el momento de establecer la relación entre el responsable del tratamiento y el encargado del tratamiento, así como identificar las cuestiones que afectan de manera directa la gestión de la relación entre los dos.

GUÍAS DE LA AEPD

1.5 Guía Reglamento General de Protección de Datos para responsables de tratamiento de la AEPD

Esta guía resume las novedades del Reglamento Europeo y los cambios que deberán tener en cuenta los responsables de las organizaciones que traten datos de carácter personal ya sean privadas o públicas. Contiene, incluso, un listado de verificación de carácter simplificado que podría ser de ayuda para aquellas entidades locales con un número de ciudadanos menor.

1.6 Guía sectorial de la AEPD sobre Protección de Datos y Administración Local

La guía trata aquellos aspectos del Reglamento que afectan a la Administración Local y cuenta , a su vez, con un catálogo de preguntas frecuentes relativas al RGPD y al tratamiento de datos de caràcter personal realizado por estos entes públicos.

1.7 Directrices para la elaboración de contratos entre responsables y encargados de tratamiento

Estas directrices son una guía elaborada, de forma conjunta, por las Autoridades de Protección de datos existentes en España. En ella encontraremos los procesos adecuados para elaborar un contrato con todas las garantías para los implicados, así como, adaptarse a todas las exigencias del RGPD.

1. 8 Guía de anonimización de la AEPD.

Esta guía está realizada para dar soporte para el caso que las entidades públicas, o privadas, requieran publicar una serie de datos con fines de estudio o estadísticos y, se garanticen la anonimidad de los sujetos objetos del estudio.

1.9 Decálogo para la adecuación al Reglamento General de Protección de Datos en las Administraciones Públicas.

Este contiene una numeración de las reglas básicas del RGPD que atañen a los organismos públicos.

1. 10 Guía para la adaptación del Reglamento General de Protección de Datos, de las Administraciones Locales, FEMP, Grupo de Trabajo para la Implantación del nuevo RGPD en las Administraciones Locales.

Esta es una guía muy recinte y muy actualiza en la que la AEPD i la FEMP han tratado el RGPD desde una prespectiva local.

1.11 Listado de cumplimiento normativo para la adaptación del RGPD

Este listado ha sido editado el pasado 13 de abril por la AEPD y es un método básico que permite obtener una visión general del grado de adecuación de un tratamiento de datos personales al RGPD, siendo especialmente útil tanto para los procesos de análisis de riesgo como en las evaluaciones de impacto

GUÍAS DEL GRUPO DE TRABAJAO DEL ARTÍCULO 29

1.12 Grupo de Trabajo del artículo 29

Los Trabajos del Grupo creado por la Directiva Europea 95/46, aunque no son jurídicamente vinculantes, tienen un importante valor doctrinal y son frecuentemente utilizados, y citados, por los legisladores y los tribunales nacionales y europeos, por lo que debemos referirnos a alguno de ellso como herramientas muy útiles para entender y aplicar la nueva normativa sobre protecció de datos.

- ***"Guidelines on Personal data breach notification under Regulation 2016/679"*** Sobre brechas en los sistemas de seguridad de tratamientos y cómo actuar frente a éstas según la normativa Europea.

- ***"Guidelines on Automated individual decision-***

making and Profiling for the purposes of Regulation 2016/67". Sobre cómo realizar perfiles individuales: detalla los derechos de los usuarios y diferencia datos de carácter especial o que pertenecen a sujetos sensibles, con el fin de realizar tratamientos más ajustados.

- ***"Data Protection Officers".*** Sobre la importantísima figura del encargado de protección de datos: realiza un riguroso estudio en lo que concierne al encargado y a lo que son sus tareas a realizar.

- ***"Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk"* for the purposes of Regulation 2016/679".** Esta guía es esencial para entender qué es la evaluación de impacto, así como para identificar el riesgo de los diferentes tratamientos.

- ***"Guidelines on the right to data portability"*** Sobre las directrices de cómo actuar en cuanto al derecho de portabilidad que, novedosamente, el Reglamento ha otorgado a los interesado

- ***"Dictamen del Grupo de Trabajo del Artículo 29 sobre el tratamiento de datos en el ámbito laboral"*** Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) así como para esclarecer si el tratamiento comporta un alto riesgo de vulneración de las disposiciones que establece el RGPD.

