Junta de Castilla y León

eclap

JORNADA

APLICANDO LA NUEVA NORMATIVA SOBRE PROTECCIÓN DE DATOS

VALLADOLID, 17 DE OCTUBRE 2018

LAS OBLIGACIONES DE LOS EMPLEADOS PÚBLICOS EN MATERIA DE PROTECCIÓN DE DATOS

Marta Abad Gutiérrez
Delegada de Protección de Datos
Consejería de Agricultura y Ganadería

Junta de Castilla y León

eclap
Escuela de Administración Pública de Castilla y León

LAS OBLIGACIONES DE LOS EMPLEADOS PÚBLICOS EN MATERIA DE PROTECCIÓN DE DATOS

Marta Abad Gutiérrez

Coordinadora de Servicios de la Secretaría General.
Delegada de Protección de Datos.
Consejería de Agricultura y Ganadería.
Junta de Castilla y León.

1 INTRODUCCIÓN (recordamos conceptos ya explicados)

1.1 ¿POR QUÉ UNA NUEVA REGULACIÓN EUROPEA?

El **RGPD es de aplicación desde el 25 de mayo de 2018.** Al tratarse de un Reglamento no necesita transposición al ordenamiento jurídico español, por lo que su contenido es directamente aplicable.

→ **En el ámbito europeo, el RGPD desplaza la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995**, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Esta Directiva regulaba un derecho a partir de una competencia económica porque la UE no tenía base legal para regular esta materia.

La Directiva no fue traspuesta por igual en todos los Estados miembros. España la traspuso con la LOPD, que no contiene ni una sola mención al artículo 18.4 CE. A partir de la LOPD, en España la autoridad de control, investiga y sanciona. En otros países no es así,

lo que determinó que muchas compañías optaran por instalarse en otros países.

En 2008, la Carta de Derechos Fundamentales de la UE reconoce el derecho a la protección de datos independiente del derecho a la intimidad y en 2009, el Tratado de Lisboa reconoce este derecho como un derecho privado. De esta forma, al incorporarlo a este Tratado, está habilitando a la UE para regular este derecho.

Y aquí surge el RGPD. De esta forma, **el derecho a la protección de datos se ha convertido en un derecho europeizado**. Las autoridades nacionales siguen teniendo las mismas competencias pero las deben coordinar con las europeas. Los Tribunales nacionales tienen que interpretar este derecho conforme al derecho europeo. Es el TJUE el que fija la interpretación vinculante.

→ **En cuanto a nuestra normativa, el RGPD desplaza a la Ley Orgánica 15/1999,** de 13 de diciembre, de protección de datos de carácter personal y su reglamento de desarrollo. Esta es la terminología correcta, el RGPD desplaza la LOPD, no la deroga, la desplaza, aunque la regulación sea idéntica, debemos citar el RGPD. La LOPD se aplica en todo lo no regulado por el RGPD.

→ **Es un derecho expuesto a los grandes retos derivados de la tecnología.**

El foco central de preocupación del RGPD es el riesgo que para la protección de derechos fundamentales y, en especial, la protección de datos de las personas físicas se puede producir como consecuencia del tratamiento masivo de datos, del cruce de esos datos dirigido a la elaboración de perfiles y de las observaciones masivas de los datos.

El RGPD se dicta para dar respuesta no solo a los retos presentes sino en especial también para hacer frente a los grandes desafíos del futuro en materia de protección de datos.

¿Cómo se adelanta al futuro el RGPD? ¿En qué clave hay que leer el RGPD? La normativa reguladora de la protección de datos hasta ahora ha sido represiva y ahora el planteamiento es proactivo. El RGPD no parte de una configuración de medidas de seguridad en función de si atendiendo a los diferentes tipos de tratamiento les corresponde unas medidas de seguridad de nivel bajo, medio o alto, sino que tendrá que partir de un análisis de riesgo inicial de los tratamientos y a partir de los resultados obtenidos, se implementan las medidas de seguridad. Es el principio de proactividad.

1.2 ¿EL RGPD SE APLICA ÍNTEGRAMENTE A LA ADMINISTRACIÓN?

Desde el 25 de mayo de 2018 el RGPD es norma directamente aplicable en su integridad a las Administraciones Públicas y a las entidades del sector público. Y aunque pudiera parecer que eso de la mercadotecnia "no se da" en la Administración, el uso cada vez más frecuente de tecnologías de la información y la comunicación o la generalización de servicios "en nube" supone que aumenten las posibilidades de que se trasfieran estos datos fuera del Espacio Económico Europeo.

La Administración está avanzando mucho en la digitalización de sus tareas, lo siguiente será al automatización a partir de ahí, el riesgo de brechas de seguridad en los tratamientos de protección de datos puede ir en escalada, de ahí la importancia de que llevemos a cabo un análisis de riesgos en cada momento.

→ En conclusión, **lo que está en juego es la protección de un derecho fundamental** y precisamente, como tantas veces hemos oído a Manuel Arenilla: **"La razón de ser de los funcionarios es ser garantes de derechos y libertades".** Lo que está en riesgo aquí es el mismo juego democrático. Pensemos en las últimas elecciones americanas, lo que está pasando en Rusia o en Cataluña…

Por eso es tan importante conocer cuáles son nuestras obligaciones y cumplirlas.

2 OBLIGACIONES DE LOS EMPLEADOS PÚBLICOS RESPECTO DEL TRATAMIENTO DE DATOS PERSONALES

2.1 CONTRIBUIR A CREAR UN CULTURA ORGANIZATIVA DE PROTECCIÓN DE DATOS

Nosotros no vamos a hacer política en materia de protección de datos pero sí debemos contribuir a que forme parte de nuestra cultura organizativa la protección de datos personales. Al igual que cuando diseñamos un nuevo procedimiento pensamos en aplicarle toda la normativa en materia de Administración electrónica o hacemos las evaluaciones de impacto que correspondan, debemos analizar si ese procedimiento/actuación conlleva una actividad de tratamientos de datos novedosa y si es así, adoptar las medidas previstas en el RGPD.

2.2 TENER LOS CONCEPTOS CLAROS

→ **¿Qué es un dato de carácter personal?** Toda información sobre una persona física identificada o identificable ("el afectado").

Por tanto, la información debe ser concerniente a una persona física.

