GUÍA PARA LA ADAPTACIÓN AL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS, DE LAS ADMINISTRACIONES LOCALES

ELABORADO POR EL GRUPO DE TRABAJO PARA LA IMPLANTACIÓN DEL NUEVO REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD) EN LAS ADMINISTRACIONES LOCALES

COMISIÓN DE SOCIEDAD DE LA INFORMACIÓN Y TECNOLOGÍAS

Desde la Red de Entidades Locales por la Transparencia y Participación Ciudadana de la FEMP volvemos a dirigirnos a las entidades locales para presentar, en este caso, la "guía para la adaptación al reglamento general de protección de datos de las administraciones locales" elaborada por un equipo multidisciplinar de técnicos locales, de la agencia española de protección de datos y expertos del ámbito jurídico y universitario.

Se trata de una guía sencilla y práctica que aborda la puesta en práctica de la nueva normativa sobre protección de datos que entra en vigor próximamente.

La convivencia del derecho de acceso a la información pública y la protección de datos de carácter personal es uno de los temas tratados y considerado como objetivo del trabajo de la Red que presido, cuestión tratada por la guía y que convive en el día a día de las administraciones locales.

Confío en que esta guía sea de vuestra utilidad y en que podamos seguir ofreciendo soluciones a las nuevas obligaciones que en esta y otras materias se imponen al sector local, adaptándolas al ámbito local.

Muchas gracias.

PRESENTACIÓN

La Comisión de Sociedad de la Información y Tecnologías de la Federación Española de Municipios y Provincias, que tengo el honor de presidir, tiene entre sus objetivos prioritarios contribuir a la difusión y correcto empleo de las más avanzadas técnicas, herramientas y metodologías, así como mejorar la normativa destinada a ayudar a los entes locales a desempeñar mejor, más eficazmente y conforme a la Ley, las funciones que los ciudadanos les han atribuido.

El pasado mes de abril se aprobó el Reglamento (UE) 2016/679 del Parlamento 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.

Todas las Administraciones Públicas deberán hacer las adaptaciones oportunas en sus procedimientos que harán posible cumplir con el citado Reglamento antes del 25 de mayo de 2018

Por este motivo, en el seno de la Comisión de Sociedad de la Información y Tecnologías de la FEMP, se constituyó un grupo de trabajo cuyo principal objetivo fue la creación de una Guía de ayuda para Entidades Locales con información facilitadora de su necesaria adaptación al Reglamento.

Pues bien, tras el trabajo realizado en los últimos meses, por fin ve la luz el presente documento, donde se pueden encontrar gran parte de las claves necesarias para el cumplimiento normativo.

Estoy seguro de que este documento permitirá que cada Administración local sea capaz de elaborar su propio itinerario hacía la consecución del objetivo: Cumplir plenamente con el RGPD. Por tanto, confío en la buena acogida de esta publicación y espero que su utilidad se refleje en el buen hacer del personal que trabaja para prestar un mejor servicio al ciudadano.

No me gustaría despedirme sin manifestar mi agradecimiento, como Presidente de la Comisión de Sociedad de la Información y Tecnologías, a todas las personas y/o entidades que han colaborado en este proyecto de manera absolutamente desinteresada: ¡Muchas gracias a todos por este magnífico trabajo!

Ramón Fernández-Pacheco Monterreal
Alcalde de Almería
Presidente de la Comisión de Sociedad de la Información y Tecnologías de la FEMP

ÍNDICE

INTRODUCCIÓN

En el mes de abril de 2016 se aprobó el Reglamento (UE) 2016/679 del Parlamento 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) (DOUE 4.5.2016).

Esta nueva regulación, que por primera vez se hace a través de un Reglamento Europeo, comportará cambios significativos en la protección de datos de carácter personal, tanto desde el punto de vista de los derechos de las personas, como de las obligaciones de las personas y entidades que tratan datos de carácter personal.

En este sentido, las Administraciones Locales, en el ejercicio de sus funciones, tratan diariamente una gran cantidad de datos personales, referidos principalmente, a sus ciudadanos, contribuyentes o terceros: Padrón de habitantes, Gestión de impuestos, Policías locales y Gestión de Infracciones, Subvenciones, Disciplina urbanística, Servicios Sociales, Proveedores de servicios, etc.

Aunque entró en vigor el 25 de mayo de 2016, el Reglamento General de Protección de Datos (RGPD) **será aplicable a partir del día 25 de mayo de 2018**. Hasta esta fecha, se abre un periodo transitorio para adaptarse a la nueva regulación. Es este período el que deberán aprovechar las Administraciones Locales para analizar las principales medidas a adoptar, así como establecer sus planes de adecuación.

Hasta el 25 de mayo de 2018, la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD) y su Reglamento de desarrollo (RLOPD), aprobado por el Real Decreto 1720/2007, de 21 de diciembre, siguen siendo de plena aplicación. A partir de esta fecha, algunos aspectos de la LOPD y del RLOPD quedarán desplazados por el RGPD. Otros aspectos, en cambio, pueden seguir siendo aplicables, bien porque queden fuera del ámbito de aplicación del RGPD o porque el mismo RGPD permite su regulación a nivel estatal.

En enero de 2017, con la finalidad de ayudar a las Entidades Locales con el cumplimiento de esta nueva Normativa, en el seno de la Comisión de Sociedad de la Información y Tecnologías de la FEMP, se creó un Grupo de Trabajo que tenía como objetivo la generación de un Itinerario de Trabajo que permitiera concienciar a las Administraciones Locales de la relevancia de este cambio legislativo y ayudar a la planificación de sus acciones de adaptación al RGPD, así como la importancia de cada una de ellas y los riesgos implicados.

Siempre de la mano de la Agencia Española de Protección de Datos (AEPD), y apoyados en la documentación de ayuda que ha venido generando, presentamos la Guía para la adaptación al RGPD de las Administraciones Locales, resultado del trabajo realizado por nuestro Grupo de Trabajo.

Se incluyen enlaces a la documentación más importante que debe conocer una Administración Local.

PASOS PARA LA ADAPTACIÓN DE LAS ADMINISTRACIONES PÚBLICAS AL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD): Recomendaciones de la AEPD.

1- PASOS RECOMENDADOS POR LA AEPD

PRIMER PASO

DESIGNAR UN DELEGADO de Protección de Datos, si procede. (Ver art.37 ***RGPD*** y art. 34 ***PLOPD***)

SEGUNDO PASO

ELABORAR EL ***RegistrodeActividadesdetratamiento***, prestando atención especialmente a los tratamientos que incluyan categorías especiales de datos o datos de menores

TERCER PASO

ANALIZAR las BASES JURÍDICAS de los TRATAMIENTOS

CUARTO PASO

EFECTUAR UN ANÁLISIS DE RIESGOS. Sobre los resultados de ese análisis, identificar e implantar las MEDIDAS TÉCNICAS Y ORGANIZATIVAS necesarias para hacer frente a los riesgos detectados sobre los derechos y libertades de los ciudadanos

QUINTO PASO

VERIFICAR LAS MEDIDAS DE SEGURIDAD tras el resultado del análisis de riesgos. Ello incluye verificar la aplicación de medidas de seguridad adecuadas, así como ESTABLECER PROTOCOLOS PARA GESTIONAR Y, EN SU CASO, NOTIFICAR quiebras de Seguridad

SEXTO PASO

SI EL TRATAMIENTO ES DE ALTO RIESGO, DETALLAR E IMPLANTAR UN PROCEDIMIENTO para realizar, una evaluación de impacto de la privacidad y, si fuera necesario, consultar previamente a la autoridad de control (art. 35 y 36, ***RGPD***)

2.- ACCIONES TRANSVERSALES NECESARIAS.

- ADECUAR LOS FORMULARIOS para adaptar el derecho de información a los requisitos del RGPD
- ADAPTAR LOS PROCEDIMIENTOS para atender los derechos de los ciudadanos, habilitando medios electrónicos
- ESTABLECER Y REVISAR LOS PROCEDIMIENTOS para acreditar el consentimiento y garantizar la posibilidad de revocarlo
- VALORAR SI LOS ENCARGADOS DE TRATAMIENTO OFRECEN GARANTÍAS de cumplimiento del RGPD y adaptar los contratos elaborados previamente
- CONFECCIONAR E IMPLANTAR POLÍTICAS DE PROTECCIÓN DE DATOS que contemplen los requisitos del ***RGPD*** (art. 24, 25, 30) y poder acreditar su cumplimiento
- ELABORAR Y LLEVAR A CABO UN PLAN DE FORMACIÓN Y CONCIENCIACIÓN para los empleados

Enlaces:

RGPD	https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/reglamentos/common/pdfs/Reglamento_UE_2016-679_Proteccion_datos_DOUE.pdf
PLOPD	http://www.mjusticia.gob.es/cs/Satellite/Portal/1292428605428?blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadervalue1=attachment%3B+filename%3DPL_OEI_TEXTO_.PDF
Registro de Actividades detratamiento	https://www.agpd.es/blog/de-la-inscripcion-de-ficheros-al-registro-de-actividades-ides-idPhp.php

DECÁLOGO PARA LA ADECUACIÓN AL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD) EN LAS ADMINISTRACIONES LOCALES.

Se presenta este Decálogo como resumen de las conclusiones del Grupo de Trabajo sobre Protección de Datos de la FEMP conjuntamente con la Agencia Española de Protección de Datos (AEPD), realizado a lo largo del 2017, El cual pone el acento y concreta las acciones que debe desarrollar cualquier **Administración Local** para adaptarse al RGPD.

Sus conclusiones han sido ya presentadas en dos jornadas realizadas en la sede de la FEMP que contaron con la participación de responsables de la AEPD, celebradas, la primera de ellas el 23 de octubre de 2017 y dirigida a Diputaciones Provinciales, Cabildos y pequeños Ayuntamientos y la segunda el 4 de diciembre de 2017 y dirigida a Ayuntamientos de más de 20.000 habitantes.

Con este documento, tratamos de poner a disposición un documento de referencia que pueda llegar a cualquier administración local y que pueda servir de lista de trabajos a realizar o como lista de comprobación de las tareas realizadas en la adaptación de los tratamientos de datos de carácter personal al nuevo RGPD.

Como explicamos en la introducción del presente documento, el RGPD fue publicado en mayo de 2016 y entró en vigor en ese mismo mes, aunque será de aplicación a partir del 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.

El ordenamiento jurídico de la Protección de los Datos de Carácter personal se complementará con la aprobación definitiva del proyecto de la nueva Ley Orgánica de Protección de Datos, cuyo trámite ya se ha iniciado en las Cortes Españolas.

Sin ánimo de exhaustividad para lo que se recomienda el acceso a las secciones que la AEPD y Agencias Autonómicas de Protección de Datos tienen en sus webs oficiales dedicadas al RGPD, el presente "decálogo", destaca los **10 puntos que deberían estar presentes en la hoja de ruta de cualquier AALL, de cara al cumplimiento del nuevo RGPD**.

PRIMERO

Identificar con precisión las finalidades y la base jurídica de los tratamientos que se llevan a cabo. (Principio de legitimación)

La vigente LOPD parte de considerar que los tratamientos solo pueden llevarse a cabo con el consentimiento de los afectados, con una serie de excepciones entre las que se encuentra el que los datos sean recogidos por las AAPP para el ejercicio de sus funciones. Asimismo, la LOPD prevé que las cesiones de datos requerirán el consentimiento de los afectados salvo que, entre otras excepciones, esa cesión esté autorizada por una ley.

El RGPD diseña un sistema de legitimación basado en seis bases jurídicas que no mantienen entre sí ninguna relación de prioridad o prelación. Entre esas bases jurídicas no se encuentran, en sentido estricto, los "fines propios de las AAPP en el ejercicio de sus competencias" ni la "autorización legal".

Ello no supone en absoluto que los tratamientos amparados en esas bases de la legislación nacional no puedan seguir llevándose a cabo. Significa tan sólo que deberán encontrarse las bases jurídicas apropiadas para esos tratamientos dentro de las que el RGPD ofrece. En particular, y para el ámbito de las AALL, son relevantes las siguientes:

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

La obligación de identificar y explicitar finalidades y bases legales de los tratamientos no deriva solo de la necesidad de cumplir con el principio de legalidad establecido en el RGPD, sino que viene impuesta por el hecho de que las finalidades o la base jurídica de los tratamientos son informaciones que deben proporcionarse a los interesados (arts.13 y 14 RGPD) y recogerse en el registro de actividades de tratamiento.

En el ámbito de las AALL, la base jurídica que legitima los tratamientos será el cumplimiento de una tarea en interés público o el ejercicio de poderes públicos, así como el cumplimiento de una obligación legal. En ambos casos deben estar establecidos en una norma. El proyecto de futura Ley Orgánica de Protección de Datos, actualmente en tramitación, establece que esa norma deberá tener rango de ley formal.

Además, de los dos supuestos de legitimación del tratamiento referidos anteriormente, también existe la posibilidad de que el tratamiento de datos se fundamente en satisfacer los intereses legítimos perseguidos por un tercero al que el responsable le comunica los datos. Este supuesto sólo sería aplicable en la Administración Local en el caso de que ese tercero no tuviese la condición de autoridad pública.

SEGUNDO

Identificar los tratamientos gestionados bajo el principio de consentimiento del interesado y su adecuación a las nuevas exigencias del RGPD.

En los casos en que la base jurídica de los tratamientos sea el consentimiento, éste deberá tener las características previstas por el RGPD, que exige que sea informado, libre, específico y otorgado por los interesados mediante una manifestación que muestre su voluntad de consentir o mediante una clara acción afirmativa.

Los consentimientos conocidos como "tácitos", basados en la inacción de los interesados, dejarán de ser válidos a partir de la fecha de aplicación del RGPD, incluso para tratamientos iniciados con anterioridad. En estos casos, deberá encontrase una base jurídica adecuada dentro de las que ofrece el RGPD. Esta base puede ser el consentimiento inequívoco tal y como lo define el RGPD u otra que resulte apropiada a las circunstancias propias de cada tratamiento, como puede ser el cumplimiento de una misión de interés público o el ejercicio de poderes públicos. En todo caso, los afectados deben ser informados del cambio de base jurídica y deben poder ejercer los derechos asociados a la nueva base.