Todos los trabajos y dictámenes estan accessibles en la dirección web: http://collections.internetmemory.org/haeu/20171122154227/http:/ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

MATERIALES DE LOS ÓRGANOS EUROPEOS

1.13 Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones

Al igual que la tecnología, la forma en que nuestros datos personales se utilizan y comparten en nuestra sociedad está en evolución constante. Es en virtud de este avance inexorable, en el año 2010, la Comisión entiende que es esencial adaptarse al mismo, y con el objetivo de actualizar y unificar el régimen, ésta presenta una iniciativa de proyecto de reglamento. Este documento será la base del posterior en ese momento, y actual RGPD.

1.14 Orientaciones de la Comisión Europea sobre la aplicación directa del Reglamento general de protección de datos.

La Comisión Europea realiza este comunicado, cuyo contenido son una serie de pautas, pretende dar una idea de la necesidad de adaptarse lo antes posible al RGPD ya que, como se expresa en el comunicado, la nueva norma es de aplicabilidad directa. En el mismo comunicado encontraremos los objetivos para las próximas fases.

1.15 Propuesta de Reglamento del Parlamento Europeo y del consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos).

Esta propuesta es el texto que precede y asienta las bases del actual Reglamento General de Protección de Datos. Útil para aquellos que tengan un interés especial en la evolución de la nueva regulación.

1.16 *A Statementon Artificial Intelligence, Robotics and 'autonomous' systems by the European Group of Ethics and Science in New Technologies.*

Este documento de 9 de abril de 2018, nos permite plantearnos la posición de la protección de datos en la Europa de la inteligéncia artificial.

REAL DECRETO NACIONAL COMPLEMENTARIO A LA NORMATIVA DE PROTECCIÓN DE DATOS

1.17 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

2. ADAPTACIÓN DE LA LOPD AL RGPD

2.1 Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal

Con el objetivo de adaptarse al RGPD, el Congreso de los Diputados, con el asesoramiento de la AEPD, redactó el proyecto de ley que, aun por aprobar, se vislumbra su aplicación a partir de los meses finales de 2018.

2.2 Informe de la AEPD sobre el Anteproyecto de la LOPD

El Gabinete Jurídico de la Agencia Española de Protección de Datos emitió el siguiente informe en su función preceptiva virtud de la anterior ley LOPD. En el mismo informe la AEPD dará su opinión sobre una ley en la que ella misma ha intervenido de forma intensa.

2.3 Dictamen del Consejo de Estado sobre el anteproyecto de la LOPD

En este texto el Consejo de Estado tratará proponer soluciones a aquellas cuestiones que puedan erigirse como dudosas o fuera de los principios constitucionales o, que en todo caso, vayan en contra de las disposiciones normativas de rango europeo.

2.4 Informe del Consejo Fiscal al Anteproyecto de Ley Orgánica de protección de datos de carácter personal.

Con arreglo a los principios de colaboración entre órganos constitucionales, han de ser expresadas las consideraciones del Ministerio Fiscal sobre aspectos que afecten a derechos y libertades fundamentales.

3. RESOLUCIONES DE LAS AUTORIDADES DE CONTROL ESPAÑOLAS.

3.1 Agencia Española de Protección de Datos

Procedimiento de Declaración de Infracción de Administraciones Públicas contra consorcio de emergencias de Gran Canaria.

La captación de imágenes a través de cámaras constituye un tratamiento de datos personales donde el responsable de las mismas es quién decide sobre la finalidad, contenido y uso del tratamiento. Este tiene que asegurar que no se capten imágenes de personas a la vía pública ni del espacio de intimidad de trabajadores y, en todo caso, tiene que avisar del uso de videovigilancia por motivos del 20.3 TE.

Procedimiento sancionador de la AEPD contra la Conselleria de Sanitat Universal de la Generalitat Valenciana.

Si los centros sanitarios por actos u omisiones revelan, entre otros, el nombre y el documento nacional de identidad de los pacientes, se considera una vulneración al principio de seguridad, consagrado en la LOPD y la directiva europea, y en la obligación de guardar el secreto profesional

En este caso, la AEPD no impone ninguna sanción económica debido a que la LOPD no prevé sanciones económicas a las Administraciones Públicas.

