PROTECCIÓN DE DATOS Y ADMINISTRACIÓN LOCAL

GUÍAS SECTORIALES AEPD

Con la colaboración de:

PROTECCIÓN DE DATOS Y ADMINISTRACIÓN LOCAL

GUÍAS SECTORIALES AEPD

Con la colaboración de:

ÍNDICE

INTRODUCCIÓN

PRESENTACIÓN

1. CONCEPTOS BÁSICOS
- 1.1. ¿Qué es un dato de carácter personal?
- 1.2. ¿Qué es un tratamiento de datos de carácter personal?
- 1.3. ¿Quién es el responsable del tratamiento?
- 1.4. ¿Quién es el encargado del tratamiento?
- 1.5. ¿Cuáles son los principios aplicables al tratamiento de datos personales?

2. ADECUACIÓN AL RGPD DE LOS TRATAMIENTOS DE DATOS DE LA ADMINISTRACIÓN LOCAL
- 2.1. El principio de responsabilidad proactiva
- 2.2. Identificación de la legitimación en el tratamiento de datos
  - 2.2.1. Interés público o poderes públicos y cumplimiento de obligación legal
  - 2.2.2. Consentimiento
  - 2.2.3. El consentimiento del artículo 28.2 de la Ley 39/2015, de 1 de octubre
  - 2.2.4. Tratamiento de categorías especiales de datos
- 2.3. Del registro de ficheros al registro de actividades de tratamiento
- 2.4. Seguridad en el tratamiento de los datos personales.
  - 2.4.1. Análisis de riesgos
  - 2.4.2. Medidas de seguridad
  - 2.4.3. Comunicación de quiebras de seguridad de los datos personales
- 2.5. Evaluaciones de Impacto en la Protección de Datos
  - 2.5.1. ¿Qué es una evaluación de impacto en la protección de datos?
  - 2.5.2. Especial referencia a las "Smart cities"
- 2.6. Privacidad desde el diseño y por defecto
- 2.7. Cumplimiento del principio de transparencia: el derecho de información en la recogida de datos personales
- 2.8. Administración Local y sus encargados de tratamiento
- 2.9. El Delegado de Protección de Datos
- 2.10. Transferencias internacionales de datos
- 2.11. Los derechos de los afectados

3. CONSULTAS FRECUENTES
- 3.1. Padrón municipal de habitantes
- 3.2. Pleno y concejales
- 3.3. Publicación de datos
- 3.4. Tratamiento de datos en el marco funcionarial y laboral
- 3.5. Videovigilancia
- 3.6. Acceso a expedientes administrativos y Ley de Transparencia
- 3.7. Comunicación de datos personales
- 3.8. Otras cuestiones

4. MATERIALES DE AYUDA PARA ADECUARSE AL RGPD

5.ANEXOS
- La Protección de Datos en ayuntamientos de más de 20.000 habitantes
- La Protección de Datos en Diputaciones Provinciales, Cabildos y Consejos Insulares

PRESENTACIÓN

En el año 2016, la Unión Europea aprobó el ***Reglamento General de Protección de Datos (RGPD)*** que, si bien entró en vigor en mayo de ese año, es 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.

Es decir, esta norma europea, además de desplazar a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su Reglamento de Desarrollo, introduce una serie de cambios en los tratamientos de datos de personales que realicen los responsables, así como los denominados encargados.

Así, se introducen, entre otros, el principio de responsabilidad activa, el principio de minimización de datos personales, la figura del Delegado de Protección de Datos, la Privacidad desde el Diseño, la Privacidad por Defecto, las notificaciones de quiebras de seguridad que puedan afectar a los datos personales y las Evaluaciones de impacto en la protección de datos.

Otras de las novedades es la supresión de la inscripción de ficheros, si bien responsables y encargados deberán configurar el denominado Registro de Actividades de Tratamiento, así como el contenido del derecho de información en la recogida de datos que debe facilitarse a los afectados, puesto que se amplía considerablemente.

Además, en lo referente a seguridad, el ***RGPD*** no parte de una configuración de medidas de seguridad en función de si atendiendo a los diferentes tipos de tratamiento les corresponde unas medidas de seguridad de nivel bajo, medio o alto, sino que se tendrá que partir de un análisis de riesgo inicial de los tratamientos y que a partir de los resultados obtenidos del mismo, se implementen las medidas de seguridad.

Junto con el *RGPD*, se encuentra en tramitación una nueva ***Ley Orgánica de Protección de Datos*** que complemente el citado ***RGPD***, puesto que dicha norma permite que los Estados desarrollen determinadas materias.

En este sentido, la ***Agencia Española de Protección de Datos (AEPD)***, consciente de la importancia de este cambio normativo, ha elaborado una serie de materiales cuya finalidad principal es facilitar que tanto responsables como encargados estén en condiciones de cumplir con los principios, derechos y garantías que establece el ***RGPD***.

Así, se ha creado una ***sección*** en la página web de la ***AEPD*** dedicada específicamente al ***RGPD***, en la que se han publicado diversos materiales al respecto, entre ellos, el ***Impacto del RGPD en las Administraciones Públicas***, el ***Delegado de Protección de Datos en las Administraciones Públicas***, la ***Guía del Reglamento General de Protección de Datos para responsables***, la ***Guía para el cumplimiento del deber de informar***, las ***Directrices para la elaboración de contratos entre responsables y encargados***, la ***Guía práctica de análisis de riesgos en los tratamientos de datos sujetos al RGPD, y la Guía práctica para las evaluaciones de impacto en la protección de datos sujetos al RGPD***.

Obviamente, entre los afectados por este cambio normativo se encuentran los Entes que integran la denominada Administración Local en relación con los tratamientos de datos de carácter personal que realicen.

PULSA SOBRE LAS PALABRAS EN ***CURSIVA*** O EL SÍMBOLO , PARA OBTENER INFORMACIÓN ADICIONAL

Respecto a estos tratamientos, y a modo de ejemplo, podemos citar el padrón municipal de habitantes, la gestión de los tributos de ámbito municipal, o subvenciones, así como la ingente cantidad de datos que pueden recabarse a través de lo que se conoce con el nombre de "smart cities".

En consecuencia, en esta Guía se analizan los aspectos más relevantes del ***RGPD*** en relación con los tratamientos de datos de la Administración Local. La Guía se completa, además, con un catálogo de preguntas frecuentes relativas a estos tratamientos, adaptadas al ***RGPD***.

Por último, indicar que en la presente Guía para referirse al titular de los datos se ha utilizado el término "afectado" y no "interesado" como recoge el ***RGPD***, para no confundirlo con el concepto de interesado que regula la ***Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas***.

1. CONCEPTOS BÁSICOS

1.1. ¿QUÉ ES UN DATO DE CARÁCTER PERSONAL?

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

Para facilitar la comprensión de esta definición, el ***RPGD*** especifica que las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de "cookies" u otros identificadores, como etiquetas de radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser usados para elaborar perfiles de las personas físicas e identificarlas.

Asimismo, el ***RGPD*** define también qué se considera "dato de salud", "datos genéticos" y "datos biométricos" de la siguiente forma:

"Datos relativos a la salud": datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

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

Los datos genéticos ya tenían la consideración de datos especialmente protegidos en el marco de la Directiva 95/46, pero solo como parte de los datos relacionados con la salud. El ***RGPD*** los separa como categoría con entidad propia, al margen de su implicación en el terreno de la salud, con lo que extiende la protección especial a tratamientos relacionados, por ejemplo, con la filiación.