Además, el consentimiento en el marco del RGPD se caracteriza por lo siguiente:

- Puede ser para uno o varios fines. En este caso:
  - Sería posible agruparlas en virtud de su vinculación (por ejemplo, consentimiento para la recepción de publicidad propia o de terceros).
  - Pero deberían desagregarse cuando los tratamientos impliquen conductas distintas (por ejemplo tratamiento por quien recaba los datos y cesión a terceros).
- Debe ser prestado de forma libre, si bien en el ámbito de las Administraciones públicas, siempre que actúen en el ejercicio de sus competencias, esta libertad puede no existir.
- Revocable.
- El responsable debe poder probar en todo momento que ha obtenido el consentimiento.
- Utilizar un lenguaje claro y sencillo

Por otra parte, también debe ser tenido en cuenta lo siguiente:

Si se usa para obtener una declaración escrita, debe quedar claramente diferenciada la parte referente a protección de datos del resto de declaraciones.

Asimismo, en el supuesto de datos sensibles el consentimiento, además de inequívoco, ha de ser explícito.

TERCERO

Cumplimiento del principio de transparencia: el derecho de información en la recogida de datos personales.

El RGPD regula el derecho de información en sus artículos 13 y 14, distinguiendo entre la información que se debe facilitar al titular de los datos dependiendo si los datos personales se han obtenido del mismo o no.

El RGPD amplía este derecho de información, respecto a lo que exigía la LOPD, en aras de la transparencia en el tratamiento de los datos personales, de tal forma que, además de los ya exigidos:

- La existencia de un fichero o tratamiento de datos personales.
- La finalidad para la cual se recaban tus datos personales.
- Quiénes son los destinatarios de la recogida de tus datos personales.
- Donde puedes ejercitar los derechos ARCO.
- La identidad de quién recaba tus datos personales.

Se deberá informar sobre los siguientes extremos:

- Los datos de contacto del Delegado de Protección de Datos (obligatorio AALL).
- La base jurídica o legitimación del tratamiento.
- El plazo o criterios de conservación y/o cancelación de la información.
- La existencia de decisiones automatizadas o elaboración de perfiles.
- La previsión de transferencias de datos a terceros países.
- El derecho a presentar una reclamación ante las autoridades de control.

Y además, en el caso de que los datos no se obtengan del propio afectado:

- El origen de los datos.
- Las categorías de los datos.

La información se proporcionará de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.

Los procedimientos, modelos o formularios diseñados de conformidad con la LOPD, deberán ser revisados y adaptados por los responsables de tratamiento, con anterioridad a la fecha de aplicación del RGPD (25 de mayo de 2018).

Para facilitar este cumplimiento, la AEPD recomienda adoptar un modelo de información por capas o niveles, que consiste en lo siguiente:

En un primer nivel, presentar una información básica (identificación del responsable, finalidad del tratamiento, ejercicio de derechos, origen de los datos, realización de perfiles), de forma resumida, en el mismo momento y medio en que se recojan los datos.

En un segundo nivel, la información adicional, presentando de forma detallada el resto de informaciones (podría incluirse la política de privacidad).

CUARTO

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

Los entes de la Administración Local deben elegir un encargado del tratamiento que ofrezca garantías suficientes respecto a la implantación y el mantenimiento de las medidas técnicas y organizativas apropiadas, de acuerdo con lo establecido en el RGPD, incluida la seguridad del tratamiento, así como del cumplimiento de la normativa de protección de datos.

Además, para demostrar que el encargado ofrece garantías suficientes, el RGPD prevé que la adhesión a códigos de conducta o a un mecanismo de certificación sirva como mecanismos de prueba.

Debemos partir de que la regulación de la relación entre el responsable y encargado del tratamiento tiene que plasmarse en un contrato o acto jurídico similar por escrito o incluso formato electrónico que los vincule.

Respecto al contenido mínimo, estará formado por el objeto, la duración, la naturaleza y finalidad del tratamiento, el tipo de datos personales y categorías de afectados, y las obligaciones y derechos del responsable.

En particular, el contrato o acto de encargo de tratamiento deberá contener:

- Las instrucciones del responsable del tratamiento.
- El deber de confidencialidad.
- Las medidas de seguridad.
- El régimen de la subcontratación.
- La forma en que el encargado asistirá al responsable en el cumplimiento de responder el ejercicio de los derechos de los afectados.
- La colaboración en el cumplimiento de las obligaciones del responsable.
- El destino de los datos al finalizar la prestación

Los que se hayan celebrado con anterioridad a la aplicación del RGPD (25 de mayo de 2018), según la Disposición Transitoria Quinta del proyecto de Ley Orgánica de Protección de Datos que se está tramitando, mantienen 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.

Para facilitar que los contratos cumplan con el RPGD, puede consultar las Directrices para la elaboración de contratos entre responsables y encargados de tratamiento.

QUINTO

Preparar los circuitos para atender los nuevos derechos de los afectados

Los afectados, como titulares de sus datos, pueden ejercitar ante la Administración Local que trate sus datos de carácter personal, los derechos de acceso, rectificación, supresión ("derecho al olvido"), oposición y limitación al tratamiento de los mismos:

Derechos del RGPD	***¿En qué consisten los derechos de los afectados?***
Derecho de acceso	A que el afectado sea informado de: • Los fines del tratamiento: categorías de datos personales que se traten y de las posibles comunicaciones de datos y sus destinatarios. • De ser posible, el plazo de conservación de tus datos. De no serlo, los criterios para determinar este plazo. • Del derecho a solicitar la rectificación o supresión de los datos, la limitación al tratamiento, u oponerse al mismo. • Del derecho a presentar una reclamación ante la Autoridad de Control. • Obtener una copia de los datos objeto del tratamiento. • Si se produce una transferencia internacional de datos, recibir información de las garantías adecuadas. • De la existencia de decisiones automatizadas (incluyendo perfiles), la lógica aplicada y consecuencias de este tratamiento. • 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.
Derecho de rectificación	• Rectificar los datos inexactos, y a que se completen los datos personales incompletos, inclusive mediante una declaración adicional.

Derecho de supresión ("el Derecho al Olvido")	**Con su ejercicio el afectado puede solicitar:** • **La supresión de los datos personales sin dilación debida cuando concurra alguno de los supuestos contemplados. Por ejemplo, tratamiento ilícito de datos, o cuando haya desaparecido la finalidad que motivó el tratamiento o recogida.** • **No obstante, se regulan una serie de excepciones en las que no procederá este derecho. Por ejemplo, cuando deba prevalecer el derecho a la libertad de expresión e información.**
Derecho a la limitación del tratamiento	**Permite al afectado:** • **Solicitar al responsable que suspenda el tratamiento de datos cuando:** - **Se impugne la exactitud de los datos, mientras se verifica dicha exactitud por el responsable;** - **El afectado ha ejercitado su derecho de oposición al tratamiento de datos, mientras se verifica si los motivos legítimos del responsable prevalecen sobre el afectado.** • **Solicitar al responsable que conserve tus datos personales cuando:** - **El tratamiento de datos sea ilícito y el afectado se oponga a la supresión de sus datos y solicite en su lugar la limitación de su uso;** - **El responsable ya no necesita los datos para los fines del tratamiento pero el afectado si los necesite para la formulación, ejercicio o defensa de reclamaciones.**
Derecho de oposición	**El afectado puede oponerse al tratamiento:** • **Cuando por motivos relacionados con su situación personal, debe cesar el tratamiento de tus datos salvo que se acredite un interés legítimo, o sea necesario para el ejercicio o defensa de reclamaciones.** • **Cuando el tratamiento tenga por objeto la mercadotecnia directa.**

La Administración Local deberá responder en el plazo máximo de un mes. Este plazo puede prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes, si bien se deberá informar al ciudadano de la citada prórroga en el plazo de un mes a partir de la recepción de la solicitud.

SEXTO

Necesidad de establecer un Registro de Actividades de Tratamiento.

Este registro sustituye a la obligación actual de notificar los ficheros y tratamientos a las autoridades de protección de datos.

Con el RGPD desaparece la obligación de notificar la inscripción de ficheros, tanto de responsables públicos o privados, en el Registro de Ficheros de la AEPD, o registro de la autoridad autonómica competente, sin perjuicio de la obligación de implementar el Registro de Actividades de Tratamiento.

Los responsables y encargados de tratamientos de la Administración Local deben mantener este Registro de Actividades de Tratamiento por escrito, incluso en formato electrónico (así lo prevé el proyecto de LOPD en tramitación), que estará a disposición de la Autoridad de Control, con el contenido que marca el art. 30 del RGPD para cada tratamiento:

Registro de actividades del RGPD	
Administración Local (responsables de tratamiento)	**Encargados de tratamiento de la Administración Local**
Nombre y datos de contacto del responsable o representante	Nombre y datos de contacto del encargado o representante
Fines del tratamiento	Categoría de tratamientos efectuados por cuenta del responsable
Nombre y datos de contacto del Delegado de Protección de Datos.	Nombre y datos de contacto del Delegado de Protección de Datos.
Categorías de datos personales.	----------
Categorías de afectados.	----------
Descripción medidas técnicas y organizativas de seguridad.	Descripción medidas técnicas y organizativas de seguridad.
Categorías de destinatarios de comunicaciones: incluidos países u organizaciones internacionales.	----------
Transferencias internacionales. Documentación de garantías adecuadas en caso del 49.1.	Transferencias internacionales. Documentación de garantías adecuadas en caso del 49.1.
Cuando sea posible, plazos previstos para las supresión de las diferentes categorías de datos.	----------

Este Registro podrá organizarse sobre la base de las informaciones de los ficheros notificados al Registro General de Protección de Datos de la AEPD, si bien no es un registro de ficheros sino de tratamientos.

Para configurar este registro de tratamientos, se puede partir de operaciones de tratamiento concretas a una finalidad básica común de todas ellas, así como de los ficheros que ya se encuentre inscritos.

Con el objetivo de facilitar esta labor, la AEPD, a través de su sede electrónica, ha puesto en marcha una nueva funcionalidad que permite a los responsables descargar los ficheros inscritos:

https://sedeagpd.gob.es/sede-electronica-eb/vistas/formCopiaContenido/copiaContenido.jsf

SEPTIMO

Necesidad de hacer un análisis de riesgo para los derechos y libertades de los ciudadanos de todos los tratamientos de datos que se desarrollen.

La protección de los derechos y libertades de los ciudadanos en relación con el tratamiento de sus datos personales que lleven a cabo los entes de la Administración Local, exige la adopción de medidas técnicas y organizativas con la finalidad de garantizar el cumplimiento de lo dispuesto en el RGPD.

Asimismo, el RGPD introduce el análisis de riesgo con la finalidad de evaluar el riesgo que puede producir el tratamiento de datos de datos personales, con anterioridad a que se inicie éste.

El RGPD obliga a que los responsables lleven a cabo una valoración del riesgo de los tratamientos que realicen, con el fin de establecer las medidas a aplicar y que variarán en función de:

- Los tipos de tratamiento.
- La naturaleza de los datos.
- El número de afectados.
- La cantidad y variedad de tratamientos que realice una misma organización.

A través de este análisis de riesgo, como hemos indicado anteriormente, se determinarán las medidas a aplicar para que los tratamientos de datos sean respetuosos con lo dispuesto en el RGPD, además de adoptar las correspondientes medidas de seguridad.

En este sentido, el RGPD prevé la realización de evaluaciones de impacto en protección de datos (EIPD), cuyas metodologías están disponibles en las webs de las Autoridades de Control, que además publicarán una lista de tratamientos tipo afectados por esta obligación.

El RGPD determina también, los siguientes supuestos en que debe realizarse obligatoriamente una evaluación de impacto:

- Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar.
- Tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9.1 o de los datos personales relativos a condenas e infracciones penales del artículo 10.
- Observación sistemática a gran escala de una zona de acceso público.

Especial atención cabrá prestar a los proyectos específicos de las "smart cities" o a las nuevas prácticas "big data". Son proyectos que pueden implicar la observación sistemática o a gran escala, que pueden conducir fácilmente a perfilados de ciudadanos o a la toma de decisiones automatizadas, con efectos jurídicos o de impacto para las personas. En este sentido, se recomienda consultar el código de buenas prácticas en protección de datos para proyectos big data, de la AEPD.

OCTAVO

Necesidad de revisar las medidas de seguridad que se aplican a los tratamientos en función del análisis de riesgo de los mismos y comunicación de brechas de seguridad.

El RGPD no establece medidas de seguridad estáticas, por lo que corresponderá al responsable determinar aquellas medidas de seguridad, que son necesarias para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales y que se adecúen a las características de los tratamientos, sus riesgos, el contexto en que se desarrollan, el estado de la técnica y los costes.

En el caso de las AAPP, incluidas las AALL, la aplicación de las medidas de seguridad estará marcada por los criterios establecidos en el Esquema Nacional de Seguridad. El Esquema está siendo revisado para adaptarlo a las exigencias del RGPD, dado que en su versión actual las medidas de seguridad para datos personales que recogía se remitían a las previsiones de la normativa de protección de datos que, como se ha indicado, ya no son válidas a la luz del RGPD.

A pesar de la nueva orientación a riesgos de las medidas de seguridad, en ningún caso el RGPD se debe de entender como la eliminación automática de todas las medidas de seguridad ya existentes.

La puesta en práctica de las políticas de privacidad en el diseño y por defecto definidas en el RGPD, deben ayudar a mitigar los riesgos desde la fase de proyecto de los nuevos tratamientos.

En este sentido, medidas como la seudonimización (eliminación de aquellos datos identificativos de los ciudadanos, conservando la reversibilidad para cuando las AALL, la puedan necesitar) pueden contribuir a reducir el riesgo en esos tratamientos.

Cuando se produzca una violación de seguridad, es decir, 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 ente de la Administración Local (responsable del tratamiento), que sufra dicha violación, siempre que exista riesgo para los derechos y libertades de las personas físicas, deberá notificarlo:

- A la AEPD, en un plazo máximo de 72 horas.
- A las personas físicas cuyos datos personales se hayan visto afectados por la brecha de seguridad, cuando antes.
- Sin perjuicio de lo anterior, a efectos de notificación se tendrán en cuenta las obligaciones derivadas del Esquema Nacional de Seguridad y las Instrucciones Técnicas aplicables.

Los entes de la Administración Local deben mantener un registro de los incidentes de seguridad y pueden elaborar un Plan de Contingencias con la finalidad de mitigar los daños cuando se produzca una brecha de seguridad, que junto con otras circunstancias de proporcionalidad pueden actuar como excepciones en la comunicación a los afectados, tal como prevé la AEPD.

NOVENO

Necesidad de designar un Delegado de Protección de Datos (DPD).

El RGPD introduce como obligatoria en el ámbito de las Administraciones Públicas la figura del denominado Delegado de Protección de Datos, por lo que los entes de la Administración Local deben proceder a su designación.

El RGPD valora que el DPD, sea una persona con conocimiento especializados en Derecho y en la práctica en materia de protección de datos. Estos conocimientos serán exigibles en relación con los tratamientos que se realicen, así como las medidas que deban adoptarse. Las funciones mínimas del Delegado se encuentran especificadas en el artículo 39 del RGPD, siendo las siguientes:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones del RPGD y demás normativa aplicable en protección de datos.
- Supervisar el cumplimiento del RGPD y demás normativa aplicable en protección de datos, y de las políticas del responsable o encargado del tratamiento en dicha materia, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación conforme al artículo 35 del RGPD.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa del artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.

Por otra parte, y dadas las funciones del DPD, su adscripción dentro de la estructura de la organización debe hacerse a órganos o unidades con competencias y funciones de carácter horizontal. Asimismo, el nivel del puesto de trabajo debe ser el adecuado para poder relacionarse con la dirección del órgano u organismo en el que desempeñe sus funciones.

- En los Ayuntamientos con población superior a 20.000 habitantes, atendiendo al volumen de datos tratados, el Delegado de Protección de Datos podría contar con un departamento de apoyo.
- En los Ayuntamientos con población inferior a 20.000 habitantes, podrían designar su Delegado de Protección de Datos, o articularlo a través de las Diputaciones Provinciales o Comunidad Autónoma respectiva.
- Secretarios, interventores y tesoreros, podrán actuar como delegados de protección de datos siempre que no exista conflicto de intereses en relación con el ejercicio de sus respectivas funciones en la gestión ordinaria del ente local en cuestión.
- El Delegado de Protección de Datos debe desempeñar sus tareas y funciones con total independencia.

La AEPD dispone de una Guía del DPD para las AA.PP en su web.

DECIMO

Adopción del principio de responsabilidad proactiva. "Accountability"

Por último, pero que también podría figurar como el primer principio del Decálogo, enunciaremos el concepto de responsabilidad proactiva establecido en el art. 5 del RGPD, como una de las obligaciones del responsable del tratamiento en relación a todos los principios referidos en el artículo primero, así como de lo especificado en los puntos anteriores de este Decálogo.

El principio de responsabilidad proactiva se puede resumir en la capacidad del responsable, es decir, de la organización, de demostrar y proporcionar evidencias del cumplimiento del RGPD en todo momento.

Para ello, creemos de vital importancia la correcta implantación del Registro de Actividades de Tratamiento y su interrelación con los aplicativos informáticos que los ejecutan, así como las trazas y evidencias que dichos aplicativos y las políticas de seguridad de la organización puedan generar para garantizar el cumplimiento de todos los principios del RGPD.

También será una garantía para el cumplimiento de los derechos de los afectados y para la salvaguarda de las contingencias de seguridad que puedan ocurrir.

En este sentido, una correcta relación entre el Registro de actividades de tratamiento y las políticas de seguridad vinculadas a los riesgos tecnológicos pueden permitir el diseño de cuadros de seguimiento del cumplimiento RGPD y la capacidad de anticipar situaciones problemáticas.

Por otro lado también deben trasladarse estas políticas proactivas a los encargados de tratamiento, con especial atención cuando los datos personales se envían fuera del Espacio Económico Europeo.

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 transfieran estos datos fuera del Espacio Económico Europeo, dentro de contratos de servicios informáticos.

En este sentido, el RGPD contiene una serie de supuestos (artículos 45 y 46), que permiten realizar dichas transferencias internacionales sin necesidad de solicitar una autorización previa por parte de las autoridades de protección de datos.

La exigencia de las políticas de seguridad, la trazabilidad informática y la metodología organizativa interna en el seguimiento de las decisiones en los nuevos tratamientos, serán clave en la gestión proactiva impuesta por el RGPD en los tratamientos de datos de carácter personal.

GUÍAS Y MATERIALES DE AYUDA DE LA AEPD PARA ADECUARSE AL RGPD

A través de su página web, la AEPD pone a disposición de los responsables, encargados y profesionales diversos materiales para facilitar la adecuación de los tratamientos a la normativa vigente de protección de datos.

Los siguientes pueden encontrarse en:

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

Sección Reglamento General de Protección de Datos (RGPD):

- Guía del RGPD para responsables del tratamiento.
- Guía para el cumplimiento del deber de información.
- Directrices para la elaboración de contratos entre responsables y encargados del tratamiento.
- Orientaciones y garantías en los procesos de anonimización de datos.
- El impacto del Reglamento General de Protección de Datos sobre las Administraciones públicas.
- El Delegado de Protección de Datos en las Administraciones Públicas.
- Guía sobre evaluación de riesgos.
- Guía sobre evaluaciones de impacto de protección de datos.
- El nuevo RGPD y su impacto sobre la actividad de las Administraciones Locales

PREGUNTAS FRECUENTES REALIZADAS POR LAS ADMINISTRACIONES LOCALES A LA AEPD.

Más allá de los nuevos aspectos normativos que se recogen en el "DECÁLOGO PARA LA ADECUACIÓN AL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD) EN LAS ADMINISTRACIONS LOCALES", se consideró de gran interés acompañarlo de un estudio sobre las preguntas más frecuentes realizadas por las AA.LL. relativas al tema de Protección de Datos.

En este sentido la FEMP y la AEPD han estado trabajando durante varios meses para recoger y sintetizar esta información, basada en las consultas que se habían formulado a la Agencia por parte de los diferentes entes locales, completada con preguntas de interés que se hicieron llegar desde el Grupo de trabajo.

El resultado abarca unas 40 preguntas/respuesta clasificadas por ámbitos de gestión de datos de carácter personal por parte de las Administraciones Locales y que se describen a continuación.

PADRÓN MUNICIPAL DE HABITANTES.

- **¿Pueden cederse los datos del Padrón Municipal a la policía local en el ejercicio de sus funciones?**

Los datos contenidos en el padrón municipal de habitantes pueden comunicarse a la policía local siempre que se cumplan los siguientes requisitos:

- Se asegure que se utilizan únicamente aquellos datos que son adecuados, pertinentes y no excesivos, que con carácter general, serán nombre, apellidos y domicilio;
- La comunicación se realice en el marco de expedientes concretos y con necesidades debidamente justificadas, relacionadas con las funciones de interés público de la Policía Local definidas en el artículo 53 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad; y
- Se garanticen la confidencialidad y seguridad de los datos personales.

Por otra parte, y atendiendo al principio de minimización de datos del RGPD, no se podría realizar una comunicación masiva de los datos del Padrón a la Policía.

No obstante, es posible habilitar los medios técnicos necesarios para que la comunicación de datos pueda realizarse mediante un acceso por parte de la Policía Local en sus propias oficinas al Padrón Municipal con las limitaciones anteriormente descritas.

- **¿Puede una Administración Local utilizar los datos del padrón para fomentar la participación ciudadana?**

El Padrón municipal de habitantes, regulado por la Ley de Bases de Régimen Local (LBRL), se concibe como un registro administrativo donde constan los datos de los vecinos de un municipio. Estos datos constituyen prueba de la residencia en el municipio y del domicilio habitual en el mismo.

Por otra parte, el artículo 69.1 de la LBRL impone a las Corporaciones locales la obligación de facilitar la más amplia información sobre su actividad y la participación de todos los ciudadanos en la vida local, pudiendo el Municipio promover toda clase de actividades y prestar cuantos servicios públicos contribuyan a satisfacer las necesidades y aspiraciones de la comunidad vecinal (artículo 25.1 LBRL), correspondiendo al Alcalde la representación del Ayuntamiento (artículo 2.1.b).

En consecuencia, y atendiendo a la obligación legal referida a los efectos de fundamentar la licitud del tratamiento de estos datos en base a lo dispuesto en el RGPD, se pueden utilizar los datos del padrón para fomentar la participación ciudadana en la medida de las funciones descritas en el art. 25 y 69 de la LBRL.

No obstante lo anterior, para el uso de otros ficheros diferentes del Padrón para las actividades descritas anteriormente, será necesario que la finalidad esté prevista legalmente o que los ciudadanos hayan consentido previamente.

- **¿Se puede comunicar información sobre la inscripción padronal de todas las personas inscritas en un inmueble al propietario del mismo?**

La Agencia Española de Protección de Datos considera que la expresión «datos del Padrón municipal» que se emplea en el artículo 16.3 de la LBRL se refiere únicamente a los datos que en sentido propio sirven para atender a la finalidad a que se destina el Padrón municipal: la determinación del domicilio o residencia habitual de los ciudadanos, la atribución de la condición de vecino, la determinación de la población del municipio y la acreditación de la residencia y domicilio.

La comunicación de datos del Padrón municipal queda limitada por el citado artículo 16.3 de la LBRL a las Administraciones públicas, por lo que atendiendo al principio de legitimación de datos del artículo 6 del RGPD, y puesto que el solicitante no ostenta tal condición, únicamente cabrá el consentimiento del afectado para el acceso a los datos del padrón en el supuesto de hecho planteado.

No obstante, una opción sería el pacto establecido en el contrato de arrendamiento, pudiendo establecerse incluso una cláusula en cuya virtud el arrendador y el arrendatario pactaran que éste último habrá de darle traslado a aquél de una copia del empadronamiento en el inmueble en el plazo que expresamente señalen; y en este sentido si para el arrendador fuera esencial el cumplimiento de esta cláusula, podría pactarse que en caso de incumplimiento en el plazo señalado se resolvería el contrato, es decir otorgarle virtualidad de condición resolutoria. A título de ejemplo, si esta fuera la voluntad de las partes, pudiera estipularse que el arrendatario habrá de dar traslado al arrendador de una copia del certificado o volante de empadronamiento en el plazo de tres meses desde la firma del contrato, y que en caso de incumplimiento podrá resolverse el contrato.

Enlaces

LBRL	https://www.boe.es/buscar/act.php?id=BOE-A-1985-5392
Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad	https://www.boe.es/buscar/act.php?id=BOE-A-1986-6859
Ley de Bases de Régimen Local	https://www.boe.es/buscar/act.php?id=BOE-A-1985-5392

PLENO Y CONCEJALES.

- **¿Se pueden publicar en Internet las actas de los Plenos municipales?**

Partiendo de que la publicación de datos, incluyendo en Internet, desde el punto de vista de protección de datos se considera una comunicación de los mismos, la publicación de las actas de los plenos municipales será conforme a la citada normativa cuando:

- no contengan datos de carácter personal;
- cuando conteniendo datos de carácter personal se refieren a actos debatidos en el Pleno o a disposiciones objeto de publicación en el Boletín Oficial que corresponda (sin perjuicio del ejercicio del derecho de oposición o cancelación de los afectados);
- En los demás supuestos, para realizar la publicación de las actas conteniendo datos de carácter personal, será necesario el consentimiento previo de los afectados.

No será objeto de publicación en aquellos supuestos en que la Corporación haya hecho uso de la facultad de declarar secreto el debate y votación por afectar al honor e intimidad de los ciudadanos.

- **¿Puede un Grupo Municipal grabar las sesiones del Pleno? ¿Y publicar la grabación en redes sociales?**

Se trata de un supuesto en que sería aplicable también la contestación que se ha indicado en la anterior pregunta frecuente, teniendo en cuenta, además, que la jurisprudencia ha considerado que se puede realizar dicha grabación.

No obstante, debe tenerse en cuenta lo siguiente:

- Las limitaciones establecidas por el propio artículo 70 de la Ley de Bases de Régimen Local cuando el Pleno, por mayoría absoluta, y tratándose derechos protegidos por el artículo 18.1 de la Constitución, acuerde que el debate y votación de estos asuntos sean secretos; en cuyo caso ni se podrá grabar ni difundir esta parte del Pleno.
- Será responsabilidad de quien graba y posteriormente publique las citadas grabaciones, el cumplimiento de las obligaciones impuestas por el RGPD.

- **¿Pueden los concejales de la oposición acceder a la documentación obrante en el Ayuntamiento en el ejercicio de sus funciones?**

La Ley de Bases de Régimen Local atribuye a los concejales la posibilidad de consultar la documentación obrante en el Ayuntamiento en el ejercicio de su actividad de control de los órganos de la Corporación y sin perjuicio de las especialidades que pudieran derivarse del régimen específico de determinados tratamientos (como los ficheros tributarios, sometidos a las limitaciones previstas en la Ley General Tributaria).

Por lo tanto, partiendo del reconocimiento de esta facultad a los citados concejales, y atendiendo a lo dispuesto en el artículo 77 de la Ley de Bases de Régimen Local, la comunicación se basaría en la existencia de la obligación por parte del Alcalde o Presidente o de la Comisión de Gobierno de facilitar cuantos antecedentes, datos o informaciones obren

en poder de los servicios de la Corporación y resulten precisos para el desarrollo de la función de control anteriormente citada.

En todo caso, debe recordarse que, los concejales que accedan a esa información sólo podrán utilizar los datos en el ámbito de sus competencias, toda vez que éste es el límite establecido en la Ley de Bases de Régimen Local.

No obstante, y de conformidad con el principio de limitación de la finalidad, del artículo 5.1.b) del RGPD, los datos deben tratarse para el control de la actividad del ente de la Administración Local correspondiente, ya que otro uso sería incompatible con dicho fin, no pudiente dar publicidad a esos datos ni comunicárselos a ningún tercero.

- **¿Se podrían ceder a los concejales la productividad y gratificaciones por servicios extraordinarios que reciba el personal de su Ayuntamiento? ¿Y los datos referentes a un proceso selectivo?**

La fundamentación para esta comunicación de datos personales sería la misma que se ha explicado en la anterior pregunta-respuesta, es decir, una comunicación de datos permitida en base al cumplimiento legal de facilitar el control que del ente de la Administración Local realizan los concejales de la oposición.

No obstante, conviene precisar lo siguiente:

La comunicación debe referirse, atendiendo al principio de minimización de datos del RGPD, a los datos que sean más recientes. Para comunicar datos de ejercicios o procesos selectivos anteriores, debería justificarse adecuadamente en qué medida coadyuvan al control de la acción del Gobierno Municipal.

- **¿Pueden los concejales de la oposición acceder a los datos tributarios obrantes en su respectivo Ayuntamiento?**

Si bien en apartados anteriores nos hemos referido a una serie de supuestos de acceso, por parte de concejales de la oposición, a la documentación obrante en el Ayuntamiento para el ejercicio de su actividad de control, el citado acceso no alcanzaría a conocer información de carácter tributario, puesto que que operaría la limitación derivada del artículo 95 de la Ley general Tributaria.

Esta limitación operaría también en caso de que la información se refiriese a categorías especiales de datos, como por ejemplo, datos de salud (si bien en este segundo caso se ignora qué finalidad podría justificar el tratamiento de estos datos por una Administración Local), por lo que su acceso se regula según lo dispuesto en el artículo 9 del RGPD. Cabría la posibilidad de conocer los mismos, si hubieran sido hechos manifiestamente públicos por los afectados.

Enlaces

Ley General Tributaria	https://www.boe.es/buscar/act.php?id=BOE-A-2003-23186

PUBLICACIÓN DE DATOS.

- **¿Se pueden publicar en Internet, incluyendo en la web de una Administración Local, imágenes de las fiestas patronales?**

Cuando se publican imágenes de personas físicas identificadas o identificables con la finalidad de informar de las actividades llevadas a cabo por organismos o instituciones, lo que implica obviamente la previa captación de imágenes de los participantes o asistentes a las mismas, considerando que los hechos así publicados podrían tener la consideración de hechos noticiables en los que se manifieste la existencia de un interés público con el fin de que se dé a conocer los mismos a la colectividad, y teniendo en cuenta, la aplicación de lo dispuesto en el artículo 20.1.a) y d) de la Constitución Española que regula la libertad de expresión e información.

En consecuencia, la captación de imágenes y su posterior difusión será considerada lícita cuando exista un interés público en su conocimiento y resulte adecuada, pertinente y no excesiva en relación con el libre ejercicio de la libertad de información, en los términos en que la doctrina constitucional ha entendido que dicho derecho prevalece sobre otros derechos fundamentales recogidos en el artículo 18 de la Constitución.

- **¿Se pueden publicar sanciones administrativas en el Boletín Oficial del Estado?**

Teniendo en cuenta que la publicación de datos personales se considera una comunicación de datos de carácter personal, la habilitación para realizar la publicación de sanciones administrativas, se encuentra en el artículo 44 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, ya que dicho precepto establece una obligación legal respecto a las citadas Administraciones. Así, según este precepto:

"Cuando los interesados en un procedimiento sean desconocidos, se ignore el lugar de la notificación o bien, intentada ésta, no se hubiese podido practicar, la notificación se hará por medio de un anuncio publicado en el Boletín Oficial del Estado.

Asimismo, previamente y con carácter facultativo, las Administraciones podrán publicar un anuncio en el boletín oficial de la Comunidad Autónoma o de la Provincia, en el tablón de edictos del Ayuntamiento del último domicilio del interesado o del Consulado o Sección Consular de la Embajada correspondiente.

Las Administraciones Públicas podrán establecer otras formas de notificación complementarias a través de los restantes medios de difusión, que no excluirán la obligación de publicar el correspondiente anuncio en el Boletín Oficial del Estado".

No obstante lo anterior, la Disposición adicional novena del proyecto de Ley Orgánica de Protección de Datos que se está tramitando, denominada "Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos", contempla lo siguiente:

- Cuando la publicación de un acto administrativo contuviese datos de carácter personal del afectado, se identificará al mismo mediante su nombre y apellidos, añadiendo las

cuatro últimas cifras numéricas del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

- Cuando se trate de la notificación por medio de anuncios, particularmente en los supuestos a los que se refiere el artículo 44 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se identificará al afectado exclusivamente mediante el número completo de su documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.
- Cuando el afectado careciera de cualquiera de los documentos mencionados en los dos párrafos anteriores, se identificará al afectado únicamente mediante su nombre y apellidos. En ningún caso debe publicarse el nombre y apellidos de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

- **¿Es posible publicar en la web de una Administración Local las licencias de obras concedidas?**

En primer lugar, debe tenerse en cuenta que las licencias podrían incorporar nombre y apellidos del solicitante, dirección postal y catastral del lugar donde se desea realizar la obra, presupuesto presentado por el promotor e importe de los impuestos de la actuación devengada.

De esta forma, este tipo de datos así como cualquier otra información contenida en los expedientes que se encuentre referida a personas físicas tendrán la consideración de dato de carácter personal por lo que su tratamiento estará sujeto a la normativa de protección de datos.

Puesto que no existe una obligación legal de las Administraciones Públicas de realizar tal publicación será necesario el consentimiento del afectado para proceder a la citada publicación.

Además, debe añadirse que entre los datos a publicar podría existir datos de carácter tributario, como es el relativo a los impuestos devengados por la realización de las obras, datos que tienen el carácter de reservados conforme a su normativa, que establece un catálogo de supuestos en que es posible tal comunicación, catalogo en el que, obviamente, no está comprendida su difusión al público en general.

- **¿Pueden publicarse en la página web de un Ayuntamiento los datos de sus habitantes, sin que se incluya su nombre y DNI, pero publicando los datos relativos a fecha de nacimiento, nacionalidad, nivel de estudios y calle sin identificar ni portal ni número?**

La finalidad de esta publicación sería que se desarrollen aplicaciones software por terceros o el propio Ayuntamiento que crucen datos del portal Opendata que sean de interés para el ciudadano.

De este modo sólo será posible la publicación de datos contenidos en los ficheros de la Administración pública, fuera de los supuestos permitidos por la Ley o en que exista un consentimiento de los afectados, si los datos se encuentran anonimizados.

Para facilitar la labor de anonimización, se puede consultar la Guía publicada por esta Agencia Española de Protección de Datos sobre "Orientaciones y garantías sobre los procedimientos de anonimización de datos personales".

Estos aspectos deben tenerse en cuenta respecto de los tratamientos y cesiones de datos a realizar por el Ayuntamiento en relación con el concepto de open data, en particular respecto de los datos que en tal calidad pudiera publicar y que sean resultado de un proceso de disociación de los datos personales obrantes en los ficheros municipales (sea el Padrón o cualquier otro que contenga datos personales), recordando que no es suficiente con eliminar los elementos que identifican directamente a la persona (nombre, dirección) como ocurre en el presente supuesto, sino que es preciso una agregación suficiente de los datos para evitar la re-identificación de las personas cuyos datos, aunque separados de los que le identifican directamente, se hacen públicos.

- **Un ciudadano que ejercitando el derecho de acceso de la Ley 19/2013, de 9 de diciembre, ha obtenido copia de las declaraciones de bienes de los concejales de un Ayuntamiento ¿Podría publicar las mismas en Internet?**

En el presente caso esta información ha sido obtenida en ejercicio del derecho de acceso a la información pública regulado por los artículos 12 y siguientes de la mencionada Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. Esto supone que cualquier tratamiento posterior de la información deberá ajustarse al RGPD. De este modo, si quien ha obtenido dicha información quiere proceder a su publicación necesitaría el consentimiento previo de los afectados, ya que no sería de aplicación el resto de causas legitimadoras del tratamiento de datos que regula el artículo 6 del RGPD.

De lo contrario, se estaría equiparando en la práctica el acceso a la información pública con la publicidad activa.

Enlaces

Ley 39/2015, de 1 de octubre	https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565
Proyecto de Ley Orgánica de Protección de Datos	http://www.mjusticia.gob.es/cs/Satellite/Portal/1292428594682?blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadervalue1=attachment%3B+filename%3DPLOPD_TEXTO_APROBADO_CM_10-11-2017.PDF
Orientaciones y garantías sobre los procedimientos de anonimización de datos personales	https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2016/Orientaciones_y_garantias_Anonimizacion.pdf
Ley 19/2013, de 9 de diciembre	https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&p=20131221&tn=2

TRATAMIENTO DE DATOS EN EL MARCO FUNCIONARIAL Y LABORAL.

- **¿Se pueden comunicar a los representantes de los trabajadores datos de carácter personal del personal que presta sus servicios en la correspondiente Administración Local?**

Como ya hemos visto anteriormente, uno de los supuestos para habilitar el tratamiento de datos consiste en el cumplimiento de una obligación legal.

Si se trata de datos referidos a personal funcionario, la comunicación vendría habilitada de la siguiente forma:

El Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público, en su artículo 39.1 establece que "Los órganos específicos de representación de los funcionarios son los Delegados de Personal y las Juntas de Personal", según proceda.

Por otro lado, en el artículo 40 enumera las funciones atribuidas a las Juntas de Personal y a los Delegados de Personal:

"a) Recibir información, sobre la política de personal, así como sobre los datos referentes a la evolución de las retribuciones, evolución probable del empleo en el ámbito correspondiente y programas de mejora del rendimiento.

b) Emitir informe, a solicitud de la Administración Pública correspondiente, sobre el traslado total o parcial de las instalaciones e implantación o revisión de sus sistemas de organización y métodos de trabajo.

c) Ser informados de todas las sanciones impuestas por faltas muy graves.

d) Tener conocimiento y ser oídos en el establecimiento de la jornada laboral y horario de trabajo, así como en el régimen de vacaciones y permisos.

e) Vigilar el cumplimiento de las normas vigentes en materia de condiciones de trabajo, prevención de riesgos laborales, Seguridad Social y empleo y ejercer, en su caso, las acciones legales oportunas ante los organismos competentes.

f) Colaborar con la Administración correspondiente para conseguir el establecimiento de cuantas medidas procuren el mantenimiento e incremento de la productividad."

A la vista de la previsión legal que se acaba de citar, las funciones atribuidas a las Juntas de Personal por el Real Decreto Legislativo 5/2015, de 30 de octubre, pueden llevarse con un adecuado desarrollo sin necesidad de proceder a una cesión masiva de los datos referentes al personal que presta sus servicios en el Órgano o Dependencia correspondiente, salvo que hubieran dado su consentimiento, y ello derivado de que, con carácter general, la cesión de datos no está contemplada específicamente en el Estatuto Básico del Empleado Público.

No obstante lo anterior, en el supuesto en que un empleado público haya planteado una queja ante su sección sindical, comité o junta correspondiente, relativa a sus condiciones de trabajo, será posible la cesión del dato específico de dicha persona.

Si se trata de datos referidos al personal laboral, la comunicación vendría habilitada de la siguiente forma:

El artículo 64 del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores, en materia de información y consulta de los trabajadores y en materia de protección de los trabajadores asalariados en caso de insolvencia del empresario, recoge las competencias del Comité de Empresa y dispone en su número 1 que: "*El comité de empresa tendrá derecho a ser informado y consultado por el empresario sobre aquellas cuestiones que puedan afectar a los trabajadores, así como sobre la situación de la empresa y la evolución del empleo en la misma, en los términos previstos en este artículo.*

Se entiende por información la transmisión de datos por el empresario al comité de empresa, a fin de que éste tenga conocimiento de una cuestión determinada y pueda proceder a su examen. (….)"

Y su número 7 apartado a) 1º atribuye a dicho órgano *"Ejercer una labor: De vigilancia en el cumplimiento de las normas vigentes en materia laboral, de Seguridad Social y empleo, así como el resto de los pactos, condiciones y usos de empresa en vigor, formulando, en su caso, las acciones legales oportunas ante el empresario y los organismos o tribunales competentes; 2º. De vigilancia y control de las condiciones de seguridad y salud en el desarrollo del trabajo en la empresa, con las particularidades previstas en este orden por el artículo 19 de esta Ley. 3º. De vigilancia del respeto y aplicación del principio de igualdad de trato y de oportunidades entre mujeres y hombres.*

b) Participar, como se determine por convenio colectivo, en la gestión de las obras sociales establecidas en la empresa en beneficio de los trabajadores o de sus familiares. (…)

9. Respetando lo establecido legal o reglamentariamente, en los convenios colectivos se podrán establecer disposiciones específicas relativas al contenido y a las modalidades del ejercicio de los derechos de información y consulta previstos en este artículo, así como al nivel de representación más adecuado para ejercerlos."

Por otra parte, también debe tenerse presente que según el artículo 8.4 del Estatuto de los Trabajadores:

4. El empresario entregará a la representación legal de los trabajadores una copia básica de todos los contratos que deban celebrarse por escrito, a excepción de los contratos de relación laboral especial de alta dirección sobre los que se establece el deber de notificación a la representación legal de los trabajadores.

Con el fin de comprobar la adecuación del contenido del contrato a la legalidad vigente, esta copia básica contendrá todos los datos del contrato a excepción del número del documento nacional de identidad o del número de identidad de extranjero, el domicilio, el estado civil, y cualquier otro que, de acuerdo con la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, pudiera afectar a la intimidad personal. El tratamiento de la información facilitada estará sometido a los principios y garantías previstos en la normativa aplicable en materia de protección de datos.

La copia básica se entregará por el empresario, en plazo no superior a diez días desde la formalización del contrato, a los representantes legales de los trabajadores, quienes la firmarán a efectos de acreditar que se ha producido la entrega.

De la norma expuesta podemos concluir, al igual que en el apartado anterior, que existe habilitación legal suficiente para comunicar a la representación legal de los trabajadores los datos necesarios para que puedan ejercer sus funciones, sin necesidad de proceder a una

información masiva. Sólo en el supuesto en que la vigilancia o control se refieran a un sujeto concreto, que haya planteado la correspondiente queja ante el Comité de Empresa, será posible la cesión de datos específicos de dicha persona.

En los demás supuestos, la función de control quedará plenamente satisfecha, mediante la comunicación de la información debidamente disociada, de forma que permita al Comité conocer las circunstancias cuya vigilancia le ha sido encomendada sin referenciar la información en un sujeto concreto.

- **¿Se puede instalar GPS en los coches de la policía local con la finalidad de localizar los vehículos y ubicación para mejorar la prestación del servicio?**

En primer lugar, y atendiendo al principio de limitación de la finalidad del artículo 5 del RGPD, cabrá obtener los datos de localización de los vehículos siempre que estén en servicio, prestando las funciones públicas que les son propias, y sin que la finalidad para la que hayan sido obtenidos pueda alterarse ni ampliarse. Es decirse, estos datos no podrán utilizarse para una finalidad incompatible.

En segundo lugar, deberá cumplirse el deber de información al afectado – en este caso, los funcionarios del cuerpo de policía local que vayan a ocupar los vehículos - por el tratamiento de datos, exigido en el artículo 13 del RGPD.

Por último, y respecto del consentimiento, el RGPD permite el tratamiento de datos cuando es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.

Por lo tanto, el tratamiento de los datos de localización del vehículo policial durante la prestación del servicio y, como consecuencia, de los policías que se encuentran en el mismo responden a la necesidad de garantizar el mejor desarrollo de sus funciones y forma parte de la prestación del servicio de protección de la personas y los bienes (seguridad pública), por lo que, el tratamiento de dicho dato vendría amparado en lo previsto en el artículo 6.1.e) del RGPD.

- **¿Podrían ser objeto de publicación un listado de horas extraordinarias de la policía local con los nombres, apellidos y número de los agentes y las horas acumuladas?**

Esta publicación se podría realizar si la misma estuviese prevista en un Acuerdo entre los representantes de la Administración y de los trabajadores. En caso contrario, para realizar la misma sería necesario el consentimiento expreso de los afectados.

- **El personal que presta servicios de atención al público ¿Está obligado a consignar en el ejercicio de sus funciones de cotejo y compulsa de documentos su nombre, apellidos y DNI?**

Atendiendo a la normativa que regula el servicio de atención al ciudadano, la denominación del cargo o puesto de trabajo del titular del órgano competente para la emisión de un documento y el nombre y dos apellidos del mismo, son suficientes para identificar al funcionario que formaliza un documento, sin que sea exigible la identificación del mismo

mediante su DNI. Este criterio parece trasladable al funcionario, que ocupando un puesto de trabajo en una unidad de Registro, coteja los documentos originales y la copia presentada, ya que resultará identificado con su nombre y apellidos si consta en el sello de compulsa, tal y como señala el precepto transcrito, la identificación del órgano y la fecha en que se realiza la misma. De este modo, la inclusión del DNI podría no ajustarse al artículo 5 del RGPD, en relación con el principio de minimización de datos, salvo que tal dato fuese exigido por una norma especial.

- **La firma electrónica utilizada por los empleados públicos ¿Es factible que en las propiedades de la firma vaya asociado el dato del DNI de la persona firmante?**

La implantación de un sistema de firma electrónica no tiene porqué modificar el contenido de los documentos que los empleados públicos firmen en el ejercicio de sus atribuciones si dicha modificación no tiene su origen en una norma. No debe así confundirse el contenido del certificado electrónico, que debe reunir los requisitos exigidos por la normativa aplicable, con el contenido del documento resultante de la firma electrónica que deberá incluir los datos requeridos por la normativa que le resulte aplicable.

Por consiguiente, 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.

Enlaces

Texto refundido de la Ley del Estatuto Básico del Empleado Público	https://www.boe.es/buscar/act.php?id=BOE-A-2015-11719
Real Decreto Legislativo 2/2015, de 23 de octubre	https://www.boe.es/buscar/act.php?id=BOE-A-2015-11430&tn=2&p=20170513

VIDEOVIGILANCIA.

- **¿Cómo se realiza el cumplimiento de la normativa de videovigilancia en la instalación de cámaras de seguridad en los edificios de la Administración Local?**

La imagen es un dato de carácter personal que permite la identificación de personas físicas, la videovigilancia con fines de preservar la seguridad de bienes y personas, supone un tratamiento de datos, y por tanto, el sometimiento al RGPD.

En líneas generales, los elementos más destacados a efectos de cumplimiento son los siguientes:

- Elaborar el registro de actividades del tratamiento que se realice a través de videovigilancia.
- Cumplir con el derecho de información mediante un cartel en el que se indique, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos de acceso y supresión que regula el RGPD.
- Adoptar las correspondientes medidas de seguridad.

- **¿Se pueden instalar cámaras de videovigilancia que graben la vía pública?**

La instalación de videocámaras en lugares públicos, tanto fijas como móviles, es competencia exclusiva de las Fuerzas y Cuerpos de Seguridad, rigiéndose el tratamiento de dicha imágenes por su legislación específica, contenida en la Ley Orgánica 4/1997, de 4 de agosto, y su Reglamento de desarrollo, sin perjuicio de que les sea aplicable, en su caso, lo previsto por el RGPD, en aspectos como la adopción de las medidas de seguridad que resulten de aplicación y la elaboración del registro de actividades en relación con el tratamiento de videovigilancia que se realice.

Su utilización en lugares públicos tienen una finalidad específica de seguridad en beneficio de la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública.

La instalación de este tipo de dispositivos de las imágenes grabadas, están sujetas a requisitos muy estrictos, ya que en primer lugar, la autorización de instalación de videocámaras fijas y la utilización de cámaras móviles, se otorga por la Delegación del Gobierno previo informe preceptivo y vinculante de la Comisión de Garantías de la Videovigilancia de la Comunidad Autónoma correspondiente.

- **¿Puede utilizar la policía local cámaras móviles o incluso realizar grabaciones con sus propias cámaras?**

Aunque se tratase de cámaras móviles o sus propias cámaras, se trataría de un supuesto cuya respuesta es la misma que en la anterior pregunta-respuesta, es decir, aplicación de la Ley Orgánica 4/1997, de 4 de agosto, y su Reglamento de desarrollo, sin perjuicio de que les sea aplicable, en su caso, lo previsto en el RGPD.

- **¿Qué requisitos debe cumplir la instalación de videovigilancia para control del tráfico?**

La instalación y uso de videocámaras y de cualquier otro medio de captación y reproducción de imágenes para el control, regulación, vigilancia y disciplina del tráfico se efectuará por la autoridad encargada de la regulación del tráfico a los fines previstos en el Real Decreto Legislativo 6/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, y demás normativa específica en la materia, y con sujeción a lo dispuesto en la normativa de protección de datos.

De esta forma, corresponderá a las Administraciones públicas con competencia para la regulación del tráfico, autorizar la instalación y uso de estos dispositivos, adoptando una resolución a tal efecto.

- **¿Podría el sistema de videovigilancia instalado grabar también la voz?**

En el supuesto planteado se trataría de la instalación de un sistema de seguridad y control de acceso a edificios captado la imagen y voz de las personas que acceden a los mismos.

Con carácter general, las grabaciones indiscriminadas de voz y 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 del RGPD, considerándose una medida intrusiva.

Enlaces

Ley Orgánica 4/1997, de 4 de agosto	https://www.boe.es/buscar/act.php?id=BOE-A-1997-17574
Reglamento de desarrollo de LO 4/1997	https://www.boe.es/buscar/act.php?id=BOE-A-1999-8648
Real Decreto Legislativo 6/2015, de 30 de octubre	https://www.boe.es/buscar/act.php?id=BOE-A-2015-11722

ACCESO A EXPEDIENTES ADMINISTRATIVOS Y LEY DE TRANSPARENCIA.

- **Cuando una Administración Local recibe una denuncia de un ciudadano ¿Es posible comunicar sus datos al denunciado?**

En el supuesto de que el denunciante haya manifestado expresamente su deseo de confidencialidad o a juicio del departamento que tramita ese expediente considera necesario garantizar la identidad del denunciante en condiciones de confidencialidad, podrá denegarse al denunciado el acceso a los datos personales del citado denunciante.

En todo caso, esta comunicación al denunciante debería producirse previa ponderación de si la misma resulta necesaria a los efectos de que las personas denunciadas en el expediente puedan ejercer en plenitud sus derechos, conforme a lo requerido por el artículo 5 del RGPD, no debiendo tener dicha comunicación un carácter genérico ni extenderse a la totalidad de los datos que figuren en la denuncia presentada voluntariamente o en el correspondiente boletín de denuncia.

- **¿Cómo afecta la normativa de protección de datos a los procedimientos de concurrencia competitiva?**

En relación con el tratamiento de datos personales en procedimientos administrativos de concurrencia competitiva, es preciso tener en cuenta, que la aceptación de las bases de la convocatoria supone prestar el consentimiento para el tratamiento de los datos personales de los afectados.

Además, debe tenerse en cuenta que la materia de los procedimientos selectivos está presidida por los principios de transparencia y publicidad, como garantes del principio de igualdad. El artículo 45 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, prevé que los actos administrativos serán objeto de publicación cuando así lo establezcan las normas reguladoras de cada procedimiento o cuando lo aconsejen razones de interés público apreciadas por el órgano competente.

En todo caso, los actos administrativos serán objeto de publicación, surtiendo ésta los efectos de la notificación, en particular, cuando se trate de actos integrantes de un procedimiento selectivo o de concurrencia competitiva de cualquier tipo.

Asimismo, la convocatoria del procedimiento deberá indicar el medio donde se efectuarán las sucesivas publicaciones, careciendo de validez las que se lleven a cabo en lugares distintos. La norma prevé que la publicación de los actos se realizará en el diario oficial que corresponda, según cual sea la Administración de la que proceda el acto a notificar.

Por otra parte, la Audiencia Nacional ha ponderado el principio de publicidad con la protección de datos de carácter personal, llegando a la conclusión de que durante la tramitación del proceso selectivo ha de prevalecer el primero. Así, ha estimado que no es exigible el consentimiento de aquellas personas que participen en un procedimiento de concurrencia competitiva para el tratamiento de las calificaciones obtenidas en dicho procedimiento y ello como garantía y exigencia de los demás participantes para asegurar la limpieza e imparcialidad del procedimiento en el que concurren.

Todo ello siempre que se publiquen aquellos datos que sean pertinentes, adecuados y limitados a lo necesario, de tal forma, que como ya hemos señalado anteriormente, a efectos de publicación tendría que tomarse en consideración lo previsto en la Disposición adicional novena del proyecto de Ley Orgánica de Protección de Datos que se está tramitando.

En consecuencia, si las bases de la convocatoria de un procedimiento de concurrencia competitiva prevén la publicación de las listas de admitidos y excluidos, incluidas las causas de la exclusión, a efectos de la legitimación para el tratamiento de datos, la publicación se fundamentaría en el cumplimiento de una obligación legal en relación con el artículo 45 de la Ley 39/2015, de 1 de octubre anteriormente citado.

Por último, por el órgano que inste la publicación se podrían adoptar las medidas necesarias para limitar el período de exposición, de forma que se evite la indexación por parte los motores de búsqueda de Internet.

- **¿Se puede facilitar a un tercero el DNI o número de teléfono existente en un expediente administrativo?**

Respecto al acceso a los expedientes administrativos, debemos distinguir lo siguiente:

a.- Si el procedimiento administrativo no ha finalizado, en virtud de lo establecido en la Ley 39/2015, de 1 de octubre, sólo podrán acceder a los datos contenidos en los expedientes quienes ostenten la condición de interesado.

b.- Si el procedimiento administrativo ha finalizado, el acceso a los datos obrantes en los expedientes se tramitaría conforme a la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno, cuya regla general es conceder el acceso a la información obrante en la Administración a la cual se ha dirigido la petición.

Ahora bien, dicho derecho no es ilimitado, estableciendo la propia Ley diversos límites en sus artículos 14 y 15, de los que interesa analizar aquí los establecidos en el artículo 15, relativos a la protección de datos de carácter personal.

En cuanto a los datos de DNI o número de teléfono, cabe efectuar la ponderación exigida por el artículo 15, pero también puede acudirse a lo previsto en el número 4 del artículo. De este modo, si se eliminan tales datos de las copias de los documentos que se faciliten de modo que no pueda saberse quien es la persona cuyos datos personales han sido tratados no resultaría de aplicación la normativa de protección de datos.

- **¿Y un proyecto de obra de edificación en un expediente de licencia urbanística o proyecto de obra pública?**

En lo que respecta a los proyectos de obra de edificación en un expediente de licencia urbanística privada o de obra pública, desde el punto de vista de la aplicación de los límites establecidos en el artículo 15 de la Ley 19/2013, de 9 de diciembre, debe tenerse en cuenta que dichos documentos pueden contener datos personales, tales como los relativos a los técnicos, o también el de los contratistas o el titular de la licencia cuando sean personas físicas, etc., por lo que en tales casos deberá acudirse a la ponderación exigida por el artículo 15 de la Ley 19/2013, de 9 de diciembre, o a la disociación de los datos personales obrantes en los documentos.

Ahora bien, debe tenerse en cuenta que el texto refundido de la Ley del Suelo y Rehabilitación Urbana, aprobado por Real Decreto Legislativo 7/2015, de 30 de octubre, reconoce en su artículo 5.f) a todos los ciudadanos el derecho a *"Ejercer la acción pública para hacer respetar las determinaciones de la ordenación territorial y urbanística, así como las decisiones resultantes de los procedimientos de evaluación ambiental de los instrumentos que las contienen y de los proyectos para su ejecución, en los términos dispuestos por su legislación reguladora."*

Por consiguiente durante el período en que puede ejercerse la acción pública urbanística, cabrá acceder a los datos personales contenidos en los expedientes de licencia urbanística por cualquier persona en el ejercicio de dicha acción, transcurrido dicho plazo será preciso acudir a lo previsto en la Ley 19/2013, de 9 de diciembre, en los términos citados.

- **¿Y podrían facilitarse datos tributarios obrantes en los expedientes administrativos?**

La Ley 19/2013, de 9 de diciembre, dispone que "*Se regirán por su normativa específica, y por esta Ley con carácter supletorio, aquellas materias que tengan previsto un régimen jurídico específico de acceso a la información.*"

Este sería el caso de los datos tributarios obrantes en el Ayuntamiento, en tanto que la hacienda de las entidades locales, tal y como declara el artículo 2.2 del Real Decreto Legislativo 2/2004, de 5 de marzo, por el que se aprueba el Texto Refundido de la Ley Reguladora de las Haciendas Locales "ostentará las prerrogativas establecidas legalmente para la Hacienda del Estado y actuará, en su caso, conforme a los procedimientos administrativos correspondientes". Ello supone que en el ejercicio de sus competencias, resultarán de aplicación a las haciendas locales las mismas prerrogativas que la Ley General Tributaria atribuye a la hacienda estatal, y en particular en lo que al acceso a los datos tributarios respecta, resulta de aplicación el artículo 95 de la Ley 57/2003, de 17 de diciembre, General Tributaria, que declara que tales datos tienen carácter reservado y permite ceder los mismos solamente en los casos que taxativamente enumera, por lo que fuera de tales supuestos no cabe su comunicación.

- **¿Se puede notificar la resolución de un procedimiento administrativo de forma conjunta a todos los interesados incluyendo todos sus datos de contacto?**

En este caso, no resulta preciso que los datos de contacto (domicilio, dirección de correo electrónico, número de teléfono) de los interesados sean comunicados al resto aunque figuren en documentos que les deban ser trasladados, ya que podría ser contrario al principio de minimización de datos del RGPD.

Enlaces

Real Decreto Legislativo 7/2015, de 30 de octubre	https://www.boe.es/buscar/act.php?id=BOE-A-2015-11723

COMUNICACIÓN DE DATOS PERSONALES.

- **¿Podría la policía local de un Ayuntamiento comunicar a la Policía Nacional la existencia de una posible infracción en materia de extranjería de unos ciudadanos?**

Los datos de los ciudadanos que presuntamente han cometido una infracción en materia de extranjería, podrían comunicarse por la policía local a la policía nacional, ya que existe

La Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad (ver artículos 1.4; 2; 3; y 53) cohonestada con la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social, en su artículo 53.1.a) considera una infracción grave " Encontrarse irregularmente en territorio español, por no haber obtenido la prórroga de estancia, carecer de autorización de residencia o tener caducada más de tres meses la mencionada autorización, y siempre que el interesado no hubiere solicitado la renovación de la misma en el plazo previsto reglamentariamente."

En este sentido, debe tenerse en cuenta el ejercicio de un poder público, como es la seguridad pública que es ejercida a través de las Fuerzas y Cuerpos de Seguridad.

- **En el anverso o reverso de un sobre que contiene la notificación de una multa ¿Puede reflejarse la cuantía de la misma así como la sanción que se impone? Y si es una multa de tráfico ¿Se podría incluir la matrícula del coche?**

Los datos que deben aparecer en la parte visible de la notificación deben ser los mínimos imprescindibles para que pueda practicarse la misma: nombre y apellidos y domicilio del destinatario o la referencia del expediente administrativo, sin que deban incluirse otros datos que puedan revelar claramente a terceros una condición desfavorable del destinatario.

- **¿Puede una Comunidad Autónoma facilitar a un Ayuntamiento los datos de las personas que reciben la Renta Mínima de Inserción para que ese Ayuntamiento pueda ofrecer a esas personas sus servicios públicos de carácter social?**

Ambas Administraciones, tanto la de carácter Autonómico como la de carácter Local, ostentan competencias en materia de servicios sociales, es decir, llevan a cabo, a efectos de la legitimación para el tratamiento de datos contemplada en el RGPD, una misión de interés público o poder público., por lo que se podrían comunicar esos datos de carácter personal.

En todo caso, una vez que los datos hayan sido comunicados al Ayuntamiento, y atendiendo al principio de limitación de la finalidad del artículo 5 del RGPD, únicamente se podrán utilizar para ofrecer los servicios sociales que presta el citado ente local.

- **¿Podría comunicarse por parte de un Ayuntamiento, los datos de los menores en situación de riesgos, a una Mancomunidad que presta servicios sociales?**

Como punto de partida, las mancomunidades están constituidas por la agrupación voluntaria de municipios, para la gestión de servicios comunes o la coordinación de diversas actuaciones,

tratándose en el presente supuesto de una mancomunidad que presta servicios sociales, y entre los mismos, se encuentran los relativos a actuaciones para proteger al menor.

Debemos partir de la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, cuyo artículo 14 establece la obligación de prestar la atención inmediata que precise cualquier menor, de actuar si corresponde a su ámbito de competencias o de dar traslado en otro caso al órgano competente y de poner los hechos en conocimiento de los representantes legales del menor, o cuando sea necesario, del Ministerio Fiscal, y en el artículo 16 se señala que son las entidades públicas competentes en materia de protección de menores las obligadas a verificar y evaluar las situaciones de desprotección que se hayan denunciado, adoptando las medidas necesarias para resolverla.

Además, también procede considerar los artículos 13, 17 y 18 de la mencionada Ley Orgánica, así como la posible existencia de normativa autonómica del ámbito territorial de los municipios agrupados en forma de mancomunidad, tanto de carácter local como la referida a servicios sociales o atención a la infancia.

Es decir, a los efectos de lo dispuesto en el RGPD, se trataría de una misión de interés público como es proteger a los menores.

En consecuencia, la comunicación de la información solicitada deberá circunscribirse a la estrictamente necesaria, en relación con la misión de interés público que realice esa Mancomunidad y que estará estrechamente ligado con sus competencias y su ámbito territorial de actuación.

En definitiva, el principio de interés superior del menor no ampara una comunicación masiva de datos a los servicios sociales de la Mancomunidad. Dicha comunicación sólo podrá tener lugar siempre que venga referida a supuestos concretos, y siempre que los datos sean necesarios para el ejercicio de competencias propias de los organismos públicos cesionarios.

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 atribuidas legalmente, precisaría de otra legitimación específica a la luz de las normas de protección de datos de carácter personal.

- **El secretario-interventor de un Ayuntamiento ¿Podría acceder a los expedientes completos de ayudas sociales concedidas?**

Como punto de partida, son expedientes en los que se tratan categorías especiales de datos, el interventor no forma parte de la comisión de servicios sociales y se le entrega el informe de valoración.

De esta forma, para habilitar la comunicación, debemos considerar la legitimación para el tratamiento de las categorías especiales de datos contempladas en el artículo 9 del RGPD.

En este sentido, el Real Decreto Legislativo 2/2004, de 5 de marzo, por el que se aprueba texto refundido de la Ley Reguladora de las Haciendas Locales, al regular el control y fiscalización de la actuación financiera de las corporaciones locales dispone en su artículo 213 que "*Se ejercerán en las entidades locales con la extensión y efectos que se determina en los artículos*

siguientes las funciones de control interno respecto de su gestión económica, de los organismos autónomos y de las sociedades mercantiles de ellas dependientes, en su triple acepción de función interventora, función de control financiero y función de control de eficacia."

El artículo 214 de la misma norma determina el ámbito de aplicación y las modalidades de ejercicio de la función interventora estableciendo que:

"1. La función interventora tendrá por objeto fiscalizar todos los actos de las entidades locales y de sus organismos autónomos que den lugar al reconocimiento y liquidación de derechos y obligaciones o gastos de contenido económico, los ingresos y pagos que de aquéllos se deriven, y la recaudación, inversión y aplicación, en general, de los caudales públicos administrados, con el fin de que la gestión se ajuste a las disposiciones aplicables en cada caso.

2. El ejercicio de la expresada función comprenderá:

a) La intervención crítica o previa de todo acto, documento o expediente susceptible de producir derechos u obligaciones de contenido económico o movimiento de fondos de valores.

b) La intervención formal de la ordenación del pago.

c) La intervención material del pago.

d) La intervención y comprobación material de las inversiones y de la aplicación de las subvenciones."

La fiscalización previa constituye así un control de legalidad respecto del cumplimiento de los requisitos a que debe someterse la concesión de ayudas de contenido económico y su extensión viene fijada en la propia norma, dispone así respecto de las facultades del personal controlador su artículo 222 lo siguiente:

"Los funcionarios que tengan a su cargo la función interventora así como los que se designen para llevar a efecto los controles financiero y de eficacia, ejercerán su función con plena independencia y podrán recabar cuantos antecedentes consideren necesarios, efectuar el examen y comprobación de los libros, cuentas y documentos que consideren precisos, verificar arqueos y recuentos y solicitar de quien corresponda, cuando la naturaleza del acto, documento o expediente que deba ser intervenido lo requiera, los informes técnicos y asesoramientos que estimen necesarios."

Por consiguiente, la fiscalización previa efectuada por el interventor de la entidad local, consistente en la verificación del cumplimiento de los requisitos legales necesarios, en el presente supuesto para la ordenación del pago, mediante el examen de todos los documentos que integran el expediente, supondría un tratamiento por razones interés público a los efectos de la legitimación contemplada por el artículo 9.2.g) del RGPD.

- **La policía local ¿Podría acceder a la relación de beneficiarios de tarjetas de estacionamiento para vehículos que transportan a personas con movilidad reducida del municipio para controlar con más eficacia el uso fraudulento de dichas tarjetas?**

El artículo 1.4 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, señala que, "el mantenimiento de la seguridad pública se ejercerá por las

distintas Administraciones Públicas a través de las Fuerzas y Cuerpos de Seguridad", entre las que se incluyen, según el artículo 2 de la propia Ley "Las Fuerzas y Cuerpos de Seguridad del Estado dependientes del Gobierno de la nación, los Cuerpos de Policía dependientes de las Comunidades Autónomas y los Cuerpos de Policía dependientes de las Corporaciones Locales".

El artículo 53.1.d) de dicha Ley Orgánica, señala que los Cuerpos de Policía Local deberán ejercer la función de Policía Administrativa, en lo relativo a las Ordenanzas, Bandos y demás disposiciones municipales dentro del ámbito de su competencia.

Por su parte, en el artículo 7.b) del Real Decreto Legislativo 6/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley sobre tráfico, circulación de vehículos a motor y seguridad vial, atribuye a los municipios *"La regulación mediante ordenanza municipal de circulación, de los usos de las vías urbanas, haciendo compatible la equitativa distribución de los aparcamientos entre todos los usuarios con la necesaria fluidez del tráfico rodado y con el uso peatonal de las calles, así como el establecimiento de medidas de estacionamiento limitado, con el fin de garantizar la rotación de los aparcamientos, prestando especial atención a las necesidades de las personas con discapacidad que tienen reducida su movilidad y que utilizan vehículos, todo ello con el fin de favorecer su integración social".*

En este sentido, la ordenanza que regule la tarjeta de estacionamiento de vehículos para personas con movilidad reducida puede atribuir a la policía local la comprobación de los datos contenidas en ella.

Por lo tanto, no habría inconveniente para que en el ejercicio de funciones específicas de comprobación y control de cumplimiento de las condiciones de uso de las referidas tarjetas, el Servicio Municipal de la Policía Local del municipio acceda a los datos contenidos en el fichero municipal oportuno, siempre que:

- Se asegure que se utilizan únicamente aquellos datos, atendiendo al principio de minimización de datos que son adecuados, pertinentes y limitados a lo necesario;
- La comunicación se realice en el marco de situaciones concretas y con necesidades debidamente justificadas, relacionadas con las funciones propias de la Policía Local; y
- Se garanticen la confidencialidad y seguridad de los datos personales.

En todo caso, la petición deberá dirigirse al responsable del tratamiento que es el que tiene la posibilidad de decidir sobre el contenido y uso del fichero.

Este criterio impediría la incorporación en bloque de la totalidad de los datos contenidos en los ficheros municipales a los ficheros de la Policía Local, siendo no obstante conforme a derecho la comunicación concreta de determinados datos, debidamente individualizados, cuando se solicite en el marco de las competencias atribuidas a la policía Municipal por la Ley Orgánica 2/1986, de 13 de marzo.

No obstante, es posible habilitar los medios técnicos necesarios para que la comunicación de datos planteada se realice de acuerdo con las limitaciones que la Legislación contempla y a la que hemos hecho referencia en párrafos anteriores.

Por consiguiente, el acceso o comunicación de los datos deberá ir presidido por una petición en la que pueda quedar identificado el funcionario o responsable de la policía que efectúa la petición e identificada la finalidad concreta para la que se necesitan los datos.

Enlaces

Ley Orgánica 4/2000, de 11 de enero	https://www.boe.es/buscar/act.php?id=BOE-A-2000-544
Ley Orgánica 1/1996, de 15 de enero	https://www.boe.es/buscar/act.php?id=BOE-A-1996-1069
Real Decreto Legislativo 2/2004	https://www.boe.es/buscar/act.php?id=BOE-A-2004-4214

OTRAS CUESTIONES.

- **¿Puede un ente local usar el número de móvil de los ciudadanos para enviar comunicaciones a través de sistemas de mensajería instantánea?**

Uno de los principios relativos al tratamiento que recoge el RGPD es el referente a que los datos personales serán recogidos con fines determinados, explícitos y legítimos, no siendo tratados ulteriormente de manera incompatible con dichos fines.

De esta forma, si el ente local hubiese recabado el dato del móvil para una finalidad determinada (por ejemplo, en la presentación de una denuncia), el uso de este dato para enviar dichas comunicaciones sería incompatible, por lo que para realizar el citado envío sería necesario el consentimiento previo de los ciudadanos, además de informarles del tratamiento que se va a realizar respecto a ese dato de carácter personal.

- **Cuándo se gestiona un servicio público por un tercero ¿Es responsable o encargado del tratamiento de los datos personales necesarios para prestar dicho servicio?**

Aunque ya nos hemos referido en el apartado 3.7 de esta Guía a este supuesto, conviene volver a incidir en él, partiendo de que la la relación entre responsable y encargado deberá estar regulada en un contrato o instrumento jurídico.

En este sentido, en la gestión de servicios públicos a través de un tercero, y conforme a lo que al respecto prevé el proyecto de Ley Orgánica de Protección de Datos que se está tramitando, este tercero ostentará también la condición de encargado de tratamiento.

- **¿Qué consideración ostentan las Diputaciones Provinciales, a efectos de la normativa de protección de datos, cuando prestan servicios a los Ayuntamientos?**

La Ley de Bases de Régimen Local atribuye a las Diputaciones Provinciales la asistencia y cooperación jurídica, económica y técnica a los Municipios, especialmente en aquellos que ostenten menor capacidad económica y de gestión.

En estos supuestos de prestación de servicios, en la medida que suponga un tratamiento de datos de carácter personal, las citadas Diputaciones, a efectos de lo previsto en el RGPD, actuarían como encargados de tratamiento

- **¿Se debe dar cumplimiento al derecho de información cuando se recaban datos personales a través de llamadas y correos electrónicos?**

El RGPD regula el derecho de información en sus artículos 13 y 14, además de que uno de los principios relativos al tratamiento que recoge la norma es el relativo a la transparencia.

Por tanto, en ambos supuestos se debe dar cumplimiento al derecho de información. Así, tal y como se expone en la Guía para el cumplimiento del deber de informar, en el caso telefónico se puede facilitar la información básica mediante una locución clara y concisa, y el resto del contenido de este derecho a través de otro medio adicional que se ponga a disposición del afectado.

En el supuesto del correo electrónico, en la primera comunicación respecto al ciudadano que haya remitido el mismo, se le podría facilitar la información básica y un enlace en el cuál pueda obtener el contenido de la información de la segunda capa.

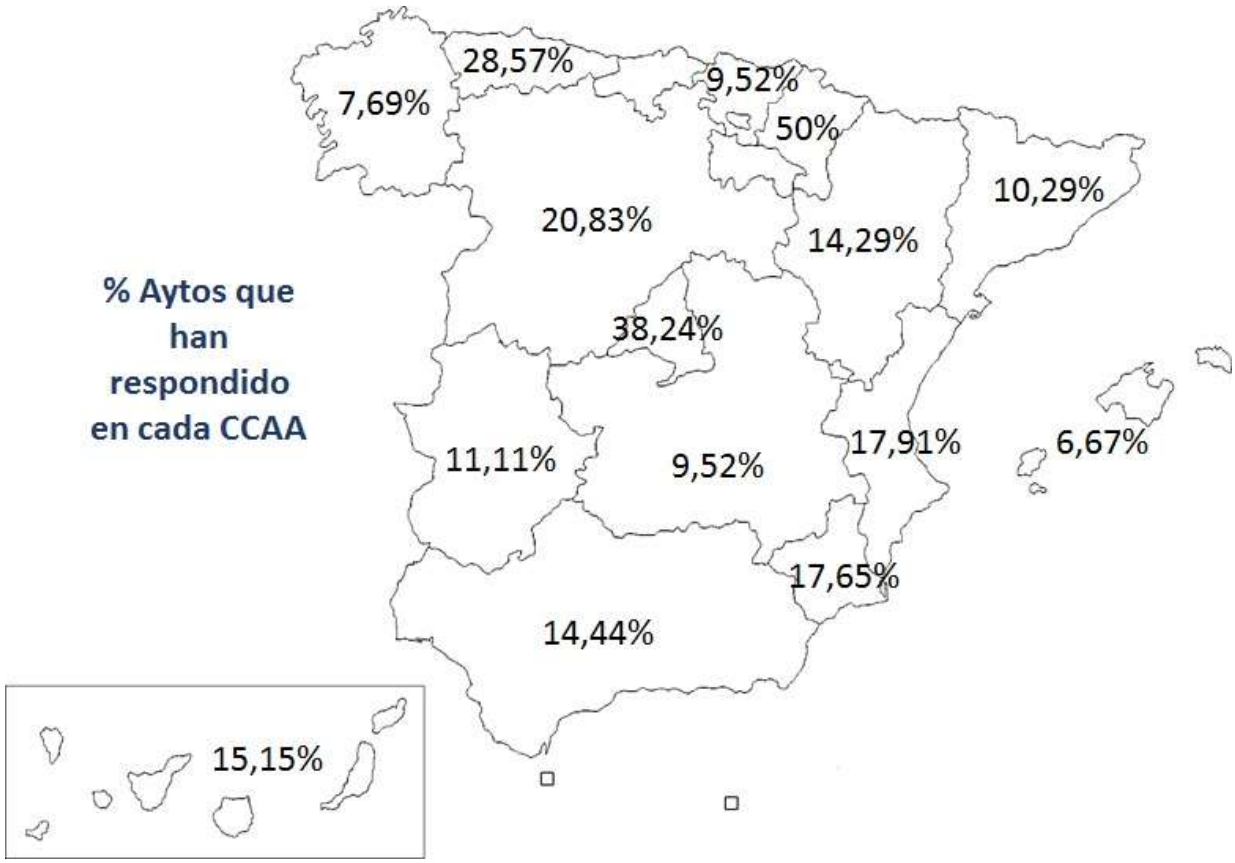
DECÁLOGO DE INCUMPLIMIENTOS MÁS FRECUENTES EN LA AA.LL.

Decálogo de incumplimientos más frecuentes en la AALL

ADAPTACIÓN DE LAS EELL AL RGPD

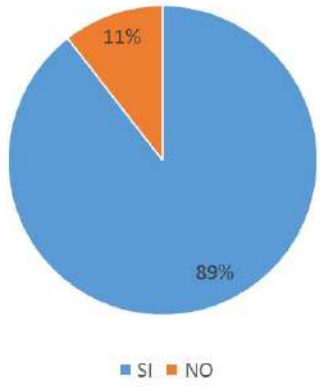
Estudio realizado en Octubre de 2017

Resultados en Ayuntamientos de más de 20.000 habitantes

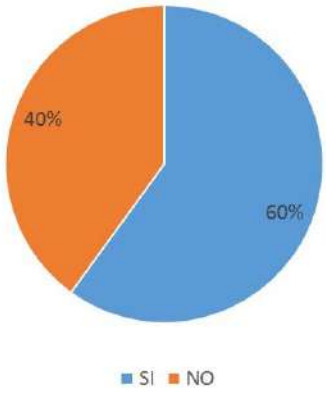


Resultados encuesta RGPD

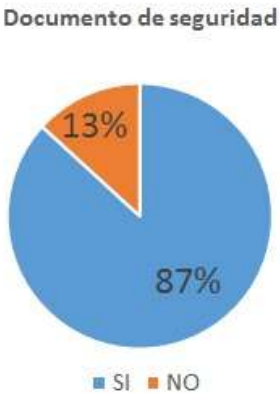
Conoce la existencia del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y

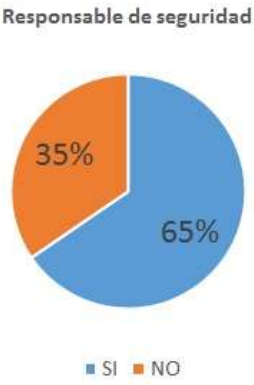


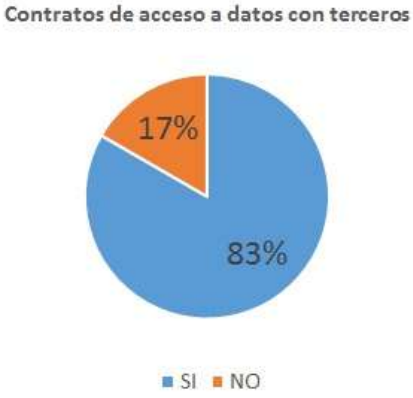
Conoce las implicaciones y cambios que el RGPD establece frente a la actual normativa Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD) y el Real Decreto 1720/2007, de 21 de diciembre, por el que se a



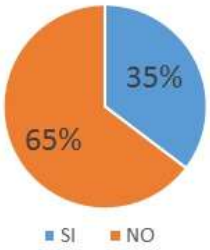
Dispone el Ayuntamiento de algunas de las siguientes medidas:



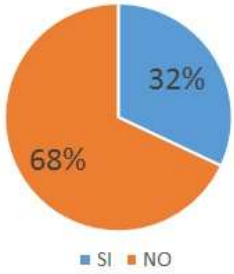




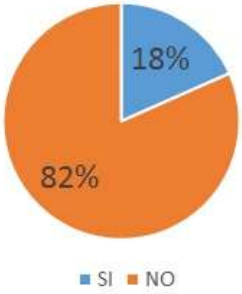
Plan de seguridad acorde con el Esquema Nacional de Seguridad



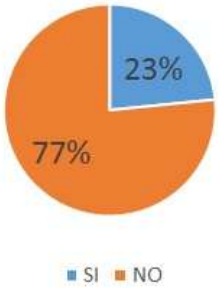
Análisis de riesgos en protección de datos



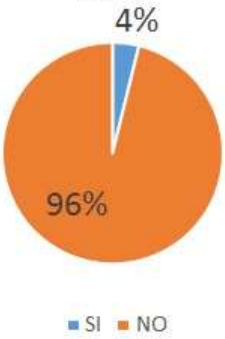
Evaluación de impacto en la protección de datos



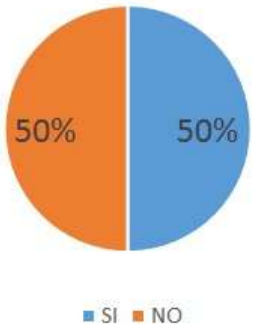
Creación del Registro de las Actividades en relación con los tratamientos de datos de su responsabilidad



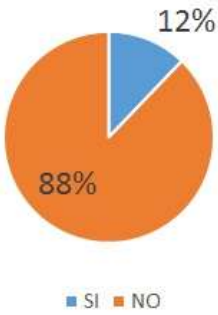
Nombramiento de un Delegado de Protección de Datos (DPO)



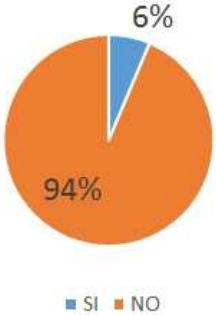
Información y transparencia del tratamiento



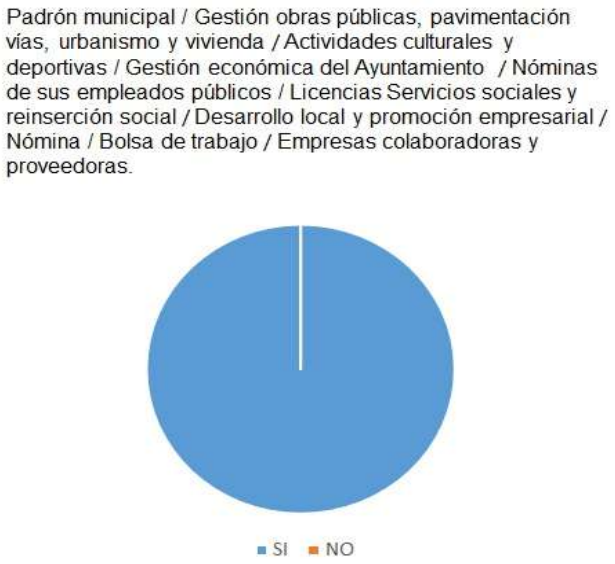
Sustitución de los contratos de acceso a datos por contratos de encargo de tratamiento

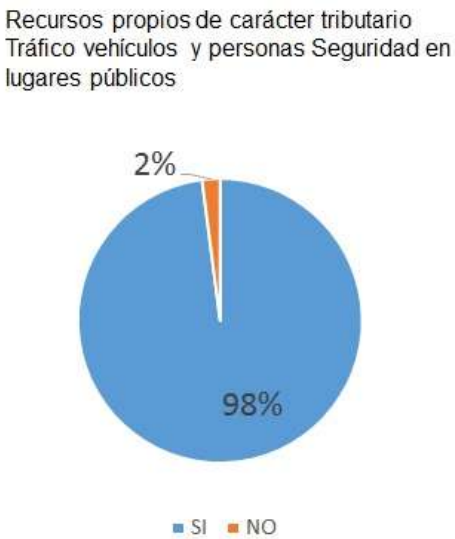


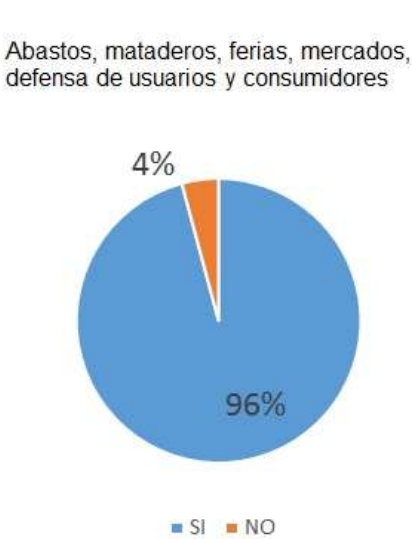
Protocolo de notificación de brechas de seguridad a la Agencia Española de Protección de Datos

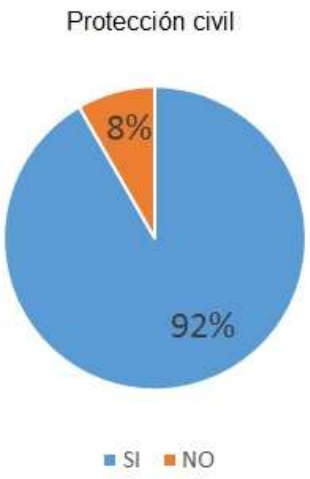


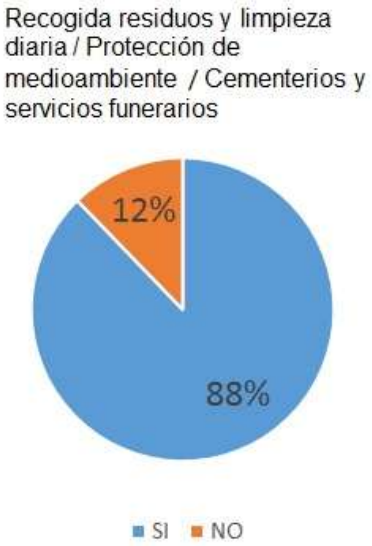
Gestiona el Ayuntamiento alguno de los siguientes recursos, procesos o funciones

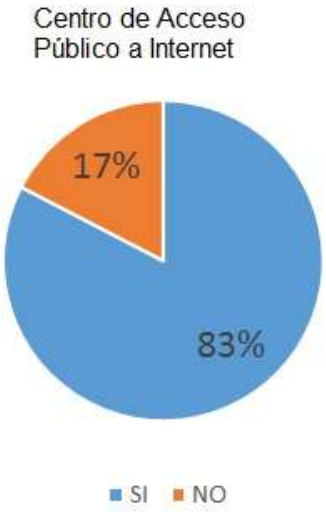


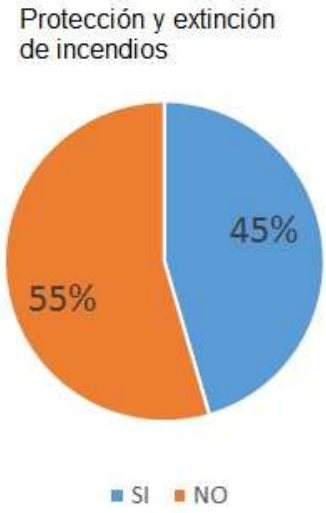


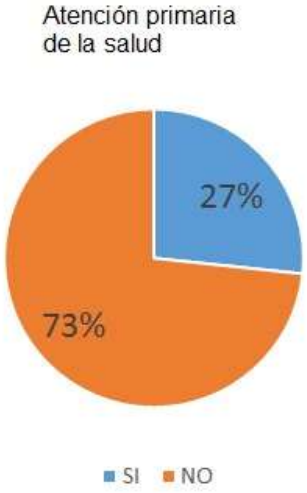



Protección civil
8%
92%
SI
NO


Recogida residuos y limpieza diaria / Protección de medioambiente / Cementerios y servicios funerarios
12%
88%
SI
NO


Centro de Acceso Público a Internet
17%
83%
SI
NO


Protección y extinción de incendios
45%
55%
SI
NO


Atención primaria de la salud
27%
73%
SI
NO

ADAPTACIÓN DE LAS EELL AL RGPD

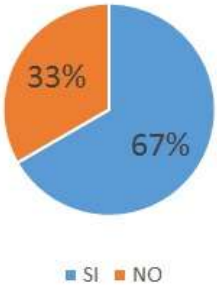
Estudio realizado en Octubre de 2017

Resultados en Diputaciones Provinciales, Cabildos y Consejos Insulares

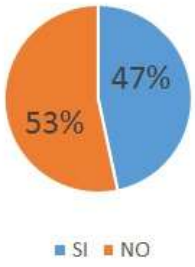
Resultados encuesta RGPD (Dip/Cab/Con)

Diputaciones Provinciales, Cabildos y Consejos Insulares participantes y CAST

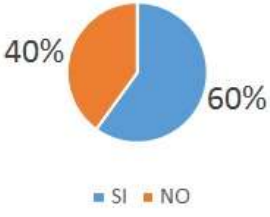
Ha realizado la Diputación/Cabildo/Consejo proyectos de adecuación de los ayuntamientos a la LOPD.



La Diputación/Cabildo/Consejo dispone de un servicio de asesoramiento en temas relacionados con la protección de datos

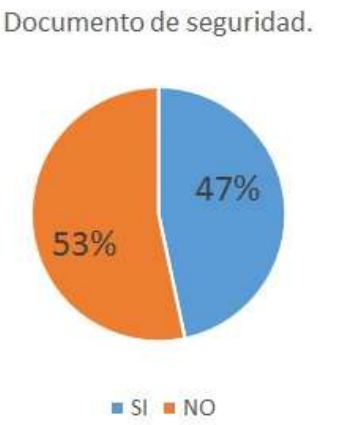


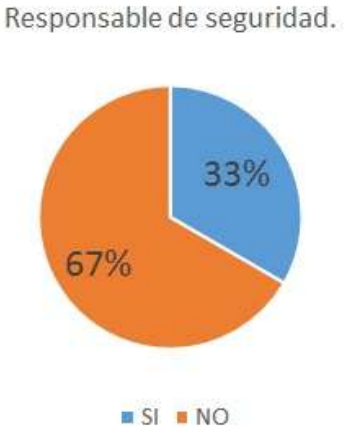
En el caso de que la Diputación/Cabildo/Consejo preste servicios a los ayuntamientos que conlleven el tratamiento de datos de carácter personal, se ha establecido el correspondiente contrato de encargado de tratamiento.



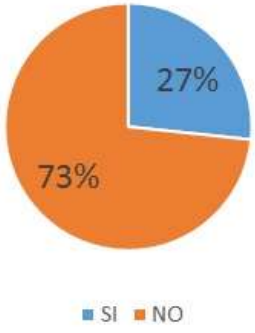
La Diputación/Cabildo/Consejo ha realizado tareas de formación y difusión de las principales novedades y obligación que conlleva el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

Disponen los Ayuntamientos de su competencia de algunas de las siguientes medidas

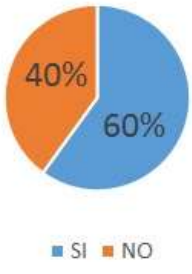




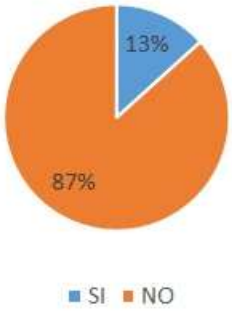
Contratos de acceso a datos con terceros



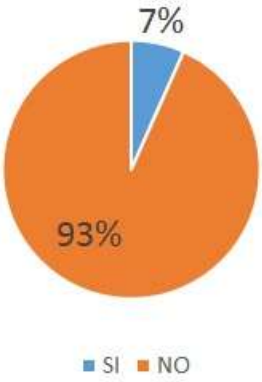
Textos informativos de protección de datos en los formularios de recogida de datos disponibles para los ciudadanos



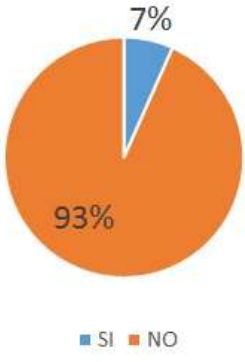
Plan de seguridad acorde con el Esquema Nacional de Seguridad



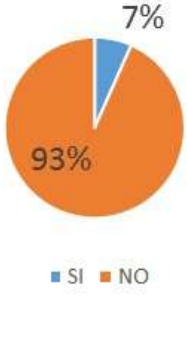
Análisis de riesgos en protección de datos.



Evaluación de impacto en la protección de datos

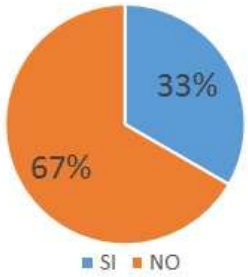


Creación del Registro de las Actividades en relación con los tratamientos de datos de su responsabilidad.

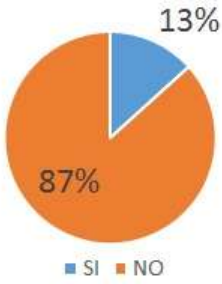


Nombramiento de un Delegado de Protección de Datos (DPO).

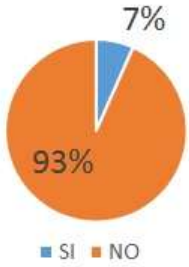
Información y transparencia del tratamiento



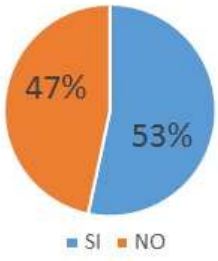
Sustitución de los contratos de acceso a datos por contratos de encargo de tratamiento



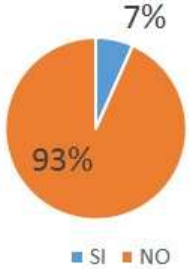
Protocolo de notificación de brechas de seguridad a la Agencia Española de Protección de Datos



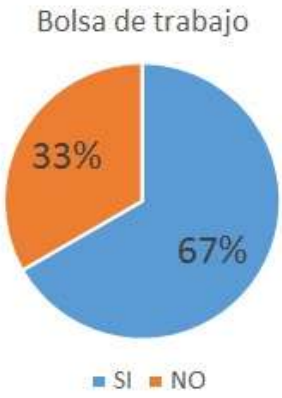
Protocolo para garantizar los derechos de acceso, rectificación, cancelación y oposición

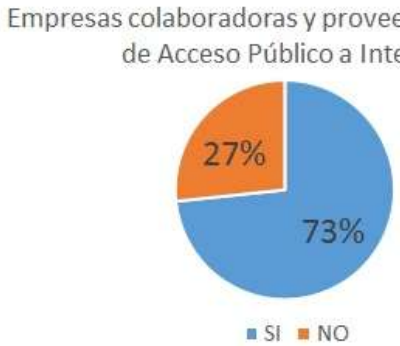


Protocolo para garantizar los derechos de supresión, limitación al tratamiento y portabilidad



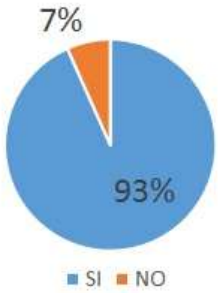
Gestionan los Ayuntamientos de su competencia alguno de los siguientes recursos, procesos o funciones



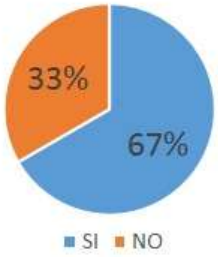


Servicios de titularidad municipal prestados por la Diputación/Cabildo/Consejo que implican tratamientos de datos de carácter personal

Recaudación de impuestos municipales / Contabilidad

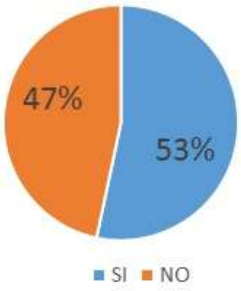


Servicios Sociales / Servicios de administración electrónica / Servicios de copias de seguridad

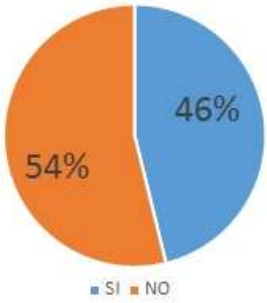


Servicios de micro-informática y asistencia técnica informática / Gestión de actividades deportivas y/o culturales /

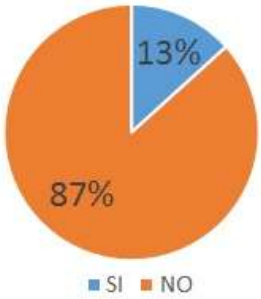
Servicios de urbanismo / Extinción de incendios



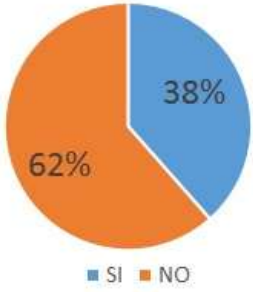
Servicios de agricultura y medio-ambiente



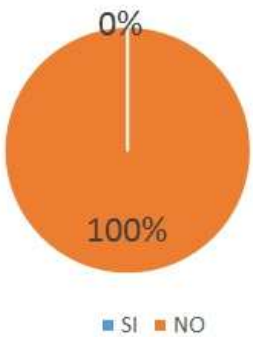
Oficina de atención al consumidor



Gestión de la contratación / Compra centralizada



Gestión de servicios de limpieza



GRUPO DE TRABAJO

Coordinador:

- **Lluís Sanz Marco**. Director de Información de Base del Ayuntamiento de Barcelona.

Responsable FEMP:

- **Pablo Mª Bárcenas**, Secretario de la Comisión de Sociedad de la Información y Tecnologías de la FEMP.

Integrantes:

- **Enric García de Pedro**, Responsable técnico LOPD del Ayuntamiento de Barcelona
- **Virginia Moreno**, Directora de Tecnologías e Innovación del Ayuntamiento de Leganés.
- **Ascen Moro**, Responsable técnico LOPD (Organización) del Ayuntamiento de Sant Feliu de Llobregat
- **Concepción Campos**, Secretaria General de la Junta de Gobierno del Ayuntamiento de Vigo
- **Javier Peña**, Jefe de Sección del Servicio de Modernización Administrativa y Nuevas Tecnologías de la Información y las Comunicaciones de la Diputación Provincial de Burgos
- **Jesús Rubí**, Adjunto a la Directora de la Agencia Española de Protección de Datos
- **Rafael García Gozalo**, Vocal Asesor Jefe del Departamento Internacional de la Agencia Española de Protección de Datos
- **Ricard Martínez Martínez**, Director de la Cátedra Microsoft sobre Privacidad y Transformación Digital de la Universidad Valencia
- **Ana Marzo**, Socia Fundadora del Equipo Marzo, Despacho Jurídico
- **Miguel Angel Lubian**, Director del Instituto CIES