3.2 Autoritat de Protecció de Dades Catalana

Informe emitido a petición de la Comisión de Garantía del Derecho de Acceso a la Información Pública en el expediente de reclamación contra un Ayuntamiento en relación con una solicitud de acceso a información del padrón municipal de habitants.

La normativa de protección de datos no impide la comunicación de información del empadronamiento al heredero de una persona muerta, aunque estos datos afecten a terceras personas, si no parece que la comunicación de información comporte un perjuicio significativo para el derecho de estas personas y, además, hay un interés legítimo de acceso a la información pública por parte del solicitante.

Dictamen en relación con la consulta de una entidad de derecho público sobre la transferencia internacional de datos personales a sus oficinas ubicadas fuera de Catalunya.

Dejando de lado las comunicaciones de datos destinados a países de la UE, las transferencias pretendidas por la entidad sólo se podrán efectuar si se aportan garantías adecuadas sobre la protección que los datos recibirán a su destino en los términos establecidos al artículo 46 del RGPD. Si los destinatarios no ofrecen un nivel adecuado de protección y no se aplican las excepciones del artículo 49.1 del RGPD, la cesión vulnera la protección de datos.Final del formulari

3.3 Agencia Vasca de Protección de Datos

Dictamen relativo a la cesión de datos obrantes en la aplicación web "gizarte.eus" gestionada por el Gobierno Vasco, a diferentes entes locales para su integración en el "módulo biscaytik".

No existe cesión de datos cuando los entes locales piden que se les devuelva datos que facilitaron a los servicios sociales si la información solicitada coincide con la aportada por los interesados. En caso contrario, se requerirá consentimiento o habilitación legal, a no ser que la información personal fuera estrictamente necesaria para el ejercicio de las competencias de la Administración solicitante, caso en que legalmente se permite la cesión de datos entre administraciones.

Dictamen que se emite en relación a una consulta sobre la cesión de datos del domicilio y del teléfono móvil de empleados públicos a la Tesorería General de la Seguridad Social.

A pesar de que se permite la comunicación de datos entre Administraciones Públicas sin consentimiento de los interesados, no es aplicable cuando la comunicación no se realiza para el ejercicio de competencias idénticas ni versan sobre las mismas materias. En este caso, la solicitud del número de teléfono móvil de empleados públicos requiere el consentimiento del interesado, a pesar de que la Administración consultada, en conformidad con el principio de colaboración entre Administraciones Públicas, podría informar a los empleados públicos afectados de que la TGSS requiere aquellos datos.

4. ANÁLISIS JURISPRUDENCIAL SOBRE LA PROTECCIÓN DE DATOS: TRIBUNAL SUPREMO, TRIBUNAL CONSTITUCIONAL Y TRIBUNAL DE JUSTÍCIA DE LA UNIÓN EUROPEA.

4.1 Tribunal de Justícia de la Unión Europea.

Asunto "X" C-486/12 de 12 de diciembre de 2013. El derecho de la administración a recibir una contrapartida por el ejercicio del derecho de acceso a los datos personales, permitido por el derecho europeo y fijado libremente por los Estados miembros, no podrá exceder el importe del coste de la comunicación de estos datos al usuario que las pida.

Asunto Digital Rights Ireland Ltd C293/12 y C594/12 de 8 de abril de 2014. La conservación de datos por prestadores de servicios por tiempos extensos cuando constituyan medidas necesarias y proporcionadas para fines específicos de orden público, como proteger la seguridad nacional sobrepasa los límites que exige el respeto del principio de proporcionalidad en relación con el derecho al respeto a la vida privada y a la libertad de expresión de la Carta de Derechos Humanos.

Asunto Google Spain, C-131/12 de 13 de mayo de 2014. La la actividad de un motor de busca tiene que considerarse un tratamiento de datos cuando cuente datos de carácter personal, el gestor de un motor de busca **tiene que considerarse responsable de este tratamiento y el derecho al**

olvido lo obliga a eliminar de la lista de resultados aquella búsqueda a partir del nombre de un usuario, a pesar de que esta información sea lícita en si misma.