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

Respecto a esta definición hay que señalar que los datos biométricos tendrán la condición de datos sensibles solo cuando sean utilizados para identificar unívocamente a una persona. Una fotografía, por ejemplo, contiene datos biométricos, pero su tratamiento no está sometido a especiales condiciones salvo que se utilice para individualizar o identificar a alguien dentro de un colectivo más amplio.

También hay que indicar que la noción de dato biométrico es muy amplia e incluye aspectos cada vez más innovadores. Se consideran datos biométricos en la medida en que permiten identificar a una persona aspectos como el patrón venoso de una mano o la forma de caminar de una persona.

Los datos de salud forman parte de la categoría de "datos especialmente protegidos", junto con aquellos:

- Que revelen ideología, afiliación sindical, religión y creencias.
- Que hagan referencia al origen racial, o a la vida sexual.
- Que se refieran a la comisión de infracciones penales o administrativas.

El *RGPD* califica este tipo de datos como "categorías especiales de datos personales".

· EJEMPLO DE CATEGORÍAS DE DATOS PERSONALES OBJETO DE TRATAMIENTO POR LA ADMINISTRACIÓN LOCAL

- **De carácter identificativo** (nombre, apellidos, teléfono, imagen, DNI/NIF).
- **De carácter tributario** (en la gestión de los tributos municipales).
- **Académicos y profesionales** (en la gestión de procedimientos selectivos, bolsas de empleo, recursos humanos).
- **En el ejercicio de la potestad sancionadora** (aquellos derivados de la tramitación de expedientes sancionadores).
- **Categorías especiales de datos** (origen racial, salud o vida sexual en un servicio de atención a mujeres víctimas de violencia de género o en la prestación de servicios sociales).
- **La implementación de las "Smart Cities"** también puede conllevar un tratamiento de diferentes datos de carácter personal.

1.2. ¿QUÉ ES UN TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL?

Cualquier actividad en la que estén presentes datos de carácter personal constituirá un tratamiento de datos, ya se realice de manera manual o automatizada, total o parcialmente, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

La Administración Local, de conformidad con la normativa de régimen local, presta una serie de servicios públicos ligados a las diferentes competencias o funciones que llevan a cabo.

Para prestar los mismos, recaban y tratan datos de carácter personal de sus ciudadanos, que son tratados total o parcialmente de forma automatizada o no.

Asimismo, para identificar los tratamientos de los Ayuntamientos se deben tener presente las competencias de los mismos en función de la población:

EJEMPLOS DE TRATAMIENTOS POR LA ADMINISTRACIÓN LOCAL

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

1.3. ¿QUIÉN ES EL RESPONSABLE DEL TRATAMIENTO DE DATOS?

El responsable del tratamiento o responsable es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

En el ámbito de la Administración Local, el responsable del tratamiento, considerando la normativa de régimen local aplicable, recaerá en los municipios, diputaciones provinciales e islas.

No obstante, sobre estas últimas procede realizar la siguiente consideración:

- Las diputaciones provinciales, consejos y cabildos insulares, serán responsables de sus respectivos tratamientos, es decir, sobre aquellos sobre los que decidan los fines de los mismos (por ejemplo, el tratamiento de datos relativo a sus recursos humanos o videovigilancia de sus instalaciones).

- Respecto a aquellos tratamientos de datos derivados de la prestación de asistencia en favor de los municipios, serán encargados de tratamiento.

También ostentarán esta condición de responsables, en la medida que traten datos de carácter personal, las entidades de ámbito territorial inferior al municipal, las comarcas, las áreas metropolitanas y las mancomunidades. Asimismo, dicha condición también recaería sobre los entes que formen parte de la Administración Institucional de la Corporaciones Locales, como podría ser organismos autónomos y entidades públicas empresariales locales.

Los Ayuntamientos son responsables del tratamiento de datos personales que efectúen. Si cuentan con Administración Institucional, será responsable cada uno de los entes que formen parte de la misma respecto a los tratamientos que lleven a cabo.

1.4. ¿QUIÉN ES EL ENCARGADO DEL TRATAMIENTO?

Es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos por cuenta del responsable del tratamiento.

Por ejemplo, cuando un Ayuntamiento encarga a un tercero (una empresa):

- La elaboración de las nóminas de su personal
- La destrucción de documentación
- El control de las cámaras de videovigilancia
- Gestión del cobro de impuestos
- Mantenimiento de los equipos informáticos

La relación entre responsable y encargado deberá estar regulada en un contrato o instrumento jurídico, a la que nos referiremos más adelante en el apartado 3.8 de esta Guía, titulado "Administración Local y sus encargados de tratamiento".

1.5. ¿CUÁLES SON LOS PRINCIPIOS APLICABLES AL TRATAMIENTO DE DATOS PERSONALES?

El *RGPD* regula en sus artículos 5 a 11 los principios que deben cumplirse y respetarse cuando se realiza el tratamiento de datos personales de los afectados.

Dentro de estos principios podemos distinguir lo siguiente:

- Los comprendidos en el artículo 5.
- La licitud del tratamiento (supuestos que legitiman el tratamiento de los datos personales).
- Las condiciones para obtener el consentimiento, incluyendo lo referente al consentimiento de los menores.
- Las condiciones para tratar las categorías especiales de datos personales y para tratar los datos personales relativos a condenas e infracciones penales.

Respecto al artículo 5 del ***RGPD***, dicho precepto contiene a su vez los siguientes principios: Licitud, lealtad y transparencia.

Los datos personales serán tratados de manera lícita, leal y transparente en relación con el afectado.

· LICITUD, LEALTAD Y TRANSPARENCIA

Los datos personales serán tratados de manera lícita, leal y transparente en relación con el afectado.

· LIMITACIÓN DE LA FINALIDAD

Los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados de manera incompatible con dichos fines. No se considerará incompatible con los fines iniciales el tratamiento posterior de los datos con fines de archivo de interés público, fines de investigación científica e histórica o fines estadísticos.

· MINIMIZACIÓN DE DATOS

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

· EXACTITUD

Los datos personales serán exactos y si fuera necesario actualizados, adoptándose medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos a los fines para los que se tratan.

· LIMITACIÓN DEL PLAZO DE CONSERVACIÓN

Los datos personales serán mantenidos de forma que se permita la identificación de los afectados no más tiempo del necesario para los fines del tratamiento. Podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo de interés público, fines de investigación científica e histórica o fines estadísticos, sin perjuicio de la aplicación de las correspondientes medidas técnicas y organizativas apropiadas que impone el RGPD.

· INTEGRIDAD Y SEGURIDAD

Los datos personales serán tratados de manera que se garantice su adecuada seguridad, incluyendo la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, aplicando las medidas técnicas y de organización apropiadas.

· RESPONSABILIDAD PROACTIVA

El responsable del tratamiento será responsable de cumplir estos principios y capaz de demostrar dicho cumplimiento.

Por tanto, estos principios deben cumplirse por las Administraciones Locales cuando realicen el tratamiento de datos de carácter personal de los afectados.