Se excluyen las personas jurídicas y las fallecidas. Las personas jurídicas pueden entrar en su ámbito de aplicación si coinciden con una persona física. En cuanto a las personas fallecidas, cosa distinta es la relevancia que puedan tener los datos de un fallecido cuya información puede impactar sobre familiares vivos.

En definitiva, que sea **un dato personal no depende del soporte ni de la fuente, lo importante es que verse sobre una persona.**

Además, el criterio de "identificabilidad" significa que no depende de la intención del responsable decir si es o no un dato personal, se trata de una visión objetiva. **Si ese dato conectado con otro hace posible identificar a una persona, es un dato personal.**

Un dato o es personal o es anónimo. Es un concepto binario.

¿Qué son las "categorías especiales de datos personales"?

- Los datos de salud.
- Los que revelen ideología, afiliación sindical, religión y creencias.
- Los que hagan referencia al origen racial o a la vida sexual.
- Los que se refieren a la comisión de infracciones penales o administrativas.

Ejemplos de categorías de datos personales objeto de tratamiento por la Administración:

- De carácter identificativo: nombre, apellidos, teléfono, imagen, DNI/NIE/NIF
- Académicos y profesionales (en la gestión de procedimientos selectivos, bolsas de empleo, recursos humanos)
- En el ejercicio de la potestad sancionadora (aquellos derivados de la tramitación de expedientes sancionadores)

- Categorías especiales de datos (origen racial, salud o vida sexual en un servicio de atención a mujeres víctimas de violencia de género o en la prestación de servicios sociales)
- De carácter tributario.
- La implementación de las "Smart cities" o apps diversas también pueden conllevar un tratamiento de diferentes datos de carácter personal.
- Los datos de acceso a nuestras web debemos tratarlos como datos personales porque ante un posible, conflicto de intereses, los Tribunales van a poder identificar al interesado.
- Las cookies, el archivo en sí mismo no es vincular a una persona, si posteriormente se hace una compra, las cookies hacen un seguimiento de las actividades del interesado y se han convertido en un dato personal.

¿Qué es un tratamiento de datos de carácter personal? Cualquier actividad en la que estén presentes datos de carácter personal ya se realice de manera manual o automatizada. Desde la **recogida** hasta la **destrucción**. Se incluyen el **acceso de terceros** a los datos que nosotros hemos recogido y **nuestro acceso a los datos que terceros** han recogido.

Ejemplos de tratamientos de datos por la Admón.:

- Subvenciones y ayudas
- Padrón municipal de habitantes
- Sanciones
- Gestión de impuestos y tributos
- Recursos humanos: acceso, concursos, bolsas de trabajo…
- Registro de documentos
- Servicios sociales
- Gestión económica: pago de facturas

¿Quién es el responsable del tratamiento?

Debe ser un directivo de la estructura orgánica de nuestra organización.

La carga sancionadora recae sobre el responsable del tratamiento.

Están omnipresentes en todo el RGPD y en el caso de las AAPP la consecuencia negativa que conlleva el incumplimiento del RGPD es que sea apercibido y que este incumplimiento se haga público con nombres y apellidos.

Es quién debe decidir sobre las medidas técnicas y organizativas aplicables al tratamiento a fin de poder garantizar y demostrar que se cumple el RGPD.

¿Quién es el encargado del tratamiento? Es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos por cuenta del responsable del tratamiento.

Ejemplos en la Administración:

- La empresa del servicio de mailing
- La empresa que destruye la documentación
- El control de las cámaras de videovigilancia
- Mantenimiento de los equipos informáticos

Es otro de los actores fundamentales de la responsabilidad proactiva.

En el RGPD la mayor parte de las obligaciones son para ambos, el responsable y el encargado.

El encargado debe ofrecer garantías suficientes de que cumple el RGPD. Entre la forma de demostración: la adhesión a códigos de conducta o la obtención de certificados de protección de datos.

Se exige que exista un contrato por escrito entre responsable y encargado.

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.

Puntualizaciones:

- **¿Interesado o afectado?** La AEPD recomienda utilizar la palabra "afectado" y no la de "interesado", para no incurrir en confusión con la terminología establecida en la Ley 39/2015, de 1 de octubre.
- **Los conocidos como "consentimientos tácitos"** han dejado de ser válidos desde la entrada en vigor del RGPD.
- **El consentimiento puede ser** para uno o varios fines, **debe ser** prestado de forma libre, es revocable, el responsable debe probar en todo momento que ha obtenido el consentimiento; se debe utilizar un lenguaje claro y sencillo.
- **El consentimiento de los menores.** El RGPD remite a que los Estados miembros puedan establecer por ley el consentimiento de los menores siempre que la edad no sea inferior a 13 años ni superior a 16. En la actualidad la edad está fijada en 14 años.

→ **Violación de la seguridad de los datos personales.** Toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

→ **Autoridad de control.** En España, la AEPD.

2.3 LOS PRINCIPIOS QUE SE DEBEN TENER EN CUENTA EN TODO TRATAMIENTO DE DATOS PERSONALES

El cumplimiento de estos principios genera deberes jurídicos para los responsables de tratamientos en las AAPP. Por tanto, el cumplimiento de tales principios interesa especialmente a la Administración Pública.

Licitud (legalidad), **lealtad** (buena fe, que el interesado sepa que se está haciendo un tratamiento de sus datos) **y transparencia.** El tratamiento solo será lícito si cumple una de estas condiciones (artículo 6 RGPD):

- El interesado dio su consentimiento.
- El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte.
- El tratamiento es necesario para cumplir una obligación legal del responsable del tratamiento.
- El tratamiento es necesario para proteger los intereses vitales del interesado o de otra persona física.
- El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
- El tratamiento sea necesario para la satisfacción de un interés legítimo del responsable del tratamiento.

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.

Importante: El RGPD no prohíbe tratar datos para fines distintos de los definidos inicialmente sino para fines incompatibles.
El nuevo fin debe cumplir las mimas condiciones que el fin originario y hay que comunicarlo al interesado.
Tener en cuenta lo que dice el considerando 50 que incluye el **criterio de la expectativa razonable del interesado**. Que el interesado pueda prever que sus datos también se van a recabar para ese otro fin.
La seudonimización es una garantía que puede justificar el cambio de finalidad.

→ **Minimización de los datos.** Debemos tratar solo los datos estrictamente necesarios.

A cumplir con este principio se dirige la disposición adicional novena del PLOPD.

→ **Exactitud.**

→ **Limitación del plazo de conservación.** Los datos personales serán mantenidos de forma que 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 periodos más largos siempre que se traten exclusivamente con fines de archivo, **fines de investigación científica o histórica o fines estadísticos**.

→ **Integridad y confidencialidad.** Recordar que el **artículo 53 TREBEP enumera entre los principios éticos, aplicables a los empleados públicos**, **guardar secreto de las materias clasificadas u otras cuya difusión esté prohibida legalmente**, manteniendo la debida discreción sobre aquellos asuntos que conozcan por razón de su cargo, sin que puedan hacer uso de la información obtenida para beneficio propio o de terceros, o en perjuicio del interés público.

IMPORTANTE: El personal de la Administración no podemos hacer uso del acceso que tenemos a datos personales de los ciudadanos en la gestión de una actividad de tratamiento, para resolver sobre otra actividad de tratamiento distinta.

2.4 NUESTRAS OBLIGACIONES RESPECTO DEL TRATAMIENTO DE DATOS SURGEN DE LOS PRINCIPIOS SEÑALADOS Y ESPECIALMENTE DEL PRINCIPIO DE RESPONSABILIDAD PROACTIVA

El RGPD ofrece un nuevo modelo de cumplimiento en materia de protección de datos, frente al modelo represivo anterior ("compliance"), orienta todo su contenido a promover la cultura proactiva de la confidencialidad, que se traduce en que los responsables estén en todo momento en disposición de demostrar ante la autoridad de control que cumplen el RGPD. Es la manifestación del término inglés "accountability", cuya forma más efectiva de acreditar su cumplimiento es documentar todas las actuaciones que se realicen en materia de protección de datos.

El hecho cierto de que la AEPD pueda publicar los nombres y apellidos de los responsables que han incumplido la normativa en materia de protección de datos, hará que, más pronto que tarde, la responsabilidad se traslade hasta el gestor de los datos personales, de ahí la importancia de que conozcamos nuestra obligaciones y cumplamos diligentemente.

La primera gran manifestación de la responsabilidad proactiva se traduce trasladar los principios enunciados a la **protección de datos desde el diseño** y **protección de datos por defecto**.

→ **Protección de datos desde el diseño.** La protección de datos ha de estar presente en las primeras fases de diseño de un procedimiento, una norma, un aplicativo informático… y forma parte de la lista de elementos a considerar antes de iniciar las sucesivas etapas de desarrollo. Este requisito se va a traducir en medidas técnicas y organizativas.

La implementación del tratamiento afecta desde los productos hardware o software hasta las máquinas o las personas.

La obligación de que se adopten los principios de privacidad desde el diseño recae en el responsable del tratamiento.

Un ejemplo de estas medidas es la **seudononimización** temprana de los datos o la **minimización** de datos.

Privacidad por defecto. Solo deben ser objeto de tratamiento los datos personales que sean estrictamente necesarios para cada uno de los fines del tratamiento, incluso llegar a que no se traten datos de carácter personal.

Estrategias que permiten implementar la privacidad por defecto:

- **El principio de "need-to-know" o "necesidad de conocer"** establece que en una organización las personas han de tener acceso solo a la información precisa para ejecutar sus tareas.
- **Recogida de datos:** Analizar los tipos de datos que se recaban con un criterio de minimización en función del servicio que se presta al usuario.
- **Tratamiento de datos:** Analizar los procesos asociados a dichos tratamientos para que se acceda a los mínimos datos personales necesarios para ejecutarlos.
- **Conservación:** Implementar una política de conservación de datos que permitan eliminar los datos que no sean estrictamente necesarios.
- **Accesibilidad:** Limitar el acceso por parte de terceros a dichos datos personales.

IMPORTANTE: Siempre debemos estar en disposición de demostrar a la autoridad de control que cumplimos con estos principios. Por tanto, se convierte en una obligación documentar, documentar y documentar.

Manifestaciones de la responsabilidad proactiva en los funcionarios que podemos documentar debidamente:

CONOCER QUIÉN ES EL/LA DELEGADO/A DE PROTECCIÓN DE DATOS DE NUESTRA ORGANIZACIÓN. CUÁLES SON SUS FUNCIONES Y CUÁNDO DEBO ACUDIR A ÉL/ELLA

- **Contar con su asesoramiento sobre los tratamientos de datos** que gestionemos, especialmente antes de iniciar el tratamiento.
- **Contar con su asesoramiento al efectuar el análisis de riesgo y evaluaciones de impacto.**
- **Cooperar** en la realización de sus tareas.

ESTABLECER EL REGISTRO INTERNO DE TRATAMIENTOS Y COLABORAR EN SU MANTENIMIENTO

- **Desaparece la exigencia de creación de los ficheros y tratamientos mediante una disposición de carácter general, publicada en un diario oficial y su notificación a la AEPD.**
- **El RGPD establece la necesidad de llevar un registro interno de actividades de tratamiento.** Como instrumento primordial para demostrar el cumplimiento y facilitar la supervisión de los tratamientos.
- **Debe llevarse tanto por los responsables como por los encargados de tratamiento.**
- **Debe estar por escrito, incluso en formato electrónico.**

→ **Debe mantenerse actualizado y a disposición de la autoridad de control.**

→ **Debe incluir una descripción de los tratamientos de datos.**

Por ejemplo: Si los datos se utilizan para el cobro del impuesto de vehículos y para informar sobre una campaña informativa sobre la contaminación producida por los vehículos, existirían dos tratamientos de datos: uno relativo al cobro del impuesto y otro referente a la campaña informativa.

→ **El RGPD establece el contenido mínimo de información:**

- Administración
- Actividad de tratamiento
- Fines del tratamiento
- Nombre y datos de contacto del DPD
- Categorías de datos personales
- Categoría de afectados
- Descripción de las medidas técnicas y organizativas de seguridad
- Categorías de destinatarios de comunicaciones, incluidos terceros países u organizaciones internacionales.
- Transferencias internacionales. Documentación de garantías adecuadas del artículo 49.1
- Cuando sea posible, plazos previstos para la supresión de las diferentes categorías de datos.

→ **Como medida de transparencia, las AAPP harán público su inventario de actividades de tratamiento**, accesible por medios electrónicos.

2.4.2 REVISAR LA LEGITIMIDAD DE LOS TRATAMIENTOS

→ **Las AAPP deben identificar con precisión las finalidades y la base jurídica de los tratamientos.** Esta obligación deriva de:

- La necesidad de cumplir con el principio de legalidad establecido en el RGPD.
- La información a proporcionar a los interesados (transparencia).
- Su constancia en el registro de actividades de tratamiento.

→ **La primera pregunta que debemos hacernos es** si hay base jurídica para llevar a cabo el tratamiento de datos. Si hay base, el tratamiento es posible. Si no hay base jurídica, el tratamiento debe eliminarse.

→ **El interés legítimo** no se aplica en la Administración.

→ **La identificación de finalidades y bases jurídica tiene exigencias adicionales en el caso en que se traten datos de los considerados como objeto de especial protección**, entre otros, salud, ideología, religión o pertenencia étnica. El tratamiento de estos datos está prohibido y solo podrá llevarse a cabo si es aplicable alguna de las excepciones previstas en el artículo 9.2 RGPD.

→ **En el caso de las AAPP será muy habitual que la base jurídica de los tratamientos sea el cumplimiento de una tarea en interés público o el ejercicio de poderes públicos.** Tanto el interés público como los poderes públicos que justifican el tratamiento deben estar establecidos en una norma de rango legal.

→ **El tratamiento puede estar basado en el consentimiento**, pero en la Administración debemos restringir el consentimiento lo más posible. La carga de la prueba corresponde al responsable. El responsable debe estar en condiciones de demostrar el consentimiento.

→ **Si tratamos datos especiales** no podemos utilizar las bases del artículo 6 debemos utilizar las bases del artículo 9.2.
Aún en este caso debemos restringir el uso del consentimiento como base jurídica legitimadora del tratamiento. La base jurídica debe ser la prevista en las letras h) e i) del artículo 9.2.

→ **En el caso de transferencias de datos a terceros países,** el RGPD exige la existencia de instrumentos jurídicamente vinculantes y exigibles entre autoridades y organismos públicos. Los acuerdos administrativos requerirán autorización de la autoridad de control.

REVISAR LOS CONTRATOS CON ENCARGADOS DE TRATAMIENTOS

→ **El RGPD establece que la relación entre responsables y encargados deberá formalizarse siempre mediante un contrato o acto jurídico que vincule al encargado.**

→ **El RGPD establece una obligación de diligencia debida en la elección de los encargados de tratamiento** por parte de los responsables, contratando únicamente encargados que estén en condiciones de cumplir con el RGPD.

→ **En el caso de las AAPP será frecuente que el encargado de tratamiento se establezca mediante actos jurídicos**, por ejemplo en

la norma de creación de órganos encargados de la prestación de servicios informáticos.

→ **Será necesario revisar y adecuar los contratos de encargo actualmente suscritos** para contemplar el contenido mínimos que exige el RGPD.

2.4.5 REVISAR LA INFORMACIÓN QUE SE OFRECE A LOS INTERESADOS

→ **La información que se ofrece a los interesados cuando se recogen sus datos (por ejemplo, en formularios web o papel o de un tercero) debe revisarse,** pues se ha reforzado la transparencia hacia el interesado, siendo la información a facilitar más amplia que la requerida hasta ahora.

→ **La información** a los interesados, tanto respecto a las condiciones de los tratamientos que les afectan como en las respuestas a los ejercicios de derechos, **deberán proporcionarse de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.**

→ **Se deberán evitar las fórmulas especialmente farragosas** y que incorporan remisiones a los textos legales.

→ **Las cláusulas informativas deberán explicar el contenido al que inmediatamente se refieren de forma clara y accesible a los interesados**, con independencia de sus conocimientos en la materia.

→ **Se establece una lista exhaustiva de la información que debe proporcionarse a los interesados** (más amplia que la que actualmente contiene la LOPD) y que incluye:

- Base jurídica del tratamiento.
- Intención de realizar transferencias internacionales.
- Datos del Delegado de Protección de Datos (si lo hubiera)
- 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 añade la fuente de la que proceden los datos personales** y, en su caso, si proceden de fuentes de acceso público.

→ **La información a los interesados deberá facilitarse por escrito**, incluidos los medios electrónicos cuando sea apropiado.

→ La importancia que el RGPD concede a la claridad y accesibilidad de la información se refleja en el hecho de que prevé que pueda proporcionarse en combinación con **iconos estandarizados** que ofrezcan una visión de conjunto del tratamiento previsto. El diseño de estos iconos deberá hacerlo la Comisión Europea.

→ Con el fin de facilitar el cumplimiento del derecho a la información en la recogida de datos personales, **la AEPD recomienda adoptar un modelo de información por capas o niveles:**

- Presentar la información básica en un primer nivel:
  - de forma resumida,
  - en el mismo momento y

- en el mismo medio de recogida
- Remitir a información adicional en un segundo nivel:
  - de forma detallada,
  - en un medio más adecuado para su presentación, comprensión y archivo.

EJERCICIO DE LOS DERECHOS DE LOS INTERESADOS

El RGPD mantiene y amplía los tradicionales derechos ARCO (acceso, rectificación, cancelación y oposición).

Derecho de acceso:

- No confundir con el **derecho de acceso de los interesados a los expedientes administrativos** que regula la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las AAPP, ni con **el derecho de acceso regulado en la Ley 19/2013, de 9 de diciembre, de transparencia**, acceso a la información pública y buen gobierno.

- **El acceso a la historia clínica** se regula por la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, si bien la AEPD es competente para atender este acceso en caso de que una vez ejercitado, la respuesta no sea satisfactoria para el ciudadano, o no se haya respondido.

- Antes debían facilitarse todos los datos de base del afectado, pero no copias o documentos (excepto en el caso de la historia clínica). Ahora **se reconoce el derecho a obtener una copia de los datos personales objeto del tratamiento**.

- **Los responsables podrán atender a este derecho facilitando el acceso remoto a un sistema seguro** que ofrezca al interesado un acceso directo a sus datos personales.

→ Derecho al olvido (derecho de supresión):

- **No es un derecho autónomo o diferenciado de los clásicos derechos ARCO** sino la consecuencia de la aplicación del derecho al borrado de los datos personales.

- **La AEPD fue pionera en considerar que el tratamiento de datos que realizan los buscadores de internet como Google, Bing o Yahoo está sometido a las normas de protección de datos** de la UE, y que los ciudadanos pueden solicitar, bajo ciertas condiciones, que los enlaces a sus datos personales no aparezcan en los resultados de una búsqueda realizada por su nombre y apellidos. Esta tesis de la AEPD fue avalada en 2014 por el Tribunal de Justicia de la UE en el caso Google Spain, afirmando 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.

- **En esencia, el "derecho al olvido" supone** lo siguiente:
  - La aplicación de los derechos de supresión y oposición a los buscadores de internet para impedir la difusión de la información cuando esta es obsoleta o no tiene relevancia ni interés público.
  - Si se estima la pretensión del interesado, la información no aparecerá en los resultados de búsqueda, pero –salvo que el "editor" (fuente original" adopte medidas al respecto- se seguirá publicando en la fuente original.
  - Si los responsables de los buscadores en internet deniegan la pretensión de un interesado, este puede presentar una reclamación ante la AEPD.
  - Los principales buscadores de internet han habilitado formularios para facilitar su ejercicio.

- El interesado puede ejercitar este derecho ante los buscadores sin necesidad de acudir a la fuente original de publicación.
- En cuando a la eliminación de fotos y videos publicados en internet sin el consentimiento del interesado, se puede ejercitar el derecho de supresión. Para ello el interesado debe dirigirse al responsable que haya publicado la información en la red, acreditando su identidad, indicando los enlaces donde aparecen los videos y fotos y solicitando el borrado de los mismos.
- Las redes sociales más populares ofrecen servicios de ayuda que permiten poner en su conocimiento, a través de sus propios formularios, cuándo se ha producido una vulneración de la privacidad o se han volcado contenidos inapropiados.

- Tener en cuenta que **no podrá ejercitarse este derecho** cuando sea necesario, entre otras cosas:
  - Para el cumplimiento de una obligación legal o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.
  - Con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.
  - Para la formulación, el ejercicio o la defensa de reclamaciones.

  Basándose en estas excepciones, la Administración podrá denegar el ejercicio de este derecho.

→ **Derecho de oposición. Referencia a dos supuestos de hecho frecuentes en la Administración:**

- **Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa**, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos

personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia. Es el caso de **la publicidad institucional remitida por una Administración Pública u órgano administrativo**, es posible el ejercicio del derecho de oposición al tratamiento, sin necesidad de que el ciudadano afectado especifique ningún motivo.

- **El ejercicio del derecho de oposición a la publicación de los datos personales del afectado en Boletines o Diarios oficiales**, así como en sitios web institucionales y en otros canales electrónicos o telemáticos administrativos, que podrá fundamentarse en la concurrencia de un motivo legítimo y fundado, referido a una situación personal de dicho afectado y basado en:
  - La elección indebida por parte del responsable del tratamiento, de una forma de publicación de los datos personales que suponga un mayor nivel de publicidad del que dicho afectado deba soportar en atención a las circunstancias concurrentes, siempre que una ley no disponga lo contrario.
  - La publicación por parte del responsable del tratamiento de datos excesivos en atención a la tipología de los mismos y al especial nivel de protección dispensada por el ordenamiento jurídico a los datos personales publicados, siempre que una Ley no disponga lo contrario.
  - El mantenimiento de la publicación de los datos personales por parte del responsable del tratamiento cuando dicha publicación haya dejado de ser necesaria o pertinente para los fines para los cuales se haya realizado.

→ Derecho a la limitación de tratamiento:

- Supone que, a petición del interesado, no se aplicarán a sus datos personales las operaciones de tratamiento que en cada caso corresponderían.

- Este derecho no es absoluto y se podrá llevar a cabo cuando:
  - El interesado ha ejercido los derechos de rectificación u oposición y el responsable está en proceso de determinar si procede atender a la solicitud.
  - El tratamiento es ilícito, el interesado podrá pedir la limitación del uso de los datos en vez de su supresión.
  - Los datos ya no son necesarios para el tratamiento, pero el interesado los necesita 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.
  - La limitación del tratamiento es un derecho de los interesados que no debe confundirse con el bloqueo de datos que existe en la legislación española.

→ Derecho a la portabilidad:

- Es una forma avanzada del derecho de acceso por el cual **la copia que se proporciona al interesado debe ofrecerse en un formato estructurado, de uso común y lectura mecánica**.

- **Solo puede ejercerse cuando:** 1. El tratamiento se efectúe por medios automatizados. 2. El tratamiento se base en el consentimiento o en un contrato. 3. Cuando el interesado lo solicita respecto a los datos que haya proporcionado al responsable y que le conciernen, incluidos los datos derivados de la actividad propia del interesado.

- **En la mayor parte de los tratamientos que realiza la Administración no se cumplen estos requisitos por lo que no puede aplicarse este derecho.**

- **Este derecho implica que los datos personales del interesado se transmiten directamente de un responsable a otro**, sin

necesidad de que sean transmitidos previamente al propio interesado, siempre que ello sea técnicamente posible.

- **No es aplicable:** a los datos de terceras personas que un interesado haya facilitado a un responsable ni cuando el interesado haya solicitado la portabilidad de datos que le incumban pero que hayan sido proporcionados al responsable por un tercero.

Limitaciones de estos derechos:

Estos derechos no son absolutos, pueden limitarse por varios factores:

- Que la limitación tenga una cobertura legal en el derecho de la UE o de los Estados miembros a través de medidas legislativas. Estas medidas serán proporcionadas y respetar en lo esencial los derechos y libertades fundamentales.
- El RGPD acepta la limitación de estos derechos se realiza un referencia a los "objetivos importantes de interés público general" y no solo a los de carácter económico o financiero, así como a la protección de la independencia judicial y a la ejecución de sentencias (si bien se indica –de demandas civiles).

Procedimiento para el ejercicio de estos derechos:

- **Los responsables deben facilitar a los interesados el ejercicio de estos derechos y los procedimientos y las formas para ello deben ser visibles, accesibles y sencillos**. Es necesario que los responsables posibiliten la presentación de solicitudes por medios electrónicos, especialmente cuando el tratamiento se realiza por estos medios.

- **El ejercicio de estos derechos será gratuito** para el interesado, excepto cuando se formulen solicitudes manifiestamente infundadas o excesivamente repetitivas, el responsable podrá

cobrar una tasa que compense los costes administrativos de atender la petición o negarse a actuar. El responsable deberá demostrar el carácter infundado o excesivo de las solicitudes que tengan un coste para el interesado.

- **La solicitud de ejercicio de los derechos debe dirigirse al responsable del tratamiento**. Puede ejercitar su derecho directamente o a través de su representante legal o voluntario nunca a través de una persona jurídica.

- **Es una facultad del interesado acudir al DPD pero el DPD no resuelve su solicitud**, debe resolverla quien tiene atribuida la competencia para dictar resoluciones, el responsable del tratamiento.

- **El interesado debe identificarse en el momento de formular la solicitud** pero si en la resolución del procedimiento del ejercicio del derecho no podemos identificarlo, podemos denegar su petición. No obstante, tener en cuenta que si se trata de un interesado con el que habitualmente nos relacionamos, por teléfono o correo-e no sería muy correcto que le denegáramos su petición por no identificarse.

- **El responsable contestará al interesado en el plazo de un mes** (natural) a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses (siendo un total de tres meses desde la recepción de la solicitud), teniendo en cuenta la complejidad y el número de solicitudes. Solo podrá ampliarse el plazo si la respuesta va ser positiva. Si nuestra respuesta va a ser que no tenemos información o que no podemos informar, no se puede ampliar. En el plazo de un mes desde la recepción de la solicitud, el responsable informará al interesado sobre cualquier prórroga.

- **Si el responsable decide no atender una solicitud, deberá informar de ello**, motivando la negativa, sin dilación y a más tardar, transcurrido un mes desde la recepción de la solicitud.

- **El responsable que trate gran cantidad de información sobre un interesado podrá pedir a este que especifique la información** a que se refiere su solicitud de acceso.

- **El responsable podrá contar con la colaboración de los encargados** para atender al ejercicio de derechos de los interesados, pudiendo incluir esta colaboración en el contrato de tratamiento. En este caso, será el encargado el que responda a la solicitud formulada por el interesado.

- **Es conveniente incorporar la supervisión del DPD cuando se vaya a resolver negativamente**.

- **Frente a la resolución negativa de ejercicio de sus derechos o una falta de respuesta, el interesado puede presentar una reclamación ante la AEPD** y una vez agotada la vía administrativa interponer **recurso** contencioso administrativo **ante la Audiencia Nacional**.

3 OBLIGACIONES DE LOS EMPLEADOS PÚBLICOS RESPECTO DE LAS MEDIDAS DE SEGURIDAD Y VIOLACIONES DE SEGURIDAD

EFECTUAR EL ANÁLISIS DE RIESGOS Y REVISAR LAS MEDIDAS DE SEGURIDAD

→ Otra consecuencia del principio de responsabilidad proactiva (“accountability”) de quienes tratan datos personales, es

determinar qué tipo de medidas se deben aplicar al tratamiento para cumplir con lo dispuesto en el RGPD.

→ **Hasta ahora**, las medidas de seguridad exigibles venían claramente enumeradas en el **Reglamento de Desarrollo de la LOPD** (RD 1720/2007) que establecía **tres niveles de exigencia, básico, medio y alto**.

→ Sin embargo, **el RGPD no establece cuáles han de ser las medidas de seguridad**, sino que indica que: *"Teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo"*.

→ Lo anterior significa que todas las actividades de tratamiento deben ser evaluadas con el objetivo de determinar el potencial riesgo al que están expuestas.

→ Tener claros algunos **conceptos:**

- El **activo:** lo que queremos proteger.
- La **amenaza:** Aquello de lo que queremos proteger el activo.
- El **impacto:** Lo que podemos evitar. Las consecuencias que la materialización de una amenaza puede tener para la imagen de la Administración en la que trabajamos y las consecuencias para el personal implicado.
- La **cuantificación del riesgo**. Es el resultado de multiplicar el impacto que tendría la amenaza por la probabilidad de que esta amenaza llegue a materializarse: RIESGO = IMPACTO x PROBABILIDAD

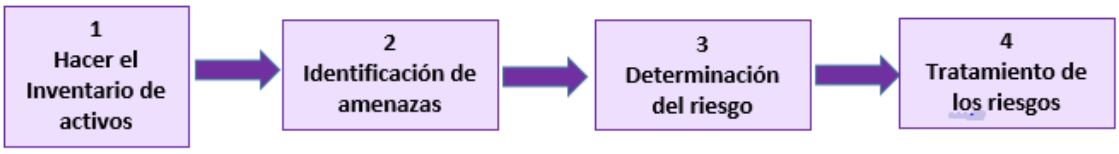
Cuando el impacto es muy alto y la probabilidad de que la amenaza se materialice también es alta, tendremos un riesgo elevado.

Por tanto, los valores serán específicos para cada organización.

→ **Análisis de riesgos.** Los riesgos no son estáticos, evolucionan según el estado de la tecnología y las situaciones de cada tratamiento.

Nos lleva a posicionarnos en nuestra zona de riesgo. Sabiendo que hay:

- Un riesgo tolerable. Acepto ciertos riesgos.
- Un riesgo gestionable. Puedo mitigar el riesgo (pongo una contraseña o evitando la oportunidad de amenaza (en vez de chequear un aplicativo una vez al mes lo hago una vez a la semana).
- Un riesgo inaceptable que me puede llevar a renunciar a algunas actividades o tratamientos.



En la identificación de las amenazas puede valer la creatividad pero en las medidas de seguridad hay poco que inventar, nuestro marco es el ENS.

En el inventario de activos deben incluirse, las instalaciones (edificios, locales, redes de comunicación), equipamientos (mobiliario, maquinaria), sistemas de información, intangibles (licencias, derechos, reputación, imagen), datos de carácter personal.

En las amenazas se incluyen los desastres naturales, las interrupciones de servicios (luz, agua, teléfono), los errores humanos.

Determinación del riesgo. Un ejemplo sencillo con una hoja Excel:

ANÁLISIS DE RIESGOS				
ACTIVO	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
Servidor 01 (Contabilidad)	Fuga de información	2	3	6
Servidor 01 (Contabilidad)	Degradación de los soportes de almacenamiento de la información	1	3	3
Router Wifi (Clientes)	Caída del sistema por sobrecarga	1	2	2
Router Wifi (Clientes)	Denegación de servicio	2	1	2
Servidor 02 (Web)	Denegación de servicio	3	2	6
Servidor 02 (Web)	Corte del suministro eléctrico	1	2	2
...				
	(Añadir a la tabla tantas filas como sea necesario)			

El riesgo es el resultado de multiplicar probabilidad x impacto
El tratamiento de los riesgos. Supone elegir las medidas de seguridad.

→ **Debemos conocer la política de riesgos corporativa**. En ella se identifican los responsables del análisis, los recursos, los procesos, los activos, la metodología para realizar el análisis de riesgo, las herramientas necesarias, la periodicidad del análisis, las medidas de seguimiento, etc. **Orden HAC/858/2014, de 30 de septiembre, por la que se aprueba la política de seguridad de la información de la Administración de la Comunidad de Castilla y León.** La información que manejamos es un valor esencial y todos debemos participar del objetivo de asegurar la información, su disponibilidad, integridad y confidencialidad. Evitar su modificación o destrucción y reducir el riesgo de pérdida.

→ **En el ámbito de las AAPP**, las medidas de seguridad exigibles son las derivadas de la aplicación del **Esquema Nacional de Seguridad**, aprobado por RD 3/2010, de 8 de enero.

→ **La metodología para análisis de riesgos es "MAGERIT"** publicada por el CCN-CERT (Centro Criptológico Nacional).

→ **Otras normas y metodologías al uso:**

- Las normas ISO 31000 y 31010 para el análisis de riesgo en general.

- La norma ISO 27005 para el análisis de riesgos para la seguridad de la información.
- Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD de la AEPD.
-

IMPORTANTE: Todos nuestros tratamientos de datos deben someterse al análisis de riesgos, las que generemos a partir del RGPD y las anteriores a la entrada en vigor del RGPD para comprobar que se ajustan a este.

→ **Evaluación de impacto de protección de datos.**

- Solo se debe realizar de forma completa sobre los tratamientos que entrañen un alto riesgo para los derechos y libertades de las personas físicas.
- También debe hacerse en los tratamientos dirigidos a la elaboración de perfiles, tratamientos a gran escala o cámaras de videovigilancia.
- El obligado a hacerla es el responsable del tratamiento.
- El DPD tiene una participación activa.
- Guía práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD de la AEPD.
- Podemos emplear los mismos criterios que hemos visto en el análisis de riesgos pero aquí las amenazas son las del considerando 75 RGPD (en el análisis de riesgos se valoran supuestos en los que el tratamiento puede dar lugar a discriminación, usurpación de identidad o pérdida financiera).

→ El análisis de riesgos y la evaluación de impacto de protección de datos determinan **las medidas de seguridad que deben aplicarse**.

¿Cuáles son las medidas de seguridad que nos atañen?

La Oficina Técnica de Seguridad lo explica muy bien y van desde el uso correcto de correo-e, la configuración de nuestras claves y contraseñas, o la seudonimización que supone eliminar aquellos

datos que permitan identificar a los ciudadanos. Se trata de un mecanismo que oculta la identidad de los afectados pero este ocultamiento de la identidad es reversible y siempre podremos re-identificar a las personas.

→ **Violaciones de seguridad.** El RGPD introduce la necesidad de gestionar las violaciones de seguridad de los datos. Se trata 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 autorizados a dichos datos.**

→ **El responsable del tratamiento** siempre que exista riesgo para los derechos y libertades de las personas físicas **debe notificarlo**:

- **A la AEPD en un plazo máximo de 72 horas**. Contenido mínimo de la comunicación:
  - Naturaleza de la quiebra de seguridad.
  - Categorías de afectados (ej: menores, discapacitados, empleados, ciudadanos)
  - Nº aproximado de afectados
  - Categorías de datos comprometidos (ej: identificativos, salud, laborales)
  - Nº de registros de datos personales afectados
  - Nombre y datos de contacto del DPD
  - Posibles consecuencias de la quiebra de seguridad sufrida.
  - Medidas adoptadas o propuestas para remediar esta quiebra.

No tenemos que esperar una respuesta por parte de la AEPD.

- **A las personas físicas cuyos datos personales se hayan visto afectados por la quiebra de seguridad cuanto antes**. Excepto:

- Si se han adoptado y aplicado medidas sobre los datos personales afectados que hagan ininteligibles los datos para cualquier persona que no esté autorizada a acceder a ellos (ej: los datos están cifrados)
- El responsable ha adoptado medidas ulteriores que garanticen que ya no existe un alto riesgo para los derechos y libertades.
- Que esta comunicación fuese un esfuerzo desproporcionado, optándose por una comunicación pública o medida semejante por la que se informe de forma efectiva a los afectados.

- **Si el encargado del tratamiento sufre una quiebra de seguridad debe notificarlo sin dilación al responsable**.

4 LEY 39/2015, DE 1 DE OCTUBRE Y LEY DE TRANSPARENCIA

Adaptación de la normativa sectorial. La entrada en vigor del RGPD no solo exige de una adaptación de la normativa básica reguladora de este derecho fundamental, constituida por la futura ley orgánica de protección de datos y su posterior desarrollo reglamentario, el RGPD impone la necesaria adaptación de normativa sectorial tan de uso común como es la normativa reguladora del procedimiento administrativo común y la normativa sobre transparencia.

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

- **Entre las múltiples formas de tratamiento de datos que llevan a cabo las Administraciones Públicas, uno de los más**

relevantes y con mayor impacto potencial es la que el nuevo RGPD califica como "comunicación por transmisión" a terceros y que como toda modalidad de tratamiento, debe ampararse en alguno de los criterios de licitud previstos en el artículo 6 RGPD. Pensemos en los supuestos tradicionales de autorizaciones otorgadas para que la Administración que tramita un expediente solicite datos a las autoridades fiscales o de la seguridad social). Se trata del artículo 28.2 de la Ley 39/2015, de 1 de octubre. Según este artículo *"Los interesados no estarán obligados a aportar documentos que hayan sido elaborados por cualquier Administración, con independencia de que la presentación de los citados documentos tenga carácter preceptivo o facultativo en el procedimiento de que se trate, siempre que el interesado haya expresado su consentimiento a que sean consultados y recabados dichos documento. 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."*

La referencia al consentimiento tácito debemos entenderla desplazada por el RGPD. En cuanto a que la causa de legitimación de este tratamiento de datos que es el interoperabilidad entre AAPP sea el consentimiento del interesado, es criterio conocido de la AEPD a través de sus guías sectoriales, que cuando las AAPP pueden legitimar la interoperabilidad de sus datos en cualquiera de las otras bases jurídicas que legitiman el tratamiento, es muy discutible que esta base jurídica sea el consentimiento. El artículo 6 RGPD se cumple si concurre al menos una de las bases que establece. Si la base es el cumplimiento de una obligación legal es difícil que pueda complementarse con el consentimiento. Esto debemos ponerlo en relación con que, según la Ley 39/2015, de 1 de octubre, las AAPP no requerirán a los interesados datos o documentos no exigidos por la normativa reguladora aplicable o que hayan sido aportados anteriormente por el interesado a cualquier Administración.

IMPORTANTE: En el RAT deberá constar entre las actividades del tratamiento, su fundamentación legal y cuáles son los destinatarios de los datos, en este caso, las otras AAPP u organismo públicos con los que se va a interactuar.

→ **Artículo 53. Derechos del interesado en el procedimiento administrativo:** *"1. Además del resto de los derechos previstos en esta Ley, los interesados en un procedimiento administrativo tienen los siguientes derechos:*

c) A no presentar documentos originales salvo que, de manera excepcional, la normativa reguladora aplicable establezca lo contrario. En caso de que, excepcionalmente, deban presentar un documento original, tendrán derecho a obtener una copia autenticada de este".

→ **Artículo 46. Indicación de notificaciones y publicaciones:** *"Si el órgano competente apreciase que la notificación por medio de anuncios o la publicación de un acto lesiona derechos o intereses legítimos, se limitará a publicar en el Diario oficial que corresponda una somera indicación del contenido del acto y del lugar donde los interesados podrán comparecer, en el plazo que se establezca, para conocimiento del contenido íntegro del mencionado acto y constancia de tal conocimiento.*

Adicionalmente y de materia facultativa, las Administraciones podrán establecer otras formas de notificación complementarias a través de los restantes medios de difusión que no excluirán la obligación de publicar en el correspondiente Diario oficial".

La disposición adicional novena del ALOPD prevé una forma de minimizar los datos de identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos.

Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público se limita a prever la obligación genérica de cada Administración de facilitar al resto de las AAPP los datos relativos a los interesados que obren en su poder, especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad (art. 155.1) y de que dicha disponibilidad de datos ha de estar *"limitada estrictamente a aquellos que son requeridos a los interesados por las restantes Administraciones para la tramitación y resolución de los procedimientos y actuaciones de su competencia, de acuerdo con la normativa reguladora de los mismos"* (art. 155.2),

Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.

- **El artículo 86 RGPD**. Tratamiento y acceso del público a documentos oficiales, dice: "Los datos personales de documentos oficiales en posesión de alguna autoridad pública u organismo público o una entidad privada para la realización de una misión en interés público podrán ser comunicados por dicha autoridad, organismo o entidad de conformidad con el Derecho de la Unión o de los Estados miembros que se les aplique a fin de conciliar el acceso del público a documentos oficiales con el derecho a la protección de los datos personales en virtud del presente Reglamento".

  Por tanto, el RGPD parte de que los datos personales de documentos que se encuentren en poder de una autoridad pública u organismo público deben poder ser comunicados, dado que el acceso público a documentos oficiales puede considerarse de interés público.
  La normativa de los Estados miembros debe conciliar el acceso del público a documentos oficiales y la reutilización de la

información del sector público con el derecho a la protección de los datos personales.
El objetivo es garantizar la eficacia en el uso transfronterizo de documentos del sector público y promover la libre circulación de la información garantizando el respeto a la seguridad jurídica, la protección de los datos personales y la propiedad intelectual e industrial.

- **La Ley 37/2007, de 16 de noviembre, consagra como límite del derecho a la reutilización el derecho a la protección de datos**, de forma que cuando los documentos contengan datos de carácter personal, la reutilización se regirá por el RGPD.

- Por tanto **en la reutilización de datos y políticas open data deberá tenerse en cuenta que**:
  - En ningún caso, **podrá ser objeto de reutilización, la información en la que la ponderación a la que se refiere la ley de transparencia, dé como resultado la prevalencia del derecho fundamental a la protección de datos personales**, salvo que se produzca la disociación de los datos de modo que se impida la identificación de las personas afectadas.

  - **Las AAPP deberán realizar un análisis de riesgos de la actividad de tratamiento que es la reutilización de datos** para determinar los riesgos a que serán sometidos los derechos fundamentales y libertades públicas de los interesados en el caso en que datos personales vayan a ser publicados en documentos reutilizables. Como todo análisis de riesgos deberá incluir, al menos:
    - Una descripción de las operaciones de tratamiento previstas y de los fines del tratamiento.
    - Una evaluación de la necesidad del tratamiento respecto a su finalidad.
    - Una evaluación de los riesgos para los derechos y libertades de los interesados.

- Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad, mecanismos que garanticen la protección de datos personales demostrando la conformidad con el RGPD.

- **Resultado:**
  - **Puede llevarse a cabo la reutilización con datos personales.** Será preciso:
    - **(1º) Tener en cuenta el principio de minimización** de datos de manera que solo sean objeto de tratamiento los datos personales que sean necesarios para los fines específicos del tratamiento.
    - **(2º) Indicar en la licencia de puesta a disposición de los documentos**:
      - La finalidad o finalidades concretas para las que es posible la reutilización futura de los datos.
      - Sus límites.
      - En el caso de que se opte por la disociación de la información, hay que advertir, en las condiciones de uso, la prohibición de revertir el procedimiento de disociación.
  - **Alto riesgo para los derechos y libertades de los interesados** (por ejemplo, por tratarse de categorías especiales de datos personales) la reutilización con datos personales no podrá llevarse a cabo sin adoptar medidas destinadas a la disociación de los datos de modo que se impida la identificación de las personas afectadas y se impida volver a identificar los datos personales.

IMPORTANTE: Las normas citadas deben complementarse con la futura LOPD y su normativa de desarrollo o la modificación específica de estas leyes.