Asunto Minister voor Immigratie, Integratie en Asiel C-141/12 y C-372/12, de 17 de julio de 2014. El derecho de acceso del usuario que tramita una solicitud administrativa, respete todos sus datos personales que sean objeto del tratamiento, comporta que se lo tiene que facilitar una idea completa de estos datos en forma inteligible, permitiéndole conocerlas y comprobar que son exactas y tratadas en conformidad con el derecho europeo con objeto de que pueda, si procede, ejercer los derechos pertinentes.

Asunto František Ryneš C-212/13 de 11 de diciembre de 2014. La utilización de un sistema de cámara de vídeo, que da lugar a la obtención de imágenes de personas que luego se almacenan en un dispositivo de grabación continuada, como un sistema de videovigilancia instalado por una persona física en su vivienda familiar con el fin de proteger los bienes, la salud y la vida de los propietarios de la vivienda y cuya vigilancia cubre también el espacio público, no constituye un tratamiento de datos efectuado en el ejercicio de actividades exclusivamente personales o domésticas a efectos de la Directiva 95/46/CE.

4.2 Tribunal Constitucional

Auto 29/2008 de 28 de enero . La protección de datos profesionales y salariales, estas tienen carácter personal como *"todas aquellas que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil[...] o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza"* implica que los órganos públicos tienen obligación de denegar cualquier solicitud de aquellas cuando no sea proporcionada, no lo autorice una ley o no responda a una necesidad justificada.

Sentencia 17/2013 de 31 de Enero. La licitud de cesión interadministrativa de datos cuando así lo permite una ley, la Ley Orgánica de derechos y libertades de los extranjeros prevé esta cesión si existiendo un determinado expediente es necesaria la información especifica que obra en manos de otro órgano de la Administración Pública y por lo tanto, si no se trata de una transmisión masiva o indiscriminada de datos.

Sentencia 29/2013 de 11 de febrero. La facultad de saber en todo momento quién dispone de los datos personales y con qué finalidad, es un "elemento característico de la definición constitucional del arte. 18.4 CE, de su núcleo esencial". Es un derecho de información del usuario que opera, incluso, cuando hay una exigencia legal por *recavar información de carácter personal sin consentimiento de aquel.

4.3 Tribunal Suprem

Sentencia 545/2015 de 15 de octubre. **El derecho al olvido: La caducidad de la acción al derecho al olvido** se inicia cuando el perjudicado conoce el fin del tratamiento puesto que los daños que deriven de este se consideran daños continuados en el tiempo. El ejercicio de este derecho también **se aplica a los tratamientos de datos por hemerotecas digitales** pues van *"perdiendo su justificación a medida que transcurre el tiempo si las personas concernidas carecen de relevancia pública y los hechos, vinculados a estas personas, carecen de interés histórico".*

Sentencia 1455/1960 de 20 de junio de 2016. El contenido derecho al olvido comporta: Un deber del responsable a *"adoptar todas las medidas razonables"* para suprimir o rectificar datos que o bien no responden a periodos necesarios y a hasta específico o bien no son exactas, necesarias y actualizadas y**, a la vez, un derecho** del usuario a oponerse a su tratamiento. Se considerará **responsable a todo aquel que colabore a un tratamiento** cuando su actividad sea ***"indispensable para el funcionamiento"*** de este.

Sentencia 1749/2016 de 13 de julio de 2016. La administración y el derecho a requerir ciertos datos a entidades privadas, el artículo 11.1 LOPD 15/1999 permite que se puedan transferir datos a terceros cuando una ley así lo autorice y por lo tanto, una solicitud por parte de la Administración Tributaría de información con finalidades fiscales no es un acto lesivo.

Sentencia 2423/2016 de 14 de noviembre.: **Una ponderación entre los derechos de protección de datos y los derecho a la libertad de expresión e información,** implica observar la especial protección que merecen las libertades de expresión y de información sobre el resto de derechos fundamentales que *"se proyecta también sobre el derecho a la protección de datos de carácter personal"* -a pesar de que esto- *"no significa que en todos los casos de conflicto tenga que predominar".*

5. ARTÍCULOS REFERENTES A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

5.1 Rafael Jiménez Asensio. "Algunas reflexiones sobre la figura del Delegado de Protección de Datos en las Administraciones Públicas"

Publicación: Revista La Administración al Dia.
Estudios y comentarios. 18 de enero de 2018.