2. ADECUACIÓN AL RGPD DE LOS TRATAMIENTOS DE LA ADMINISTRACIÓN LOCAL

2.1. EL PRINCIPIO DE RESPONSABILIDAD PROACTIVA.

Este concepto, como principio esencial en el tratamiento de datos personales, se establece en el artículo 5 del *RGPD* al que hemos hecho referencia anteriormente. En concreto, según su apartado 2, la responsabilidad proactiva es una de las obligaciones del responsable del tratamiento en relación a los principios referidos en el apartado 1 del mismo artículo. Por lo tanto, es una de las nuevas obligaciones que se establecen en el *RGPD* para asegurar el cumplimiento de dichos principios, y que consiste en la capacidad del responsable, es decir, de la organización, de demostrar y proporcionar evidencias de dicho cumplimiento.

El *RGPD* establece un catálogo de medidas que el responsable y, en ocasiones los encargados, deben aplicar para garantizar que los tratamientos son conformes a la norma europea.

A continuación se desglosan este catálogo de medidas que inciden en el mencionado principio de responsabilidad proactiva, y que además, puede tomarse en cuenta como *"hoja de ruta"* para adaptar los tratamientos al *RGPD*.

2.2. IDENTIFICACIÓN DE LA LEGITIMACIÓN EN EL TRATAMIENTO DE LOS DATOS PERSONALES

2.2.1. Interés público o poderes públicos y cumplimiento de obligación legal

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 Administraciones públicas 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 no puedan seguir llevándose a cabo. Significa que deberán encontrarse las bases jurídicas apropiadas para esos tratamientos dentro de las que el *RGPD* ofrece.
En particular, y para el ámbito de la Administración Local, 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.

· LEGITIMACIÓN EN EL TRATAMIENTO DE LOS DATOS PERSONALES: INTERÉS PÚBLICO / PODERES PÚBLICOS

En el ámbito de la Administración Local 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, debe existir una previsión normativa con rango de ley.

EJEMPLOS

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

PULSA SOBRE LAS PALABRAS EN *CURSIVA* O EL SÍMBOLO , PARA OBTENER INFORMACIÓN ADICIONAL

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.

2.2.2. Consentimiento

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 afectados 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 afectados, dejarán de ser válidos a partir del 25 de mayo de 2018, 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.

· LEGITIMACIÓN EN EL TRATAMIENTO DE LOS DATOS PERSONALES: CONSENTIMIENTO

Este consentimiento debe ser "inequívoco", lo que supone que se preste mediante una manifestación del afectado o mediante una clara acción afirmativa.

Así, no se consideran formas válidas de obtener el consentimiento el uso de casillas ya marcadas o la inacción.

En cambio, sí son acordes al *RGPD*, la utilización de una declaración por escrito, o la marcación de casillas en un sitio web de Internet.

EJEMPLOS

- La suscripción a través de un servicio ofrecido por un Ayuntamiento en su página web para recibir comunicaciones referidas a las actividades culturales.
- La inscripción en una bolsa de trabajo.

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

- Puede ser para uno o varios fines. En este caso:
  A. Sería posible agruparlas en virtud de su vinculación (por ejemplo, consentimiento para la recepción de publicidad propia o de terceros).
  B. 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 obtenerlo 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.

· LEGITIMACIÓN EN EL TRATAMIENTO DE LOS DATOS PERSONALES: CONSENTIMIENTO DE LOS MENORES

El ***RGPD*** determina que los Estados miembros pueden establecer por ley el consentimiento de los menores siempre que la edad no sea inferior a 13 años ni superior a 16.

En la actualidad, esa edad está fijada en los 14 años.

2.2.3. El consentimiento del artículo 28.2. de la *Ley 39/2015, de 1 de octubre*

Según el citado apartado 2 del artículo 28 de esta Ley, "Los interesados no estarán obligados a aportar documentos que hayan sido elaborados por cualquier Administración, con independencia de que la presentación de los citados documentos tenga carácter preceptivo o facultativo en el procedimiento de que se trate, siempre que el interesado haya expresado su consentimiento a que sean consultados o recabados dichos documentos. Se presumirá que la consulta u obtención es autorizada por los interesados salvo que conste en el procedimiento su oposición expresa o la ley especial aplicable requiera consentimiento expreso".

En relación con este precepto, y teniendo en cuenta que el RGPD a efectos de consentimiento no permite el denominado como "tácito", el acceso a los documentos por parte de la Administración pública correspondiente podría fundamentarse en el artículo 6.1.e) del RGPD, es decir, cuando el tratamiento sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, vinculado al hecho de que, de conformidad con la ***Ley 39/2015, de 1 de octubre***, las Administraciones Públicas no requerirán a los interesados datos o documentos no exigidos por la normativa reguladora aplicable o que hayan sido aportados anteriormente por el interesado a cualquier Administración.

En este sentido, será suficiente con que la Ley hubiese determinado quién es la Administración competente.

2.2.4. Tratamiento de categorías especiales de datos

El *RGPD* incluye en el concepto de categorías especiales de datos los denominados datos especialmente protegidos en la LOPD como son las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, los que revelen el origen racial o étnico, y los relativos a la salud o a la vida u orientación sexual de una persona.

También incorpora nuevas categorías de datos como son los datos genéticos y los datos biométricos.

La regla general contemplada en el Reglamento es la prohibición del tratamiento de categorías especiales de datos (art. 9).

No obstante, se recoge un amplio abanico de excepciones a esta regla general, destacando las siguientes en relación con los tratamientos de este tipo de datos que realicen los entes de la Administración Local:

- El tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del afectado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del afectado;

- El tratamiento es necesario para proteger intereses vitales del afectado o de otra persona física, en el supuesto de que el afectado no esté capacitado, física o jurídicamente, para dar su consentimiento;

- El tratamiento se refiere a datos personales que el afectado ha hecho manifiestamente públicos;

- El tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

- El tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del afectado".

· TRATAMIENTO DE CATEGORÍAS ESPECIALES DE DATOS

El interés público habilita el tratamiento de datos de salud por los servicios sociales de ámbito municipal, cuya prestación esté reconocida por una norma de rango legal.

La normativa de protección de datos, a diferencia del *RGPD* que no se pronuncia al respecto, ha establecido un sistema reforzado de protección para los datos relativos a las infracciones y sanciones administrativas.

En todo caso, y sin perjuicio de su desarrollo por el legislador español, estarían legitimados para el tratamiento de datos relativos a infracciones y sanciones administrativas los órganos competentes para la instrucción del procedimiento sancionador, para la declaración de las infracciones o la imposición de sanciones, y siempre y cuando se proceda al tratamiento de los datos necesarios para esta finalidad.

Como motivos de interés público amparado en habilitaciones legales que exceptúan la prohibición, el propio *RGPD* recoge expresamente los siguientes supuestos:

- El tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social.

- El tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios.

- El tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

2.3. DEL REGISTRO DE FICHEROS AL REGISTRO DE ACTIVIDADES DE TRATAMIENTO

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, que estará a disposición de la Autoridad de Control, en el que se incluya una descripción de los tratamientos de datos que realicen con la siguiente información:

· 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	Categorías de tratamientos efectuados por cuenta de cada 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 de las medidas técnicas y organizativas de seguridad.	Descripción de las medidas técnicas y organizativas de seguridad.
Categorías de destinatarios de comunicaciones, incluidos terceros países u organizaciones internacionales.	
Transferencias internacionales. Documentación de garantías adecuadas 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.	. . . . .

PULSA SOBRE LAS PALABRAS EN *CURSIVA* O EL SÍMBOLO , PARA OBTENER INFORMACIÓN ADICIONAL

A este respecto, señalar que, como su denominación indica, se trata de un registro de actividades de tratamiento, y no de un registro de ficheros.

Por ejemplo: si los datos que se utilizan para el cobro del impuesto de vehículos se usan para informar sobre una campaña informativa sobre la contaminación producida por los citados vehículos, existirían dos tratamientos de esos datos: uno relativo al cobro del mencionado impuesto; y el otro referente a la citada campaña.

· RGPD: REGISTRO DE ACTIVIDADES DEL TRATAMIENTO

La implementación de este registro obliga a inventariar todos los tratamientos que esté realizando cada entidad local.

Como hemos visto, se establece un contenido mínimo para este registro, por lo que esa tarea de inventario debe incluir la identificación de todos los elementos que deben incorporarse en relación con cada tratamiento.

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 encuentren 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:

POR EJEMPLO:

Un fichero de recursos humanos cuya finalidad fuese la gestión de los mismos así como la provisión de puestos de trabajo supondría dos actividades de tratamiento diferentes: por una parte, la referente a recursos humanos (personal que ya forma parte de la entidad); por otra, la relativa a la provisión de puestos. Por lo tanto, habría que configurar cada uno de ellos como una actividad de tratamiento diferente.

El fichero de videovigilancia de un edificio de un Ayuntamiento y el relativo al control de acceso al citado edificio, podrían ser una única actividad de tratamiento, puesto que la finalidad es la misma: seguridad.

PULSA SOBRE LAS PALABRAS EN *CURSIVA* O EL SÍMBOLO , PARA OBTENER INFORMACIÓN ADICIONAL

A modo de ejemplo, se exponen dos registros de actividades, en el que se incluye también el apartado "Legitimación del tratamiento", puesto que tal y como hemos visto anteriormente, es necesario documentar la misma:

· REGISTRO DE ACTIVIDADES PADRÓN DE HABITANTES

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

ACTIVIDAD DE TRATAMIENTO.
Padrón municipal de habitantes.

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

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

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

CATEGORÍAS DE AFECTADOS.
Ciudadanos residentes en el municipio.

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

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

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

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

· REGISTRO DE ACTIVIDADES SEGURIDAD

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

ACTIVIDAD DE TRATAMIENTO
Seguridad

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

FINES DEL TRATAMIENTO
Garantizar la seguridad de personas e instalaciones

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

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

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

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

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

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

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

2.4. SEGURIDAD EN EL TRATAMIENTO DE LOS DATOS PERSONALES

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, la norma europea introduce el análisis de riesgo con la finalidad de evaluar el riesgo que puede producir el tratamiento de datos de datos personales.

Por ejemplo, si un ente de la Administración Local no garantiza la confidencialidad del tratamiento de datos de personas físicas derivados de un procedimiento sancionador, y se produce una vulneración del deber de secreto, esta circunstancia podría suponer consecuencias negativas tanto para el responsable como para las personas físicas cuyos datos personales hayan sido revelados.

Por otra parte, el ***RGPD*** regula lo referente a las comunicaciones de quiebras de seguridad, tanto respecto a los ciudadanos afectados como a la Autoridad de Control de Protección de Datos correspondiente.

2.4.1. Análisis de riesgo

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.

Este análisis del riesgo variará 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.

· ANÁLISIS DE RIESGO

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

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

2.4.2. Implementación de medidas 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.

El anterior Título VIII del Real Decreto 1720/2007 establecía unos controles mínimos de obligado cumplimiento para garantizar la seguridad de los datos que se incorporan a los controles o medidas de seguridad que habrá que tener en cuenta en el *RGPD* dentro de los procesos de análisis de riesgos, por lo que las medidas de seguridad ya existentes se deben de mantener y revisar en el marco de dichos procesos. En ningún caso el *RGPD* se debe de entender como la eliminación automática de todas las medidas de seguridad ya existentes.

Así, según el artículo 32 del *RGPD* las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo se definen en función del estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas.

En definitiva, el primer paso para determinar las medidas de seguridad será la evaluación del riesgo a la que anteriormente nos hemos referido. Una vez evaluado el riesgo, será necesario determinar las medidas de seguridad encaminadas para reducir o eliminar los riesgos para el tratamiento de los datos.

Por otra parte, lo previsto en el *Esquema Nacional de Seguridad* es aplicable a cualquier información de las Administraciones Públicas sin distinción del soporte en el que se encuentre, por lo que en cuanto a las medidas de seguridad se refiere, este esquema es acorde al enfoque de riesgo del *RGPD* y se constituye en una herramienta válida para la gestión del riesgo y la adopción de las medidas de seguridad en las citadas Administraciones.

· MEDIDAS DE SEGURIDAD

El *RGPD* no establece un catálogo de medidas de seguridad, que se implementarán en función del análisis del riesgo realizado.

En el ámbito de las Administraciones públicas, incluyendo la Administración Local, es aplicable al tratamiento de datos lo dispuesto en el *Esquema Nacional de Seguridad*.

A este respecto, puede consultar los siguientes documentos:

- *Guía estratégica en seguridad para Entes locales*.
- *Guía para Entidades locales de menos de 2000 habitantes.*

La seudonimización puede contribuir a reducir el nivel de riesgo de los tratamientos.

Supone eliminar aquellos que datos permitan identificar a los ciudadanos, dejando accesibles aquellos datos o información personal que se necesita para el tratamiento. Se trata de un mecanismo que oculta la identidad de los afectados pero este ocultamiento de la identidad es reversible y siempre podremos re-identificar a las personas.

PULSA SOBRE LAS PALABRAS EN *CURSIVA* O EL SÍMBOLO , PARA OBTENER INFORMACIÓN ADICIONAL

2.4.3. Comunicación de quiebras de seguridad de los datos personales

Cuando se produzca una violación o quiebra 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 la sufra, 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.

· CONTENIDO MÍNIMO DE LA COMUNICACIÓN DE LA QUIEBRA DE SEGURIDAD A LA *AEPD*

Naturaleza de la quiebra de seguridad:

Categorías de afectados (por ejemplo: menores, discapacitados, empleados, ciudadanos).
- Nº aproximado de afectados.
- Categorías de datos comprometidos (por ejemplo: Identificativos, salud, laborales).
- Nº registros de datos personales afectados.

Nombre y datos de contacto del Delegado de Protección de Datos.

Posibles consecuencias de la quiebra de seguridad sufrida.

Medidas adoptadas o propuestas para remediar esta quiebra.

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

· COMUNICACIÓN DE LA QUIEBRA SEGURIDAD A LOS AFECTADOS

Regla general: comunicación a los afectados

EXCEPCIONES:

Si se han adoptado y aplicado medidas sobre los datos personales afectados, particularmente aquellas que hagan ininteligibles los datos para cualquier persona que no esté autorizada a acceder ellos (por ejemplo: se han cifrado los datos personales).

El responsable ha adoptado medidas ulteriores que garanticen que ya no existe un alto riesgo para los derechos y libertades.