Resumen: Falta poco para la plena aplicabilidad del Reglamento (UE) 2016/679 y este artículo trata la pretensión de esta entrada y enmarca el problema centrándose sobre todo en la figura del Delegado de Protección de Datos. El artículo analiza el estatuto jurídico del Delegado de Protección de Datos; el nivel orgánico quedebería tener y cómo se deberían cubrir estos singulares puestos de trabajo, señalando con todo los nuevos retos de las administraciones públicas.

5.2 Enrique Rubio Torrano. "Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal"

Publicación: Revista Doctrinal Aranzadi Civil-Mercantil num.1/2018 parte Legislación.
Editorial Aranzadi, S.A.U., Cizur Menor. 2018.

Resumen: "El 10 de noviembre de 2017, el Consejo de Ministros aprobó el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, una vez procedido al trámite de envio al Consejo de Estado, que llevó a cabo las correspondientes observaciones al texto presentado y que, al hilo de

las mismas, experimentó algunas modificaciones. El texto fue sometido al correspondiente procedimiento legislativo tras su ingreso en el Congreso de los Diputados (Boletín Oficial de las Cortes Generales. Congreso de los Diputados, 24 de noviembre de 2017). El comentario que sigue encuadra la nueva Ley Orgánica en el marco normativo y jurisprudencial europeo y español."

5.3 Miguel Ángel Ácero. "España es una referencia en la legislación sobre la protección de datos"

Publicación: Vlex
Id. vLex: VLEX-554490454

Resumen: Miguel Ángel Acero es experto en innovación y tecnología de CTIC Centro Tecnológico, y experto en e-commerce (comercio electrónico) y seguridad digital entre otras materias, todas ligadas a las nuevas tecnologías de la información y la comunicación. En el presente analiza la situación actual del uso de la red y sus consecuencias. "Cuando utilizamos las redes sociales facilitamos información sobre nosotros y autorizamos a las grandes corporaciones a que la usen".

5.4 Lucia Salvador Alamar. "La protección de datos"

Publicación: Vlex
Id.Lex:VLEX-695713969

Resumen: Dos años pasan volando. Se aproxima el plazo de dos años concedido por el Reglamento Europeo de Protección de Datos [Reglamento (UE) 201 6/679] a todas las empresas u organizaciones establecidas en la Unión Europea, públicas o privadas, que recaben o traten datos personales de personas físicas en el desarrollo de su actividad para adaptarse a esta nueva normativa, que será de plena aplicación a partir del 25 de mayo de 2018.

5.5 Ana Isabel Herrán Ortiz. "Aproximación al derecho a la protección de datos personales en Europa. El reglamento general de protección de datos personales a debate"

Publicación: R.E.D.S.núm.8, enero-julio 2016
ISSN:2340-4647

Resumen: Recientemente se publicaba el esperado Reglamento General de Protección de Datos en la Unión Europea. Mucho tiempo se ha tenido que esperar hasta la aprobación de esta norma, y muchas han sido las expectativas jurídicas que este texto había generado. Pretendemos en este trabajo presentar unas breves notas que analicen algunas de las novedades más significativas de este Reglamento, que si bien no será aplicable hasta 2018, exigirá, como tendremos ocasión de explicar, un gran esfuerzo de los Estados miembros para adaptar su derecho nacional al nuevo contexto legal europeo en protección de datos personales.

5.6 Concepción Campos Acuña, "Los 7 imprescindibles en protección de datos para el ámbito local", El Consultor de los Ayuntamientos y Juzgados, enero 2018

Publicación: LA LEY *828/2018*

Resumen: En el presente artículo, examinamos los 7 imprescindibles a tener en cuenta por las Entidades Locales para dar cumplimiento a las previsiones recogidas en el Reglamento Europeo de Protección de Datos, aplicable a partir de una fecha próxima: 25 de mayo de 2018.

5.7 Noticia sobre la reprimenda de la AEPD al creador de un grupo de WhatsApp il·legal

Publicación: Vlex
Id.Lex: VLEX-694748717

Resumen: La Agencia de Protección de Datos amonesta a un restaurante mallorquín por elaborar un listado con los datos de los clientes que reservaron una mesa.

6. LIBROS DE RECIENTE PUBLICACIÓN RELACIONADOS CON EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS.

1. Reglamento General de Protección de Datos

Jose Luis Piñar Aragoneses, 2016. Editorial Reus.