Que esta comunicación fuese un esfuerzo desproporcionado, optándose por una comunicación pública o medida semejante por la que se informe de forma efectiva a los afectados.

Por otra parte, si el encargado del tratamiento sufre una quiebra de seguridad, éste debe notificar sin dilación al responsable la existencia de la misma. El *RGPD* no indica ni el formato de dicha notificación ni el plazo máximo para que se realice dicha notificación, ya que el plazo establecido para el responsable se fija a partir del conocimiento de la quiebra de seguridad. Por lo tanto, el responsable deberá fijar por tanto las obligaciones de notificación del encargado, de tal forma que le permitan cumplir con los requisitos que a dicho responsable sí obliga el *RGPD*, en particular, en relación a los datos que es necesario notificar a terceros.

Los entes de la Administración Local pueden elaborar una Plan de Contingencias con la finalidad de mitigar los daños cuando se produzca una quiebra de seguridad.

También deben mantener un registro de los incidentes de seguridad.

2.5. EVALUACIONES DE IMPACTO EN LA PROTECCIÓN DE DATOS.

2.5.1. ¿Qué una evaluación de impacto en la protección de datos?

La evaluación de impacto en protección de datos (EIPD) es una herramienta con carácter preventivo que debe realizar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas. En la práctica, la EIPD permite determinar el nivel de riesgo que entraña un tratamiento, con el objetivo de establecer las medidas de control más adecuadas para reducir el mismo hasta un nivel considerado aceptable

El *RGPD* señala también que cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entraña un alto riesgo para los derechos y libertades, el responsable realizará, antes del tratamiento, una evaluación de impacto. Si se trata de operaciones similares que supongan riesgos similares, se podrá realizar una única evaluación.

Sobre las operaciones que requieran una evaluación de impacto de acuerdo a lo dispuesto en el párrafo anterior, la Autoridad de Control establecerá y publicará una lista al respecto.

Igualmente, podrá publicar otra lista respecto a aquellos tratamientos que no requieran dicha evaluación de impacto.

Además, el *RGPD* determina los siguientes supuestos en que debe realizarse 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.

Una de las cuestiones básicas a tener en cuenta en la realización de una evaluación de impacto es la participación del delegado de protección de datos.

La *AEPD* dispone de una *Guía práctica para las evaluaciones de impacto en la protección de datos sujetas al RGPD* datos que puede utilizarse como referencia.

2.5.2. Especial referencia a las "Smart cities"

La tecnología actual ofrece la posibilidad a los responsables de los municipios de obtener información sobre los ciudadanos en tiempo real. Esta información puede obtenerse mediante sensores o mediante la información de determinados servicios. Por ejemplo, entre los sensores, podríamos citar los contadores inteligentes de transeúntes que permiten la obtención del número de personas que transitan por la vía pública y la dirección en la que caminan, y entre los servicios, los de telefonía móvil mediante los cuales podemos obtener de forma muy aproximada la cifra de personas que se encuentran en un determinado espacio público o los de transporte público que pueden aportar información acerca de cuántas personas se trasladan de un lugar a otro.

El número de fuentes y sensores de las que es posible obtener información es cada vez mayor y el cruce de estas informaciones con información de distinto origen o fuentes proporciona valiosa información que puede ayudar a gestionar los servicios de un municipio de forma más eficiente. Lógicamente, a mayor información, mayor exactitud de la misma y mayor eficiencia en la gestión de servicios públicos.

Además, también podemos obtener información de los eventos que tienen lugar en un determinado municipio o de los horarios comerciales de grandes superficies y centros de ocio, que es de gran utilidad para gestionar tanto servicios públicos como servicios privados, y otorga a ambos la posibilidad de elaborar modelos o pautas de comportamiento de los ciudadanos que pueden convertirse en un mecanismo de coordinación público-privado que aumente el grado de sostenibilidad y eficiencia de los servicios de un municipio.

Por ejemplo, podemos obtener estadísticas del comportamiento de los ciudadanos que acceden a un centro de ocio de forma que tengamos información sobre promedios de tiempo y distribución de los lugares en los que transitan; a partir de esta información, se pueden sugerir a los responsables del centro de ocio horarios de cierre escalonado, de manera que ayuden a prevenir aglomeraciones de personas en determinados espacios públicos y gestionar el transporte público en consecuencia. Incluso, esta información puede ser utilizada en tiempo real, y coordinada con la distribución de otros servicios como la seguridad o servicios de emergencia.

No obstante lo anterior, a mayor información y mayor número de fuentes de las que se obtiene, más riesgo existe para la privacidad y la protección de datos de los ciudadanos. Otro factor de riesgo a tener en cuenta es la frecuencia con la que obtenemos la información.

Por lo tanto, antes de la puesta en producción de un proyecto "Smart City" es necesario realizar un análisis previo del mismo valorando el volumen de la información que se pretende procesar y el número y tipo de fuentes desde las que se pretende obtener dicha información o incluso el tiempo durante el que se pretende conservar esta información.

En consonancia con lo anterior, será necesaria la realización de una evaluación de impacto relativa a la protección de datos o incluso una consulta previa a la Autoridad de protección de datos, según lo previsto en la sección tercera del ***RGPD***.

En todo caso, los principios de protección de datos siempre serán tenidos en cuenta en el diseño de un proyecto Smart City (como ya se ha comentado a menor volumen de datos menor riesgo para los derechos y libertades de las personas) por lo que la información procesada y su tratamiento se limitará al mínimo imprescindible para la finalidad que se pretende, aplicando el principio de minimización de datos.

Asimismo, también se tendrá en consideración la seudonimización, consistente en tratar los datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

Por ejemplo, en ningún caso sería proporcional realizar una clasificación del número de ciudadanos por el tipo de orientación sexual de los establecimientos de una determinada zona de un municipio o el tratamiento del número de personas que se encuentran en un determinado espacio de culto religioso. En general se evitará el posible etiquetado de las personas mediante categorías especiales de datos; únicamente sería proporcional el tratamiento de esta información en términos estadísticos relativos al número de personas o a los horarios de afluencia de las mismas a dichos espacios.

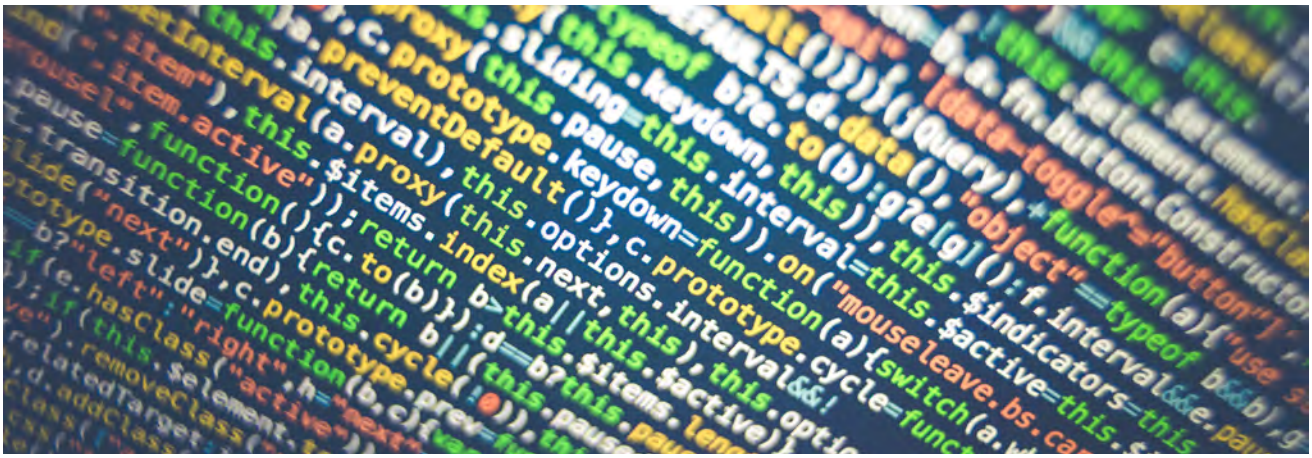
El periodo de conservación de la información también deberá ser tenido en cuenta, ya que si bien se puede conservar la información estadística, se deben establecer límites cuando la información que se obtenga pudiera permitir directa o indirectamente identificar a las personas. Los límites de conservación se ponderarán según el tipo de información que se vaya a tratar o los riesgos de identificación de las personas.

En todo caso, cuando se diseñe un sistema "Smart City" se tendrá en cuenta la privacidad desde el diseño de dicho sistema y especial atención deberá ser tenida en cuenta con relación a los principios relativos al tratamiento a los que se refiere el capítulo segundo del ***RGPD***, y se evitará el tratamiento de información relacionada directa o indirectamente con categorías especiales de datos personales a las que se refiere el artículo 9 del ***RGPD***.

También debe tenerse en consideración la posibilidad de que existan decisiones automatizadas, incluyendo la elaboración de perfiles, que produzcan efectos jurídicos o que le afecten significativamente de modo similar.

No obstante, se recomienda tener en cuenta un posible marco de gobernanza de la información en el que se defina la finalidad de la misma y los mecanismos de acceso y términos de uso necesarios que aseguren el uso adecuado de la información.

Si el tratamiento de datos que se pretende realizar supone un tratamiento masivo de información, se recomienda consultar el código de buenas prácticas en protección de datos para proyectos ***big data***.



2.6. PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO

El ***RGPD*** contiene dos principios para la implementación efectiva de la responsabilidad proactiva, como son los de protección de datos desde el diseño y protección de datos por defecto.

El principio de **protección de datos desde el diseño** supone que la protección de datos ha de estar presente en las primeras fases de concepción de un proyecto y formar parte de la lista de elementos a considerar antes de iniciar las sucesivas etapas de desarrollo.

Por supuesto, estos requisitos se van a traducir en medidas técnicas y organizativas con el objeto de aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento.

Un ejemplo de dichas medidas, que se establece de forma expresa en el *RGPD*, es que el propio tratamiento incorpore medidas para la seudonimización de los datos personales o la minimización de datos.

Por su parte, **la protección de datos por defecto** estriba en que sólo sean objeto de tratamiento los datos personales que sean estrictamente necesarios para cada uno de los fines de tratamiento. Es decir, independientemente del conjunto de datos recogidos por el responsable con el objeto de implementar los distintos servicios que se proporcionan al sujeto de los datos, el responsable ha de compartimentar el uso del conjunto de datos entre los distintos tratamientos, de tal forma que no todos los tratamientos accedan a todos los datos, sino que actúen solo sobre aquellos que sean necesarios y en los momentos en que sea estrictamente necesario. Si fuera posible por la naturaleza del proceso, llegar incluso a que no se traten datos de carácter personal.

En particular, se destaca como uno de los principios de protección de datos por defecto que los datos no sean accesibles a un número indeterminado de personas físicas, sin la intervención del sujeto de los datos.

Además, debe tenerse en cuenta lo siguiente respecto a la protección de datos por defecto:

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

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

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

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

2.7. 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.

Hasta el *RGPD* la información que debía facilitarse era la siguiente:

- 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.

Sin embargo, con el ***RGPD*** este derecho de información, en aras de la transparencia en el tratamiento de los datos personales, se amplía considerablemente, de tal forma que, entre otros, se deberá informar sobre los siguientes extremos:

- Los datos de contacto del Delegado de Protección de Datos (obligatorio para la Administración Local);
- La base jurídica o legitimación del tratamiento;
- El plazo o criterios de conservación 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.

· RGPD: DERECHO DE INFORMACIÓN

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).

EJEMPLOS

Formularios para darse de alta en el Padrón Municipal de Habitantes o para solicitar una subvención.

La página web de un Ayuntamiento en la medida en que recabe datos de carácter personal.

Para facilitar esta tarea puede consultar la ***Guía para el cumplimiento del deber de informar***.

En el caso de que los datos no se obtengan del propio afectado, por proceder de alguna cesión legítima, el responsable informará a las personas interesadas dentro de un plazo razonable, pero en cualquier caso:

- Antes de un mes desde que se obtuvieron los datos personales;
- Antes o en la primera comunicación con el afectado;
- Antes de que los datos, en su caso, se hayan comunicado a otros destinatarios.

Esta obligación de informar se debe cumplir sin necesidad de requerimiento alguno, y el responsable deberá poder acreditar con posterioridad que ha sido satisfecha.

El *RGPD* también regula una serie de supuestos en los que no será necesario cumplir con este derecho de información:

- Cuando el afectado ya disponga de la información.

- Si los datos no proceden del afectado, cuando la comunicación resulte imposible o suponga un esfuerzo desproporcionado, el registro o la comunicación esté expresamente establecido por el Derecho de la Unión o de los Estados miembros, o cuando los datos deban seguir teniendo carácter confidencial por un deber legal de secreto.

Los procedimientos de recogida de información pueden ser muy variados y, por tanto, los modos de informar a los afectados deben adaptarse a las circunstancias de cada uno de los medios empleados para la recopilación o registro de los datos.

Por ejemplo, algunas de las formas más habituales de recogida de datos y, en consecuencia, a través de los cuales hay que informar, pueden ser:

Por otra parte, las comunicaciones al afectado sobre datos ya disponibles, o tratamientos adicionales, pueden hacerse llegar, entre otros medios, por correo postal, mensajería electrónica, así como notificaciones emergentes en servicios y aplicaciones.

Las características de cada uno de los medios varían en cuanto a extensión, disponibilidad de espacio, legibilidad, posibilidad de vincular informaciones, etc. En cualquier caso, la información a las personas interesadas debe proporcionarse: con un lenguaje claro y sencillo, de forma concisa, transparente, inteligible y de fácil acceso.

Para facilitar este cumplimiento, se 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).