Reseña del editor: "Este libro es la primera obra colectiva en España, y seguramente en Europa, sobre el nuevo Reglamento Europeo de Protección de Datos. En él se desgranan las principales novedades que incorpora la nueva normativa, que será plenamente aplicable a partir de mayo de 2018. [...]Incorpora, entre otras cuestiones, nuevos principios como el privacy by default, privacy by design o el principio de responsabilidad proactiva (accountability); derechos nuevos como el derecho al olvido o el derecho a la portabilidad; regula e impulsa la figura del Delegado de Protección de Datos (DPO), importante novedad para nuestro país."

2. Claves prácticas para la protección de datos: Protección de Datos Personales: adaptaciones necesarias al nuevo Reglamento europeo

Luis Felipe López Álvarez, 2017. Editorial Francis Lefebvre.

Reseña del editor:"[...] Esta nueva monografía de la colección Claves Prácticas resulta imprescindible para quienes ejerzan el puesto de Delegado de Protección de Datos, pero también para startups, servicios de cloud computing, empresas, abogados, profesionales, Administraciones Públicas y, en general, para cualquier que, de una forma u otra, esté afectado por la normativa de protección de datos, o por quien pretenda iniciarse en la materia. [...]En resumen, un manual de marcado carácter práctico, que expone lo que hay y lo que viene, un texto de fácil consulta indispensable para quien tenga que gestionar el día a día de la protección de datos de carácter personal."

3. Practicum Protección de Datos 2018

Javier. Álvarez Hernando, 2017. Editorial Aranzadi.

Reseña del editor: "Estudio de los asuntos más relevantes en materia de protección de datos personales desde una

perspectiva jurídica, de una forma sencilla y estructurada, incluyendo, los ficheros de morosidad; videovigilancia; tratamientos de datos de abogados y procuradores; comunidades de propietarios, centros de salud, Administración Pública y centros de formación. [...]."

4. Nuevo Reglamento Europeo de Protección de Datos Versus Big Data

Faustino Gudín Rodríguez Magariños, 2018. Editorial Tirant lo Blanch

Reseña del editor: "[...[] No es este el caso, pocas regulaciones han sido tan aclamadas como necesarias como el nuevo Reglamento. Con esta norma, de aplicación directa y prevalente para todos los ciudadanos de la Unión, Europa se erige en una potencia mundial un marco de referencia mundial y, a la par, se postula como quizás la sociedad democrática más avanzada. En consecuencia, conocer y saber utilizar esta importantísima normativa se nos antoja tanto un deber del jurista como una necesidad ciudadana. No obstante, este capital instrumento normativo sólo puede ser apropiadamente comprendido y calibrado, dentro del complejo acervo normativo y jurisprudencial que le confiere su verdadero sentido."

5. El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos

José López Calvo, 2018. Editorial Bosch.

Reseña del editor: "[...] La presente obra, coordinada por José López Calvo, realiza un examen exhaustivo de su texto, así como del proyecto de ley de Protección de Datos de Carácter Personal que aprobó el Consejo de Ministros el 10 de noviembre de 2017. Del mismo modo y gracias a la participación de un equipo de autores de reconocido prestigio y probada solvencia, se incorpora la perspectiva y el criterio de las principales instituciones, sectores y operadores implicados que analizan la trascendencia sectorial del nuevo marco regulatorio. Finalmente, la obra se completa con aportaciones eminentemente prácticas que trasladan experiencias concretas para facilitar la implantación del nuevo marco."

6. Una revisión del derecho fundamental a la protección de datos de carácter personal

Mónica Martínez López Sáez, 2018. Editorial Tirant lo Blanch

Reseña del editor: "[...] El presente estudio ha procurado analizar la situación actual y los avances recientes, a nivel normativo y jurisprudencial, para moldear y reforzar el derecho fundamental a la protección de datos de carácter personal, como respuesta al imparable progreso tecnológico-digital. Se pretende, por lo tanto, identificar, por un lado, los diferentes sistemas de protección, así como las sinergias y lagunas jurídicas existentes en el ámbito del derecho de la protección de datos en la Unión Europea y el Consejo de Europa, y por otro, dar respuesta a los retos a los que se enfrenta para el establecimiento de un sistema de protección efectiva."