EPÍGRAFE	INFORMACIÓN BÁSICA (1ª CAPA, RESUMIDA)	INFORMACIÓN ADICIONAL (2ª CAPA, DETALLADA)
RESPONSABLE *DEL TRATAMIENTO*	Identidad del responsable del tratamiento	Datos de contacto del responsable
		Identidad y datos de contacto del representante
		Datos de contacto del delegado de protección de datos
FINALIDAD *DEL TRATAMIENTO*	Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles	Descripción ampliada de los fines del tratamiento
		Plazos o criterios de conservación de los datos
		Decisiones automatizadas, perfiles y lógica ampliada
LEGITIMACIÓN *DEL TRATAMIENTO*	Base jurídica del tratamiento	Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo
		Obligación o no de facilitar datos y consecuencias de no hacerlo
DESTINATARIOS *DE CESIONES O TRANMSFERENCIAS*	Previsión o no de cesiones	Destinatarios o categorías de destinatarios
	Previsión de transferencias, o no, a terceros paises	Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones especificas aplicables
DERECHOS *DE LAS PERSONAS INTERESADAS*	Referencia al ejercicio de derechos	Como ejercer los derechos de acceso, rectificaciones, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento
		Derecho a retirar el consentimiento prestado
		Derecho a reclamar ante la autoridad de control
PROCEDENCIA *DE LOS DATOS*	Fuente de los datos (cuando no proceden del interesado)	Información detallada del origen de los datos, incluso si proceden fuentes de acceso público
		Categorías de datos que se traten

2.8. ADMINISTRACIÓN LOCAL Y SUS ENCARGADOS DEL 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***, y que garantice la protección de los derechos de las personas afectadas. Existe, por tanto, un deber de diligencia en la elección del responsable. El Considerando 81 del ***RGPD*** prevé que el encargado del tratamiento debe ofrecer suficientes garantías en lo referente a conocimientos especializados, fiabilidad y recursos, con vistas a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del Reglamento, incluida la seguridad del tratamiento, así como del cumplimiento de la normativa de protección de datos.

· **POR EJEMPLO,** en la elección de servicios de "computación en nube" ("cloud computing") de empresas de fuera de la Unión Europea podría tenerse en consideración si cumplen respecto al régimen jurídico de transferencias internacionales que contempla el ***RGPD***.

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 contratos con encargados de tratamiento que realicen los entes de la Administración Local deberán contener, al menos, el contenido referido.

Los ya celebrados, en la medida de lo posible, podrían ir adecuándose también.

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

2.9. EL DELEGADO DE PROTECCIÓN DE DATOS (DPD) EN LA ADMINISTRACIÓN LOCAL

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.

La norma europea señala que el ***Delegado de Protección de Datos*** será una persona con conocimiento especializado 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 para garantizar un tratamiento adecuado de los datos personales objeto de esos tratamientos.

Las funciones 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.

· DESIGNACIÓN DEL DELEGADO DE PROTECCIÓN DE DATOS EN LA ADMINISTRACIÓN LOCAL

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

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

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

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

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

También cabe la posibilidad de que se pueda prestar por entidades privadas especializadas.

El Delegado de Protección de Datos debe desempeñar sus tareas y funciones con total independencia.

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

La AEPD ha puesto en marcha, en colaboración con ENAC, el ***Esquema de Certificación de Delegados de Protección de Datos***. Esta certificación es voluntaria.

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.

Además, debe tenerse en cuenta lo siguiente:

- En entidades de gran tamaño, lo lógico es que el DPD lo sea a tiempo completo;
- En entidades pequeñas, pueda compaginar las funciones de DPD con otras tareas.

2.10. TRANSFERENCIAS INTERNACIONALES DE DATOS

Cuando los datos personales se envían fuera del ámbito del Espacio Económico Europeo, que comprende todos los Estados miembros de la Unión Europea, más Noruega, Islandia y Liechtenstein, se produce una transferencia internacional de datos.

Aunque podría 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.

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.

· TRANSFERENCIA INTERNACIONAL DE DATOS EN LA ADMINISTRACIÓN LOCAL

Dependiendo del tipo de prestación, los responsables en el ámbito de la Administración Local deberían tener en cuenta esas posibles implicaciones internacionales y la necesidad de que esas transferencias se lleven a cabo sobre la base de los adecuados instrumentos.

2.11. 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 de RGPD	¿En que 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 ("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:** 1. 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. 2. 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.

PULSA SOBRE LAS PALABRAS EN *CURSIVA* O EL SÍMBOLO , PARA OBTENER INFORMACIÓN ADICIONAL

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, indicando los motivos de la dilación. Si el ciudadano presentase la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el ciudadano solicite que se facilite de otro modo.

· DERECHOS DE LOS AFECTADOS SOBRE EL TRATAMIENTO DE SUS DATOS PERSONALES

Los entes de la Administración Local deben establecer mecanismos visibles, accesibles y sencillos, incluidos medios electrónicos, para el ejercicio de derechos.

Estos mecanismos, en particular, cuando se trate del ejercicio por medios electrónicos, deben incorporar procedimientos para verificar la identidad de los afectados que los utilizan, así como de la recepción del ejercicio del correspondiente derecho, y su oportuna contestación.

Como hemos visto, el RGPD introduce nuevos derechos. De ellos, el que puede ejercerse más frecuentemente en el ámbito de la Administración Local es el de limitación del tratamiento: debe suspenderse el tratamiento de datos cuando los ciudadanos soliciten la rectificación o supresión al responsable hasta que se resuelva su solicitud.

3. CONSULTAS FRECUENTES

3.1. 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*;

- 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 tratamientos 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.

3.2. 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:

- 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 datos 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.

3.3. 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".

¿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 podrían 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, catálogo 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, con la finalidad de desarrollar software por terceros o por el propio Ayuntamiento, que crucen datos del Portal Opendata que sean de interés para el ciudadano?

Sólo será posible la publicación de datos contenidos en los tratamientos de la Administración pública, fuera de los supuestos permitidos por la Ley o en los 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 la 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 tratamientos 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.

3.4. 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.

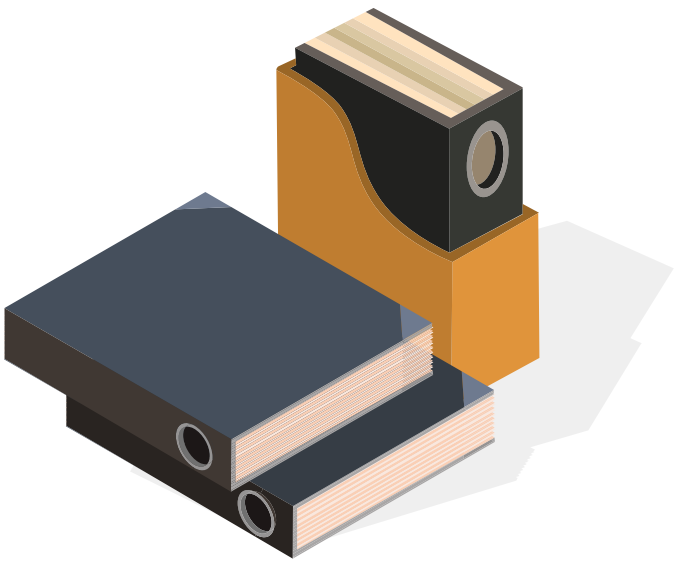
b) Emitir informe, a solicitud de la Administración Pública correspondiente, sobre el traslado total o parcial de las instalaciones e implantación o revisión de sus sistemas de organización y métodos de trabajo.

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) atribuye a dicho órgano "Ejercer una labor:

> **1º** 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. (…)

Y según el apartado 9 del citado precepto:

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:

> 4º 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 del personal al servicio de un Ayuntamiento con la finalidad de localizar los vehículos y ubicación para mejorar la prestación del servicio?

En primer lugar, precisar que se trataría de coches que pertenecen a la corporación municipal y que son facilitados a sus trabajadores para realizar sus respectivas funciones y tareas.

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 decir, estos datos no podrán utilizarse para una finalidad incompatible.

En segundo lugar, deberá cumplirse el deber de información al afectado –en este caso, los trabajadores que vayan a utilizar los vehículos- por el tratamiento de datos, exigido en el artículo 13 del ***RGPD***.

Por último, y respecto a la legitimación para el tratamiento de datos, el ***RGPD*** permite este tratamiento cuando es necesario en el marco de la ejecución de un contrato.

Por lo tanto, el tratamiento de los datos de localización del vehículo durante la prestación del servicio y, como consecuencia, de los trabajadores que se encuentran en el mismo responden a la necesidad de garantizar el mejor desarrollo de sus funciones así como del servicio público que estén prestando, por lo que, el tratamiento de dicho dato estaría amparado por lo previsto en el artículo 6.1.b) 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.

En todo caso, es recomendable la utilización de un sello del órgano correspondiente, sin necesidad de que aparezca la identificación del funcionario que realiza esta labor.

Respecto a 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.

3.5. 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, está sometida 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?

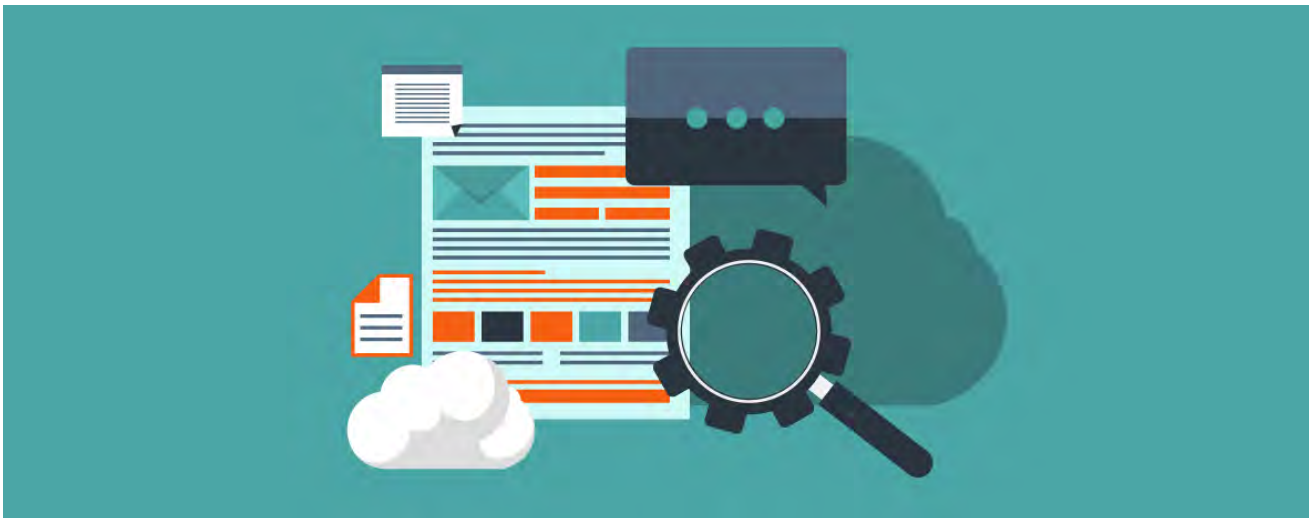
En el supuesto planteado se trataría de la instalación de un sistema de seguridad y control de acceso a edificios captado la imagen y voz de las personas que acceden a los mismos.
Con carácter general, las grabaciones indiscriminadas de voz y conversaciones del público en general que acceden a los edificios de un Ayuntamiento a través de sistemas de videovigilancia no cumpliría el principio de minimización de datos del RGPD, considerándose una medida intrusiva.

3.6. 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.



¿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*.

¿Qué información se puede publicar en el Portal de Transparencia?

La *Ley 19/2013, de 9 de diciembre*, de transparencia, acceso a la información pública y buen gobierno, regula en su Capítulo II la denominada "Publicidad activa", estableciendo una serie de supuestos de publicación obligatoria a través de los denominados Portales de Transparencia.

En este sentido, en aquellas Comunidades Autónomas que han aprobado su respectiva ley de transparencia, éstas también recogen la citada "Publicidad activa".

En la medida que pudiese afectar la publicación a datos de carácter personal, la legitimación para dicha publicación vendría dada por el artículo 6.1.c) del RGPD, es decir, el cumplimiento de una obligación legal.

No obstante, debe tenerse en cuenta lo siguiente:

- Serán de aplicación, en su caso, los límites al derecho de acceso a la información pública previstos en el artículo 14 y, especialmente, el derivado de la protección de datos de carácter personal, regulado en el artículo 15 de la *Ley 19/2013, de 9 de diciembre*. A este respecto, cuando la información contuviera categorías especiales de datos, la publicidad sólo se llevará a cabo previa disociación de los mismos.

- Los afectados por la publicación podría ejercitar el derecho de oposición a la publicación de sus datos, y suponer la supresión de los mismos. Por ejemplo, una persona víctima de violencia de género, que si bien de acuerdo a lo indicado anteriormente se podría realizar la publicación de sus datos meramente identificativos, alega dicha condición en aras de garantizar su seguridad para que esta publicación no se realice.

¿Se pueden publicar los datos de los licitadores y actas de las mesas de contratación? ¿Y los miembros de las mesas de contratación y comités de expertos?

El artículo 63 de la *Ley 9/2017, de 8 de noviembre*, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, determina una serie de supuestos de publicación obligatoria, que en la medida que afecte a datos de carácter personal, la legitimación se fundamentaría en el artículo 6.1.c) del RGPD relativo al cumplimiento de una obligación legal.

Asimismo, debe considerarse lo siguiente:

- Para la publicación del número e identidad de los licitadores participantes, respecto a personas físicas, además de su nombre y apellidos, será suficiente con publicar las últimas cuatro cifras del NIF.

- Respecto al a publicación de las actas de la mesa de contratación relativas al procedimiento de contratación, no será necesario que en el contenido de las actas objeto de publicación figure las firmas del Presidente y Secretario de la mesa.

- Respecto a la publicación de los miembros de las mesas de contratación y comités de expertos, será suficiente con publicar nombres y apellidos, y cargos de los mismos.

- Al igual que en la pregunta-respuesta anterior, sería posible el ejercicio del derecho de oposición por los afectados.

3.7. 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 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 y los datos de los menores en situación de vulnerabilidad, 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.

¿Podría acceder la policía local 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 las siguientes funciones:

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 referidos, 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 de los datos.

Este criterio impediría la incorporación en bloque de la totalidad de los datos contenidos en los tratamientos municipales a los tratamientos 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.

3.8. 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.

¿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.

PULSA SOBRE LAS PALABRAS EN ***CURSIVA*** O EL SÍMBOLO , PARA OBTENER INFORMACIÓN ADICIONAL

4. MATERIALES DE AYUDA 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 al RGPD.

- *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.*
  - *Tareas de adaptación al RGPD.*
  - *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 práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD.*
  - *Guía práctica de análisis de riesgos en los tratamientos de datos personales al RGPD.*

PROTECCIÓN DE DATOS Y ADMINISTRACIÓN LOCAL

GUÍAS SECTORIALES AEPD

Con la colaboración de: