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

RECOPILACIÓN DE MATERIALES REALIZADA POR EL GRUPO DE TRABAJO PARA LA IMPLANTACIÓN DEL NUEVO REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD) EN LAS ADMINISTRACIONES LOCALES, CREADO POR LA COMISIÓN DE SOCIEDAD DE LA INFORMACIÓN Y TECNOLOGÍAS DE LA FEMP

FEMP
FEDERACION ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

RED
RED DE ENTIDADES LOCALES POR LA TRANSPARENCIA Y PARTICIPACIÓN CIUDADANA

Desde la Red de Entidades Locales por la Transparencia y Participación Ciudadana de la FEMP volvemos a dirigirnos a las entidades locales para presentar, en este caso, la publicación "Orientaciones para la adaptación de las administraciones locales al Reglamento General de Protección de Datos" elaborada por un equipo multidisciplinar de técnicos locales, de la Agencia Española de Protección de Datos y expertos del ámbito jurídico y universitario.

Se trata de un documento sencillo y práctico que aborda la puesta en práctica de la nueva normativa sobre protección de datos que entra en vigor próximamente.

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

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

Muchas gracias.

Carlos González Serna
Alcalde de Elche
Presidente de la Red de Entidades Locales
por la Transparencia y la Participación Ciudadana de la FEMP

PRESENTACIÓN

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

El pasado mes de abril se aprobó el Reglamento (UE) 2016/679 del Parlamento y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

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

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

Esta Guía ha sido posible gracias al trabajo impulsado desde la Agencia Española de Protección de Datos, de quienes la FEMP, y el grupo de trabajo de nuestra Comisión, ha querido ir de la mano, y consideramos que en ella se pueden encontrar gran parte de las claves necesarias para el cumplimiento normativo, así como tomar conciencia de la situación de partida en la que se encuentran nuestras Administraciones Locales.

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

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

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

ÍNDICE

1 INTRODUCCIÓN

En el mes de abril de 2016 se aprobó el Reglamento (UE) 2016/679 del Parlamento y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) (DOUE 4.5.2016).

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

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

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

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

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

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

EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

2

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE **(Reglamento general de protección de datos)**

CAPÍTULO I. Disposiciones Generales

Artículo 1 Objeto

1. El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos.
2. El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.
3. La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

Artículo 2 Ámbito de aplicación material

1. El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.
2. El presente Reglamento no se aplica al tratamiento de datos personales:
   a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión;
   b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE;
   c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas;
   d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.
3. El Reglamento (CE) n.o 45/2001 es de aplicación al tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos de la Unión. El Reglamento (CE) n.o 45/2001 y otros actos jurídicos de la Unión aplicables a dicho tratamiento de datos de carácter personal se adaptarán a los principios y normas del presente Reglamento de conformidad con su artículo 98.
4. El presente Reglamento se entenderá sin perjuicio de la aplicación de la Directiva 2000/31/CE, en particular sus normas relativas a la responsabilidad de los prestadores de servicios intermediarios establecidas en sus artículos 12 a 15.

Artículo 3 Ámbito territorial

1. El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.
2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que se encuentren en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:
   a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o
   b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.
3. El presente Reglamento se aplica al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público.

Artículo 4 Definiciones

A efectos del presente Reglamento se entenderá por:

1. «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;
2. «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, Limitación, supresión o destrucción;
3. «limitación del tratamiento»: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro;
4. «elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;
5. «seudonimización»: el tratamiento de 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;
6. «fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;
7. «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; 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;
8. «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

9. «destinatario»: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;
10. «tercero»: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;
11. «consentimiento del interesado»: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;
12. «violación de la seguridad de los datos personales»: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;
13. «datos genéticos»: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;
14. «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;
15. «datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;
16. «establecimiento principal»:
    1) en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal;
    2) en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente Reglamento;
17. «representante»: persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento;
18. «empresa»: persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica;
19. «grupo empresarial»: grupo constituido por una empresa que ejerce el control y sus empresas controladas;
20. «normas corporativas vinculantes»: las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta;

21. «autoridad de control»: la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51;
22. «autoridad de control interesada»: la autoridad de control a la que afecta el tratamiento de datos personales debido a que:
    1) el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control;
    2) los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o
    3) se ha presentado una reclamación ante esa autoridad de control;
23. «tratamiento transfronterizo»:
    1) el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o
    2) el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro;
24. «objeción pertinente y motivada»: la objeción a una propuesta de decisión sobre la existencia o no de infracción del presente Reglamento, o sobre la conformidad con el presente Reglamento de acciones previstas en relación con el responsable o el encargado del tratamiento, que demuestre claramente la importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión;
25. «servicio de la sociedad de la información»: todo servicio conforme a la definición del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo;
26. «organización internacional»: una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo.

CAPÍTULO II. Principios

Artículo 5 Principios relativos al tratamiento

1. Los datos personales serán:
    a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);
    b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);
    c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);
    d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

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

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

Artículo 6 Licitud del tratamiento

1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

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

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

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

   d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

   e) 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;

   f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

   Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

2. Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX.

3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por:

   a) el Derecho de la Unión, o

   b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento.

   La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de

conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

4. Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:
   a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;
   b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;
   c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;
   d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;
   e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.

Artículo 7 Condiciones para el consentimiento

1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.
2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.
3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.
4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

Artículo 8 Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información

1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.

   Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.

2. El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.
3. El apartado 1 no afectará a las disposiciones generales del Derecho contractual de los Estados miembros, como las normas relativas a la validez, formación o efectos de los contratos en relación con un niño.

Artículo 9 Tratamiento de categorías especiales de datos personales

1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.
2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:
   a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;
   b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado 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 interesado;
   c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;
   d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;
   e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;
   f) 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;
   g) 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 interesado;
   h) 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, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

i) 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, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, 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 interesado.

3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.
4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.

Artículo 10 Tratamiento de datos personales relativos a condenas e infracciones penales

El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas.

Artículo 11 Tratamiento que no requiere identificación

1. Si los fines para los cuales un responsable trata datos personales no requieren o ya no requieren la identificación de un interesado por el responsable, este no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado con la única finalidad de cumplir el presente Reglamento.
2. Cuando, en los casos a que se refiere el apartado 1 del presente artículo, el responsable sea capaz de demostrar que no está en condiciones de identificar al interesado, le informará en consecuencia, de ser posible. En tales casos no se aplicarán los artículos 15 a 20, excepto cuando el interesado, a efectos del ejercicio de sus derechos en virtud de dichos artículos, facilite información adicional que permita su identificación.

CAPÍTULO III. Derechos del interesado

Sección 1. Transparencia y modalidades

Artículo 12 Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado

1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.
2. El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 22. En los casos a que se refiere el artículo 11, apartado 2, el responsable no se negará a actuar a petición del interesado con el fin de ejercer sus derechos en virtud de los artículos 15 a 22, salvo que pueda demostrar que no está en condiciones de identificar al interesado.
3. El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.
4. Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.
5. La información facilitada en virtud de los artículos 13 y 14 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán a título gratuito. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá:
   a) cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o
   b) negarse a actuar respecto de la solicitud.

   El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.
6. Sin perjuicio de lo dispuesto en el artículo 11, cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud a que se refieren los artículos 15 a 21, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.
7. La información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente.
8. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 92 a fin de especificar la información que se ha de presentar a través de iconos y los procedimientos para proporcionar iconos normalizados.

Sección 2. Información y acceso a los datos personales

Artículo 13 Información que deberá facilitarse cuando los datos personales se obtengan del interesado

1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:
   a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
   b) los datos de contacto del delegado de protección de datos, en su caso;
   c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
   cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;
   d) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
   e) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.
2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;

b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;

d) el derecho a presentar una reclamación ante una autoridad de control;

e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;

f) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.
4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.

Artículo 14 Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado

1. Cuando los datos personales no se hayan obtenidos del interesado, el responsable del tratamiento le facilitará la siguiente información:
   a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
   b) los datos de contacto del delegado de protección de datos, en su caso;
   c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;
   d) las categorías de datos personales de que se trate;
   e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
   f) en su caso, la intención del responsable de transferir datos personales a un destinatario en un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de ellas o al hecho de que se hayan prestado.
2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente respecto del interesado:
   a) el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo;
   b) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable del tratamiento o de un tercero;
   c) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
   d) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada;
   e) el derecho a presentar una reclamación ante una autoridad de control;
   f) la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;
   g) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.
3. El responsable del tratamiento facilitará la información indicada en los apartados 1 y 2:
   a) dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos;
   b) si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado, o
   c) si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.
4. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de los datos personales para un fin que no sea aquel para el que se obtuvieron, proporcionará al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y cualquier otra información pertinente indicada en el apartado 2.

5. Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que:
   a) el interesado ya disponga de la información;
   b) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información;
   c) la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, o
   d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria.

Artículo 15 Derecho de acceso del interesado

1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:
   a) los fines del tratamiento;
   b) las categorías de datos personales de que se trate;
   c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;
   d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;
   e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;
   f) el derecho a presentar una reclamación ante una autoridad de control;
   g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;
   h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.
2. Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia.
3. El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.
4. El derecho a obtener copia mencionado en el apartado 3 no afectará negativamente a los derechos y libertades de otros.

Sección 3. Rectificación y supresión

Artículo 16 Derecho de rectificación

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

Artículo 17 Derecho de supresión («el derecho al olvido»)

1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:
   a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;
   b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;
   c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;
   d) los datos personales hayan sido tratados ilícitamente;
   e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;
   f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.
2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.
3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:
   a) para ejercer el derecho a la libertad de expresión e información;
   b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;
   c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;
   d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o
   e) para la formulación, el ejercicio o la defensa de reclamaciones.

Artículo 18 Derecho a la limitación del tratamiento

1. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:
   a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;
   b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;
   c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;
   d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.
2. Cuando el tratamiento de datos personales se haya limitado en virtud del apartado 1, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.
3. Todo interesado que haya obtenido la limitación del tratamiento con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación.

Artículo 19 Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento

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

Artículo 20 Derecho a la portabilidad de los datos

1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:
   a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y
   b) el tratamiento se efectúe por medios automatizados.
2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.
3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
4. El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros.

Sección 4. Derecho de oposición y decisiones individuales automatizadas

Artículo 21 Derecho de oposición

1. El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.
2. Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.
3. Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.
4. A más tardar en el momento de la primera comunicación con el interesado, el derecho indicado en los apartados 1 y 2 será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.
5. En el contexto de la utilización de servicios de la sociedad de la información, y no obstante lo dispuesto en la Directiva 2002/58/CE, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.
6. Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.

Artículo 22 Decisiones individuales automatizadas, incluida la elaboración de perfiles

1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.
2. El apartado 1 no se aplicará si la decisión:
   a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;
   b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o
   c) se basa en el consentimiento explícito del interesado.
3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.
4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

Sección 5. Limitaciones

Artículo 23 Limitaciones

1. El Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar:
   a) la seguridad del Estado;
   b) la defensa;
   c) la seguridad pública;
   d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención;
   e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social;
   f) la protección de la independencia judicial y de los procedimientos judiciales;
   g) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas;
   h) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g);
   i) la protección del interesado o de los derechos y libertades de otros;
   j) la ejecución de demandas civiles.
2. En particular, cualquier medida legislativa indicada en el apartado 1 contendrá como mínimo, en su caso, disposiciones específicas relativas a:
   a) la finalidad del tratamiento o de las categorías de tratamiento;
   b) las categorías de datos personales de que se trate;
   c) el alcance de las limitaciones establecidas;
   d) las garantías para evitar accesos o transferencias ilícitos o abusivos;
   e) la determinación del responsable o de categorías de responsables;
   f) los plazos de conservación y las garantías aplicables habida cuenta de la naturaleza alcance y objetivos del tratamiento o las categorías de tratamiento;
   g) los riesgos para los derechos y libertades de los interesados, y
   h) el derecho de los interesados a ser informados sobre la limitación, salvo si puede ser perjudicial a los fines de esta.

CAPÍTULO IV. Responsable del tratamiento y encargado del tratamiento

Sección 1. Obligaciones generales

Artículo 24 Responsabilidad del responsable del tratamiento

1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.
2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.
3. La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.

Artículo 25 Protección de datos desde el diseño y por defecto

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.
2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.
3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.

Artículo 26 Corresponsables del tratamiento

1. Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que se les aplique a ellos. Dicho acuerdo podrá designar un punto de contacto para los interesados.
2. El acuerdo indicado en el apartado 1 reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los interesados. Se pondrán a disposición del interesado los aspectos esenciales del acuerdo.

3. Independientemente de los términos del acuerdo a que se refiere el apartado 1, los interesados podrán ejercer los derechos que les reconoce el presente Reglamento frente a, y en contra de, cada uno de los responsables.

Artículo 27 Representantes de responsables o encargados del tratamiento no establecidos en la Unión

1. Cuando sea de aplicación el artículo 3, apartado 2, el responsable o el encargado del tratamiento designará por escrito un representante en la Unión.
2. La obligación establecida en el apartado 1 del presente artículo no será aplicable:
   a) al tratamiento que sea ocasional, que no incluyan el manejo a gran escala de categorías especiales de datos indicadas en el artículo 9, apartado 1, o de datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, y que sea improbable que entrañe un riesgo para los derechos y libertades de las personas físicas, teniendo en cuenta la naturaleza, contexto, alcance y objetivos del tratamiento, o
   b) a las autoridades u organismos públicos.
3. El representante estará establecido en uno de los Estados miembros en que estén los interesados cuyos datos personales se traten en el contexto de una oferta de bienes o servicios, o cuyo comportamiento esté siendo controlado.
4. El responsable o el encargado del tratamiento encomendará al representante que atienda, junto al responsable o al encargado, o en su lugar, a las consultas, en particular, de las autoridades de control y de los interesados, sobre todos los asuntos relativos al tratamiento, a fin de garantizar el cumplimiento de lo dispuesto en el presente Reglamento.
5. La designación de un representante por el responsable o el encargado del tratamiento se entenderá sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable o encargado.

Artículo 28 Encargado del tratamiento

1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.
2. El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.
3. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:
   a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;
   b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;

c) tomará todas las medidas necesarias de conformidad con el artículo 32;

d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;

e) asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;

f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;

g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;

h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

4. Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado a que se refiere el apartado 3, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.
5. La adhesión del encargado del tratamiento a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a que se refieren los apartados 1 y 4 del presente artículo.
6. Sin perjuicio de que el responsable y el encargado del tratamiento celebren un contrato individual, el contrato u otro acto jurídico a que se refieren los apartados 3 y 4 del presente artículo podrá basarse, total o parcialmente, en las cláusulas contractuales tipo a que se refieren los apartados 7 y 8 del presente artículo, inclusive cuando formen parte de una certificación concedida al responsable o encargado de conformidad con los artículos 42 y 43.
7. La Comisión podrá fijar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.
8. Una autoridad de control podrá adoptar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el mecanismo de coherencia a que se refiere el artículo 63.
9. El contrato u otro acto jurídico a que se refieren los apartados 3 y 4 constará por escrito, inclusive en formato electrónico.
10. Sin perjuicio de lo dispuesto en los artículos 82, 83 y 84, si un encargado del tratamiento infringe el presente Reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento.

Artículo 29 Tratamiento bajo la autoridad del responsable o del encargado del tratamiento

El encargado del tratamiento y cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo podrán tratar dichos datos siguiendo instrucciones del responsable, a no ser que estén obligados a ello en virtud del Derecho de la Unión o de los Estados miembros.

Artículo 30 Registro de las actividades de tratamiento

1. Cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:
   a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;
   b) los fines del tratamiento;
   c) una descripción de las categorías de interesados y de las categorías de datos personales;
   d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
   e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
   f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
   g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.
2. Cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:
   a) el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;
   b) las categorías de tratamientos efectuados por cuenta de cada responsable;
   c) en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
   d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30, apartado 1.
3. Los registros a que se refieren los apartados 1 y 2 constarán por escrito, inclusive en formato electrónico.
4. El responsable o el encargado del tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la autoridad de control que lo solicite.
5. Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.

Artículo 31 Cooperación con la autoridad de control

El responsable y el encargado del tratamiento y, en su caso, sus representantes cooperarán con la autoridad de control que lo solicite en el desempeño de sus funciones.

Sección 2. Seguridad de los datos personales

Artículo 32 Seguridad del tratamiento

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:
   a) la seudonimización y el cifrado de datos personales; la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
   b) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
   c) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.
2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.
3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.
4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.

Artículo 33 Notificación de una violación de la seguridad de los datos personales a la autoridad de control

1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.
2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.
3. La notificación contemplada en el apartado 1 deberá, como mínimo:
   a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
   b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;

c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;

d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo.

Artículo 34 Comunicación de una violación de la seguridad de los datos personales al interesado

1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

   a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

   b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;

   c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3.

Sección 3. Evaluación de impacto relativa a la protección de datos y consulta previa

Artículo 35 Evaluación de impacto relativa a la protección de datos

1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

a) 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;

b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o

c) observación sistemática a gran escala de una zona de acceso público.

4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.

5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.

6. Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.

7. La evaluación deberá incluir como mínimo:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

8. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.

9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.

11. En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento.

Artículo 36 Consulta previa

1. El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo.
2. Cuando la autoridad de control considere que el tratamiento previsto a que se refiere el apartado 1 podría infringir el presente Reglamento, en particular cuando el responsable no haya identificado o mitigado suficientemente el riesgo, la autoridad de control deberá, en un plazo de ocho semanas desde la solicitud de la consulta, asesorar por escrito al responsable, y en su caso al encargado, y podrá utilizar cualquiera de sus poderes mencionados en el artículo 58. Dicho plazo podrá prorrogarse seis semanas, en función de la complejidad del tratamiento previsto. La autoridad de control informará al responsable y, en su caso, al encargado de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, indicando los motivos de la dilación. Estos plazos podrán suspenderse hasta que la autoridad de control haya obtenido la información solicitada a los fines de la consulta.
3. Cuando consulte a la autoridad de control con arreglo al apartado 1, el responsable del tratamiento le facilitará la información siguiente:
   a) en su caso, las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento, en particular en caso de tratamiento dentro de un grupo empresarial;
   b) los fines y medios del tratamiento previsto;
   c) las medidas y garantías establecidas para proteger los derechos y libertades de los interesados de conformidad con el presente Reglamento;
   d) en su caso, los datos de contacto del delegado de protección de datos;
   e) la evaluación de impacto relativa a la protección de datos establecida en el artículo 35, y
   f) cualquier otra información que solicite la autoridad de control.
4. Los Estados miembros garantizarán que se consulte a la autoridad de control durante la elaboración de toda propuesta de medida legislativa que haya de adoptar un Parlamento nacional, o de una medida reglamentaria basada en dicha medida legislativa, que se refiera al tratamiento.
5. No obstante lo dispuesto en el apartado 1, el Derecho de los Estados miembros podrá obligar a los responsables del tratamiento a consultar a la autoridad de control y a recabar su autorización previa en relación con el tratamiento por un responsable en el ejercicio de una misión realizada en interés público, en particular el tratamiento en relación con la protección social y la salud pública.

Sección 4. Delegado de protección de datos

Artículo 37 Designación del delegado de protección de datos

1. El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:
   a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;
   b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o
   c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos con arreglo al artículo 9 o de datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.
2. Un grupo empresarial podrá nombrar un único delegado de protección de datos siempre que sea fácilmente accesible desde cada establecimiento.

3. Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño.
4. En casos distintos de los contemplados en el apartado 1, el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen a categorías de responsables o encargados podrán designar un delegado de protección de datos o deberán designarlo si así lo exige el Derecho de la Unión o de los Estados miembros. El delegado de protección de datos podrá actuar por cuenta de estas asociaciones y otros organismos que representen a responsables o encargados.
5. El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39.
6. El delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.
7. El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control.

Artículo 38 Posición del delegado de protección de datos

1. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.
2. El responsable y el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de las funciones mencionadas en el artículo 39, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.
3. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.
4. Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento.
5. El delegado de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros.
6. El delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses.

Artículo 39 Funciones del delegado de protección de datos

1. El delegado de protección de datos tendrá como mínimo las siguientes funciones:
   a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;
   b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;

d) cooperar con la autoridad de control;

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

2. El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Sección 5. Códigos de conducta y certificación

Artículo 40 Códigos de conducta

1. Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación del presente Reglamento, teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas.
2. Las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta o modificar o ampliar dichos códigos con objeto de especificar la aplicación del presente Reglamento, como en lo que respecta a:

   a) el tratamiento leal y transparente;

   b) los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos;

   c) la recogida de datos personales;

   d) la seudonimización de datos personales;

   e) la información proporcionada al público y a los interesados;

   f) el ejercicio de los derechos de los interesados;

   g) la información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño;

   h) las medidas y procedimientos a que se refieren los artículos 24 y 25 y las medidas para garantizar la seguridad del tratamiento a que se refiere el artículo 32;

   i) la notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados;

   j) la transferencia de datos personales a terceros países u organizaciones internacionales, o

   k) los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos que permitan resolver las controversias entre los responsables del tratamiento y los interesados relativas al tratamiento, sin perjuicio de los derechos de los interesados en virtud de los artículos 77 y 79.

3. Además de la adhesión de los responsables o encargados del tratamiento a los que se aplica el presente Reglamento, los responsables o encargados a los que no se aplica el presente Reglamento en virtud del artículo 3 podrán adherirse también a códigos de conducta aprobados de conformidad con el apartado 5 del presente artículo y que tengan validez general en virtud del apartado 9 del presente artículo, a fin de ofrecer garantías adecuadas en el marco de las transferencias de datos personales a terceros países u organizaciones internacionales a tenor del artículo 46, apartado 2, letra e). Dichos responsables o encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de los interesados.
4. El código de conducta a que se refiere el apartado 2 del presente artículo contendrá mecanismos que permitan al organismo mencionado en el artículo 41, apartado 1, efectuar el control obliga-

torio del cumplimiento de sus disposiciones por los responsables o encargados de tratamiento que se comprometan a aplicarlo, sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes con arreglo al artículo 51 o 56.

5. Las asociaciones y otros organismos mencionados en el apartado 2 del presente artículo que proyecten elaborar un código de conducta o modificar o ampliar un código existente presentarán el proyecto de código o la modificación o ampliación a la autoridad de control que sea competente con arreglo al artículo 55. La autoridad de control dictaminará si el proyecto de código o la modificación o ampliación es conforme con el presente Reglamento y aprobará dicho proyecto de código, modificación o ampliación si considera suficientes las garantías adecuadas ofrecidas.
6. Si el proyecto de código o la modificación o ampliación es aprobado de conformidad con el apartado 5 y el código de conducta de que se trate no se refiere a actividades de tratamiento en varios Estados miembros, la autoridad de control registrará y publicará el código.
7. Si un proyecto de código de conducta guarda relación con actividades de tratamiento en varios Estados miembros, la autoridad de control que sea competente en virtud del artículo 55 lo presentará por el procedimiento mencionado en el artículo 63, antes de su aprobación o de la modificación o ampliación, al Comité, el cual dictaminará si dicho proyecto, modificación o ampliación es conforme con el presente Reglamento o, en la situación indicada en el apartado 3 del presente artículo, ofrece garantías adecuadas.
8. Si el dictamen a que se refiere el apartado 7 confirma que el proyecto de código o la modificación o ampliación cumple lo dispuesto en el presente Reglamento o, en la situación indicada en el apartado 3, ofrece garantías adecuadas, el Comité presentará su dictamen a la Comisión.
9. La Comisión podrá, mediante actos de ejecución, decidir que el código de conducta o la modificación o ampliación aprobados y presentados con arreglo al apartado 8 del presente artículo tengan validez general dentro de la Unión. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.
10. La Comisión dará publicidad adecuada a los códigos aprobados cuya validez general haya sido decidida de conformidad con el apartado 9.
11. El Comité archivará en un registro todos los códigos de conducta, modificaciones y ampliaciones que se aprueben, y los pondrá a disposición pública por cualquier medio apropiado.

Artículo 41 Supervisión de códigos de conducta aprobados

1. Sin perjuicio de las funciones y los poderes de la autoridad de control competente en virtud de los artículos 57 y 58, podrá supervisar el cumplimiento de un código de conducta en virtud del artículo 40 un organismo que tenga el nivel adecuado de pericia en relación con el objeto del código y que haya sido acreditado para tal fin por la autoridad de control competente.
2. El organismo a que se refiere el apartado 1 podrá ser acreditado para supervisar el cumplimiento de un código de conducta si:
   a) ha demostrado, a satisfacción de la autoridad de control competente, su independencia y pericia en relación con el objeto del código;
   b) ha establecido procedimientos que le permitan evaluar la idoneidad de los responsables y encargados correspondientes para aplicar el código, supervisar el cumplimiento de sus disposiciones y examinar periódicamente su aplicación;
   c) ha establecido procedimientos y estructuras para tratar las reclamaciones relativas a infracciones del código o a la manera en que el código haya sido o esté siendo aplicado por un responsable o encargado del tratamiento, y para hacer dichos procedimientos y estructuras transparentes para los interesados y el público, y
   d) ha demostrado, a satisfacción de la autoridad de control competente, que sus funciones y cometidos no dan lugar a conflicto de intereses.

3. La autoridad de control competente someterá al Comité, con arreglo al mecanismo de coherencia a que se refiere el artículo 63, el proyecto que fije los requisitos de acreditación de un organismo a que se refiere el apartado 1 del presente artículo.
4. Sin perjuicio de las funciones y los poderes de la autoridad de control competente y de lo dispuesto en el capítulo VIII, un organismo a tenor del apartado 1 del presente artículo deberá, con sujeción a garantías adecuadas, tomar las medidas oportunas en caso de infracción del código por un responsable o encargado del tratamiento, incluida la suspensión o exclusión de este. Informará de dichas medidas y de las razones de las mismas a la autoridad de control competente.
5. La autoridad de control competente revocará la acreditación de un organismo a tenor del apartado 1 si los requisitos de acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicho organismo infringe el presente Reglamento.
6. El presente artículo no se aplicará al tratamiento realizado por autoridades y organismos públicos.

Artículo 42 Certificación

1. Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados. Se tendrán en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas.
2. Además de la adhesión de los responsables o encargados del tratamiento sujetos al presente Reglamento, podrán establecerse mecanismos de certificación, sellos o marcas de protección de datos aprobados de conformidad con el apartado 5, con objeto de demostrar la existencia de garantías adecuadas ofrecidas por los responsables o encargados no sujetos al presente Reglamento con arreglo al artículo 3 en el marco de transferencias de datos personales a terceros países u organizaciones internacionales a tenor del artículo 46, apartado 2, letra f). Dichos responsables o encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de los interesados.
3. La certificación será voluntaria y estará disponible a través de un proceso transparente.
4. La certificación a que se refiere el presente artículo no limitará la responsabilidad del responsable o encargado del tratamiento en cuanto al cumplimiento del presente Reglamento y se entenderá sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes en virtud del artículo 55 o 56.
5. La certificación en virtud del presente artículo será expedida por los organismos de certificación a que se refiere el artículo 43 o por la autoridad de control competente, sobre la base de los criterios aprobados por dicha autoridad de conformidad con el artículo 58, apartado 3, o por el Comité de conformidad con el artículo 63. Cuando los criterios sean aprobados por el Comité, esto podrá dar lugar a una certificación común: el Sello Europeo de Protección de Datos.
6. Los responsables o encargados que sometan su tratamiento al mecanismo de certificación dará al organismo de certificación mencionado en el artículo 43, o en su caso a la autoridad de control competente, toda la información y acceso a sus actividades de tratamiento que necesite para llevar a cabo el procedimiento de certificación.
7. La certificación se expedirá a un responsable o encargado de tratamiento por un período máximo de tres años y podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los criterios pertinentes. La certificación será retirada, cuando proceda, por los organismos de certificación a que se refiere el artículo 43, o en su caso por la autoridad de control competente, cuando no se cumplan o se hayan dejado de cumplir los criterios para la certificación.
8. El Comité archivará en un registro todos los mecanismos de certificación y sellos y marcas de protección de datos y los pondrá a disposición pública por cualquier medio apropiado.

Artículo 43 Organismo de certificación

1. Sin perjuicio de las funciones y poderes de la autoridad de control competente en virtud de los artículos 57 y 58, los organismos de certificación que tengan un nivel adecuado de pericia en materia de protección de datos expedirán y renovarán las certificaciones una vez informada la autoridad de control, a fin de esta que pueda ejercer, si así se requiere, sus poderes en virtud del artículo 58, apartado 2, letra h). Los Estados miembros garantizarán que dichos organismos de certificación sean acreditados por la autoridad o el organismo indicado a continuación, o por ambos:
   a) la autoridad de control que sea competente en virtud del artículo 55 o 56;
   b) el organismo nacional de acreditación designado de conformidad con el Reglamento (CE) n.o 765/2008 del Parlamento Europeo y del Consejo (1) con arreglo a la norma EN ISO/IEC 17065/2012 y a los requisitos adicionales establecidos por la autoridad de control que sea competente en virtud del artículo 55 o 56.
2. Los organismos de certificación mencionados en el apartado 1 únicamente serán acreditados de conformidad con dicho apartado si:
   a) han demostrado, a satisfacción de la autoridad de control competente, su independencia y su pericia en relación con el objeto de la certificación;
   b) se han comprometido a respetar los criterios mencionados en el artículo 42, apartado 5, y aprobados por la autoridad de control que sea competente en virtud del artículo 55 o 56, o por el Comité de conformidad con el artículo 63;
   c) han establecido procedimientos para la expedición, la revisión periódica y la retirada de certificaciones, sellos y marcas de protección de datos;
   d) han establecido procedimientos y estructuras para tratar las reclamaciones relativas a infracciones de la certificación o a la manera en que la certificación haya sido o esté siendo aplicada por un responsable o encargado del tratamiento, y para hacer dichos procedimientos y estructuras transparentes para los interesados y el público, y
   e) han demostrado, a satisfacción de la autoridad de control competente, que sus funciones y cometidos no dan lugar a conflicto de intereses.
3. La acreditación de los organismos de certificación a que se refieren los apartados 1 y 2 del presente artículo se realizará sobre la base de los requisitos aprobados por la autoridad de control que sea competente en virtud del artículo 55 o 56 o por el Comité en virtud del artículo 63. En caso de acreditación de conformidad con el apartado 1, letra b), del presente artículo, estos requisitos complementarán los contemplados en el Reglamento (CE) n.o 765/2008 y las normas técnicas que describen los métodos y procedimientos de los organismos de certificación.
4. Los organismos de certificación a que se refiere el apartado 1 serán responsable de la correcta evaluación a efectos de certificación o retirada de la certificación, sin perjuicio de la responsabilidad del responsable o del encargado del tratamiento en cuanto al cumplimiento del presente Reglamento. La acreditación se expedirá por un período máximo de cinco años y podrá ser renovada en las mismas condiciones, siempre y cuando el organismo de certificación cumpla los requisitos establecidos en el presente artículo.
5. Los organismos de certificación a que se refiere el apartado 1 comunicarán a las autoridades de control competentes las razones de la expedición de la certificación solicitada o de su retirada.
6. La autoridad de control hará públicos los requisitos a que se refiere el apartado 3 del presente artículo y los criterios a que se a refiere el artículo 42, apartado 5, en una forma fácilmente accesible. Las autoridades de control comunicarán también dichos requisitos y criterios al Comité.
7. No obstante lo dispuesto en el capítulo VIII, la autoridad de control competente o el organismo nacional de acreditación revocará la acreditación a un organismo de certificación a tenor del apartado 1 del presente artículo si las condiciones de la acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicho organismo de certificación infringe el presente Reglamento.

8. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 92, a fin de especificar las condiciones que deberán tenerse en cuenta para los mecanismos de certificación en materia de protección de datos a que se refiere el artículo 42, apartado 1.
9. La Comisión podrá adoptar actos de ejecución que establezcan normas técnicas para los mecanismos de certificación y los sellos y marcas de protección de datos, y mecanismos para promover y reconocer dichos mecanismos de certificación, sellos y marcas. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

CAPÍTULO V. Transferencias de datos personales a terceros países u organizaciones internacionales

Artículo 44 Principio general de las transferencias

Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado.

Artículo 45 Transferencias basadas en una decisión de adecuación

1. Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica.
2. Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos:
   a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos;
   b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y
   c) los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

3. La Comisión, tras haber evaluado la adecuación del nivel de protección, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado a tenor de lo dispuesto en el apartado 2 del presente artículo. El acto de ejecución establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. El acto de ejecución especificará su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control a que se refiere el apartado 2, letra b), del presente artículo. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.
4. La Comisión supervisará de manera continuada los acontecimientos en países terceros y organizaciones internacionales que puedan afectar a la efectiva aplicación de las decisiones adoptadas con arreglo al apartado 3 del presente artículo y de las decisiones adoptadas sobre la base del artículo 25, apartado 6, de la Directiva 95/46/CE.
5. Cuando la información disponible, en particular tras la revisión a que se refiere el apartado 3 del presente artículo, muestre que un tercer país, un territorio o un sector específico de ese tercer país, o una organización internacional ya no garantiza un nivel de protección adecuado a tenor del apartado 2 del presente artículo, la Comisión, mediante actos de ejecución, derogará, modificará o suspenderá, en la medida necesaria y sin efecto retroactivo, la decisión a que se refiere el apartado 3 del presente artículo. Dichos actos de ejecución se adoptarán de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.

   Por razones imperiosas de urgencia debidamente justificadas, la Comisión adoptará actos de ejecución inmediatamente aplicables de conformidad con el procedimiento a que se refiere el artículo 93, apartado 3.
6 La Comisión entablará consultas con el tercer país u organización internacional con vistas a poner remedio a la situación que dé lugar a la decisión adoptada de conformidad con el apartado 5.
7. Toda decisión de conformidad con el apartado 5 del presente artículo se entenderá sin perjuicio de las transferencias de datos personales al tercer país, a un territorio o uno o varios sectores específicos de ese tercer país, o a la organización internacional de que se trate en virtud de los artículos 46 a 49.
8. La Comisión publicará en el *Diario Oficial de la Unión Europea* y en su página web una lista de terceros países, territorios y sectores específicos en un tercer país, y organizaciones internacionales respecto de los cuales haya decidido que se garantiza, o ya no, un nivel de protección adecuado.
9. Las decisiones adoptadas por la Comisión en virtud del artículo 25, apartado 6, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas por una decisión de la Comisión adoptada de conformidad con los apartados 3 o 5 del presente artículo.

Artículo 46 Transferencias mediante garantías adecuadas

1. A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.
2. Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por:
   a) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;
   b) normas corporativas vinculantes de conformidad con el artículo 47;
   c) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2;
   d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2;

e) un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o

f) un mecanismo de certificación aprobado con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.

3. Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas contempladas en el apartado 1 podrán igualmente ser aportadas, en particular, mediante:

a) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o

b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.

4. La autoridad de control aplicará el mecanismo de coherencia a que se refiere el artículo 63 en los casos indicados en el apartado 3 del presente artículo.

5. Las autorizaciones otorgadas por un Estado miembro o una autoridad de control de conformidad con el artículo 26, apartado 2, de la Directiva 95/46/CE seguirán siendo válidas hasta que hayan sido modificadas, sustituidas o derogadas, en caso necesario, por dicha autoridad de control. Las decisiones adoptadas por la Comisión en virtud del artículo 26, apartado 4, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas, en caso necesario, por una decisión de la Comisión adoptada de conformidad con el apartado 2 del presente artículo.

Artículo 47 Normas corporativas vinculantes

1. La autoridad de control competente aprobará normas corporativas vinculantes de conformidad con el mecanismo de coherencia establecido en el artículo 63, siempre que estas:

a) sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus empleados;

b) confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales, y

c) cumplan los requisitos establecidos en el apartado 2.

2. Las normas corporativas vinculantes mencionadas en el apartado 1 especificarán, como mínimo, los siguientes elementos:

a) la estructura y los datos de contacto del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta y de cada uno de sus miembros;

b) las transferencias o conjuntos de transferencias de datos, incluidas las categorías de datos personales, el tipo de tratamientos y sus fines, el tipo de interesados afectados y el nombre del tercer o los terceros países en cuestión;

c) su carácter jurídicamente vinculante, tanto a nivel interno como externo;

d) la aplicación de los principios generales en materia de protección de datos, en particular la limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento, el tratamiento de categorías especiales de datos personales, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes;

e) los derechos de los interesados en relación con el tratamiento y los medios para ejercerlos, en particular el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles de conformidad con lo dispuesto en el artículo 22, el derecho a presentar una reclamación ante la autoridad de control competente y

ante los tribunales competentes de los Estados miembros de conformidad con el artículo 79, y el derecho a obtener una reparación, y, cuando proceda, una indemnización por violación de las normas corporativas vinculantes;

f) la aceptación por parte del responsable o del encargado del tratamiento establecidos en el territorio de un Estado miembro de la responsabilidad por cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro de que se trate no establecido en la Unión; el responsable o el encargado solo será exonerado, total o parcialmente, de dicha responsabilidad si demuestra que el acto que originó los daños y perjuicios no es imputable a dicho miembro;

g) la forma en que se facilita a los interesados la información sobre las normas corporativas vinculantes, en particular en lo que respecta a las disposiciones contempladas en las letras d), e) y f) del presente apartado, además de los artículos 13 y 14;

h) las funciones de todo delegado de protección de datos designado de conformidad con el artículo 37, o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, así como de la supervisión de la formación y de la tramitación de las reclamaciones;

i) los procedimientos de reclamación;

j) los mecanismos establecidos dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos incluirán auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del interesado. Los resultados de dicha verificación deberían comunicarse a la persona o entidad a que se refiere la letra h) y al consejo de administración de la empresa que controla un grupo empresarial, o de la unión de empresas dedicadas a una actividad económica conjunta, y ponerse a disposición de la autoridad de control competente que lo solicite;

k) los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la autoridad de control;

l) el mecanismo de cooperación con la autoridad de control para garantizar el cumplimiento por parte de cualquier miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, en particular poniendo a disposición de la autoridad de control los resultados de las verificaciones de las medidas contempladas en la letra j);

m) los mecanismos para informar a la autoridad de control competente de cualquier requisito jurídico de aplicación en un país tercero a un miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, que probablemente tengan un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes, y

n) la formación en protección de datos pertinente para el personal que tenga acceso permanente o habitual a datos personales.

3. La Comisión podrá especificar el formato y los procedimientos para el intercambio de información entre los responsables, los encargados y las autoridades de control en relación con las normas corporativas vinculantes a tenor de lo dispuesto en el presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

Artículo 48 Transferencias o comunicaciones no autorizadas por el Derecho de la Unión

Cualquier sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país que exijan que un responsable o encargado del tratamiento transfiera o comunique datos personales únicamente será reconocida o ejecutable en cualquier modo si se basa en un acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el país tercero requirente y la Unión o un Estado miembro, sin perjuicio de otros motivos para la transferencia al amparo del presente capítulo.

Artículo 49 Excepciones para situaciones específicas

1. En ausencia de una decisión de adecuación de conformidad con el artículo 45, apartado 3, o de garantías adecuadas de conformidad con el artículo 46, incluidas las normas corporativas vinculantes, una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional únicamente se realizará si se cumple alguna de las condiciones siguientes:
   a) el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas;
   b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado;
   c) la transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica;
   d) la transferencia sea necesaria por razones importantes de interés público;
   e) la transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones;
   f) la transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento;
   g) la transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta.

   Cuando una transferencia no pueda basarse en disposiciones de los artículos 45 o 46, incluidas las disposiciones sobre normas corporativas vinculantes, y no sea aplicable ninguna de las excepciones para situaciones específicas a que se refiere el párrafo primero del presente apartado, solo se podrá llevar a cabo si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofreció garantías apropiadas con respecto a la protección de datos personales. El responsable del tratamiento informará a la autoridad de control de la transferencia. Además de la información a que hacen referencia los artículos 13 y 14, el responsable del tratamiento informará al interesado de la transferencia y de los intereses legítimos imperiosos perseguidos.
2. Una transferencia efectuada de conformidad con el apartado 1, párrafo primero, letra g), no abarcará la totalidad de los datos personales ni categorías enteras de datos personales contenidos en el registro. Si la finalidad del registro es la consulta por parte de personas que tengan un interés legítimo, la transferencia solo se efectuará a solicitud de dichas personas o si estas han de ser las destinatarias.
3. En el apartado 1, el párrafo primero, letras a), b) y c), y el párrafo segundo no serán aplicables a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus poderes públicos.
4. El interés público contemplado en el apartado 1, párrafo primero, letra d), será reconocido por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.
5. En ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el Derecho de la Unión o de los Estados miembros podrá, por razones importantes de interés público, establecer expresamente límites a la transferencia de categorías específicas de datos a un tercer país u organización internacional. Los Estados miembros notificarán a la Comisión dichas disposiciones.

6. El responsable o el encargado del tratamiento documentarán en los registros indicados en el artículo 30 la evaluación y las garantías apropiadas a que se refiere el apartado 1, párrafo segundo, del presente artículo.

Artículo 50 Cooperación internacional en el ámbito de la protección de datos personales

En relación con los terceros países y las organizaciones internacionales, la Comisión y las autoridades de control tomarán medidas apropiadas para:

a) crear mecanismos de cooperación internacional que faciliten la aplicación eficaz de la legislación relativa a la protección de datos personales;

b) prestarse mutuamente asistencia a escala internacional en la aplicación de la legislación relativa a la protección de datos personales, en particular mediante la notificación, la remisión de reclamaciones, la asistencia en las investigaciones y el intercambio de información, a reserva de las garantías adecuadas para la protección de los datos personales y otros derechos y libertades fundamentales;

c) asociar a partes interesadas en la materia a los debates y actividades destinados a reforzar la cooperación internacional en la aplicación de la legislación relativa a la protección de datos personales;

d) promover el intercambio y la documentación de la legislación y las prácticas en materia de protección de datos personales, inclusive en materia de conflictos de jurisdicción con terceros países.

CAPÍTULO VI. Autoridades de control independientes

Sección 1. Independencia

Artículo 51 Autoridad de control

1. Cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades públicas independientes (en adelante «autoridad de control») supervisar la aplicación del presente Reglamento, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión.
2. Cada autoridad de control contribuirá a la aplicación coherente del presente Reglamento en toda la Unión. A tal fin, las autoridades de control cooperarán entre sí y con la Comisión con arreglo a lo dispuesto en el capítulo VII.
3. Cuando haya varias autoridades de control en un Estado miembro, este designará la autoridad de control que representará a dichas autoridades en el Comité, y establecerá el mecanismo que garantice el cumplimiento por las demás autoridades de las normas relativas al mecanismo de coherencia a que se refiere el artículo 63.
4. Cada Estado miembro notificará a la Comisión las disposiciones legales que adopte de conformidad con el presente capítulo a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior que afecte a dichas disposiciones.

Artículo 52 Independencia

1. Cada autoridad de control actuará con total independencia en el desempeño de sus funciones y en el ejercicio de sus poderes de conformidad con el presente Reglamento.
2. El miembro o los miembros de cada autoridad de control serán ajenos, en el desempeño de sus funciones y en el ejercicio de sus poderes de conformidad con el presente Reglamento, a toda influencia externa, ya sea directa o indirecta, y no solicitarán ni admitirán ninguna instrucción.
3. El miembro o los miembros de cada autoridad de control se abstendrán de cualquier acción que sea incompatible con sus funciones y no participarán, mientras dure su mandato, en ninguna actividad profesional que sea incompatible, remunerada o no.

4. Cada Estado miembro garantizará que cada autoridad de control disponga en todo momento de los recursos humanos, técnicos y financieros, así como de los locales y las infraestructuras necesarios para el cumplimiento efectivo de sus funciones y el ejercicio de sus poderes, incluidos aquellos que haya de ejercer en el marco de la asistencia mutua, la cooperación y la participación en el Comité.
5. Cada Estado miembro garantizará que cada autoridad de control elija y disponga de su propio personal, que estará sujeto a la autoridad exclusiva del miembro o miembros de la autoridad de control interesada.
6. Cada Estado miembro garantizará que cada autoridad de control esté sujeta a un control financiero que no afecte a su independencia y que disponga de un presupuesto anual, público e independiente, que podrá formar parte del presupuesto general del Estado o de otro ámbito nacional.

Artículo 53 Condiciones generales aplicables a los miembros de la autoridad de control

1. Los Estados miembros dispondrán que cada miembro de sus autoridades de control sea nombrado mediante un procedimiento transparente por:
   - su Parlamento,
   - su Gobierno,
   - su Jefe de Estado, o
   - un organismo independiente encargado del nombramiento en virtud del Derecho de los Estados miembros.
2. Cada miembro poseerá la titulación, la experiencia y las aptitudes, en particular en el ámbito de la protección de datos personales, necesarias para el cumplimiento de sus funciones y el ejercicio de sus poderes.
3. Los miembros darán por concluidas sus funciones en caso de terminación del mandato, dimisión o jubilación obligatoria, de conformidad con el Derecho del Estado miembro de que se trate.
4. Un miembro será destituido únicamente en caso de conducta irregular grave o si deja de cumplir las condiciones exigidas en el desempeño de sus funciones.

Artículo 54 Normas relativas al establecimiento de la autoridad de control

1. Cada Estado miembro establecerá por ley todos los elementos indicados a continuación:
   a) el establecimiento de cada autoridad de control;
   b) las cualificaciones y condiciones de idoneidad necesarias para ser nombrado miembro de cada autoridad de control;
   c) las normas y los procedimientos para el nombramiento del miembro o miembros de cada autoridad de control;
   d) la duración del mandato del miembro o los miembros de cada autoridad de control, no inferior a cuatro años, salvo el primer nombramiento posterior al 24 de mayo de 2016, parte del cual podrá ser más breve cuando sea necesario para proteger la independencia de la autoridad de control por medio de un procedimiento de nombramiento escalonado;
   e) el carácter renovable o no del mandato del miembro o los miembros de cada autoridad de control y, en su caso, el número de veces que podrá renovarse;
   f) las condiciones por las que se rigen las obligaciones del miembro o los miembros y del personal de cada autoridad de control, las prohibiciones relativas a acciones, ocupaciones y prestaciones incompatibles con el cargo durante el mandato y después del mismo, y las normas que rigen el cese en el empleo.
2. El miembro o miembros y el personal de cada autoridad de control estarán sujetos, de conformidad con el Derecho de la Unión o de los Estados miembros, al deber de secreto profesional, tanto durante su mandato como después del mismo, con relación a las informaciones confidenciales

de las que hayan tenido conocimiento en el cumplimiento de sus funciones o el ejercicio de sus poderes. Durante su mandato, dicho deber de secreto profesional se aplicará en particular a la información recibida de personas físicas en relación con infracciones del presente Reglamento.

Sección 2. Competencia, funciones y poderes

Artículo 55 Competencia

1. Cada autoridad de control será competente para desempeñar las funciones que se le asignen y ejercer los poderes que se le confieran de conformidad con el presente Reglamento en el territorio de su Estado miembro.
2. Cuando el tratamiento sea efectuado por autoridades públicas o por organismos privados que actúen con arreglo al artículo 6, apartado 1, letras c) o e), será competente la autoridad de control del Estado miembro de que se trate. No será aplicable en tales casos el artículo 56.
3. Las autoridades de control no serán competentes para controlar las operaciones de tratamiento efectuadas por los tribunales en el ejercicio de su función judicial.

Artículo 56 Competencia de la autoridad de control principal

1. Sin perjuicio de lo dispuesto en el artículo 55, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento será competente para actuar como autoridad de control principal para el tratamiento transfronterizo realizado por parte de dicho responsable o encargado con arreglo al procedimiento establecido en el artículo 60.
2. No obstante lo dispuesto en el apartado 1, cada autoridad de control será competente para tratar una reclamación que le sea presentada o una posible infracción del presente Reglamento, en caso de que se refiera únicamente a un establecimiento situado en su Estado miembro o únicamente afecte de manera sustancial a interesados en su Estado miembro.
3. En los casos a que se refiere el apartado 2 del presente artículo, la autoridad de control informará sin dilación al respecto a la autoridad de control principal. En el plazo de tres semanas después de haber sido informada, la autoridad de control principal decidirá si tratará o no el caso de conformidad con el procedimiento establecido en el artículo 60, teniendo presente si existe un establecimiento del responsable o encargado del tratamiento en el Estado miembro de la autoridad de control que le haya informado.
4. En caso de que la autoridad de control principal decida tratar el caso, se aplicará el procedimiento establecido en el artículo 60. La autoridad de control que haya informado a la autoridad de control principal podrá presentarle un proyecto de decisión. La autoridad de control principal tendrá en cuenta en la mayor medida posible dicho proyecto al preparar el proyecto de decisión a que se refiere el artículo 60, apartado 3.
5. En caso de que la autoridad de control principal decida no tratar el caso, la autoridad de control que le haya informado lo tratará con arreglo a los artículos 61 y 62.
6. La autoridad de control principal será el único interlocutor del responsable o del encargado en relación con el tratamiento transfronterizo realizado por dicho responsable o encargado.

Artículo 57 Funciones

1. Sin perjuicio de otras funciones en virtud del presente Reglamento, incumbirá a cada autoridad de control, en su territorio:
   a) controlar la aplicación del presente Reglamento y hacerlo aplicar;
   b) promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento. Las actividades dirigidas específicamente a los niños deberán ser objeto de especial atención;

c) asesorar, con arreglo al Derecho de los Estados miembros, al Parlamento nacional, al Gobierno y a otras instituciones y organismos sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento;

d) promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben en virtud del presente Reglamento;

e) previa solicitud, facilitar información a cualquier interesado en relación con el ejercicio de sus derechos en virtud del presente Reglamento y, en su caso, cooperar a tal fin con las autoridades de control de otros Estados miembros;

f) tratar las reclamaciones presentadas por un interesado o por un organismo, organización o asociación de conformidad con el artículo 80, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable, en particular si fueran necesarias nuevas investigaciones o una coordinación más estrecha con otra autoridad de control;

g) cooperar, en particular compartiendo información, con otras autoridades de control y prestar asistencia mutua con el fin de garantizar la coherencia en la aplicación y ejecución del presente Reglamento;

h) llevar a cabo investigaciones sobre la aplicación del presente Reglamento, en particular basándose en información recibida de otra autoridad de control u otra autoridad pública;

i) hacer un seguimiento de cambios que sean de interés, en la medida en que tengan incidencia en la protección de datos personales, en particular el desarrollo de las tecnologías de la información y la comunicación y las prácticas comerciales;

j) adoptar las cláusulas contractuales tipo a que se refieren el artículo 28, apartado 8, y el artículo 46, apartado 2, letra d);

k) elaborar y mantener una lista relativa al requisito de la evaluación de impacto relativa a la protección de datos, en virtud del artículo 35, apartado 4;

l) ofrecer asesoramiento sobre las operaciones de tratamiento contempladas en el artículo 36, apartado 2;

m) alentar la elaboración de códigos de conducta con arreglo al artículo 40, apartado 1, y dictaminar y aprobar los códigos de conducta que den suficientes garantías con arreglo al artículo 40, apartado 5;

n) fomentar la creación de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos con arreglo al artículo 42, apartado 1, y aprobar los criterios de certificación de conformidad con el artículo 42, apartado 5;

o) llevar a cabo, si procede, una revisión periódica de las certificaciones expedidas en virtud del artículo 42, apartado 7;

p) elaborar y publicar los requisitos para la acreditación de organismos de supervisión de los códigos de conducta con arreglo al artículo 41 y de organismos de certificación con arreglo al artículo 43;

q) efectuar la acreditación de organismos de supervisión de los códigos de conducta con arreglo al artículo 41 y de organismos de certificación con arreglo al artículo 43;

r) autorizar las cláusulas contractuales y disposiciones a que se refiere el artículo 46, apartado 3;

s) aprobar normas corporativas vinculantes de conformidad con lo dispuesto en el artículo 47;

t) contribuir a las actividades del Comité;

u) llevar registros internos de las infracciones del presente Reglamento y de las medidas adoptadas de conformidad con el artículo 58, apartado 2, y

v) desempeñar cualquier otra función relacionada con la protección de los datos personales.

2. Cada autoridad de control facilitará la presentación de las reclamaciones contempladas en el apartado 1, letra f), mediante medidas como un formulario de presentación de reclamaciones que pueda cumplimentarse también por medios electrónicos, sin excluir otros medios de comunicación.

3. El desempeño de las funciones de cada autoridad de control será gratuito para el interesado y, en su caso, para el delegado de protección de datos.
4. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, la autoridad de control podrá establecer una tasa razonable basada en los costes administrativos o negarse a actuar respecto de la solicitud. La carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud recaerá en la autoridad de control.

Artículo 58 Poderes

1. Cada autoridad de control dispondrá de todos los poderes de investigación indicados a continuación:
   a) ordenar al responsable y al encargado del tratamiento y, en su caso, al representante del responsable o del encargado, que faciliten cualquier información que requiera para el desempeño de sus funciones;
   b) llevar a cabo investigaciones en forma de auditorías de protección de datos;
   c) llevar a cabo una revisión de las certificaciones expedidas en virtud del artículo 42, apartado 7;
   d) notificar al responsable o al encargado del tratamiento las presuntas infracciones del presente Reglamento;
   e) obtener del responsable y del encargado del tratamiento el acceso a todos los datos personales y a toda la información necesaria para el ejercicio de sus funciones;
   f) obtener el acceso a todos los locales del responsable y del encargado del tratamiento, incluidos cualesquiera equipos y medios de tratamiento de datos, de conformidad con el Derecho procesal de la Unión o de los Estados miembros.
2. Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:
   a) sancionar a todo responsable o encargado del tratamiento con una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el presente Reglamento;
   b) sancionar a todo responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;
   c) ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado en virtud del presente Reglamento;
   d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado;
   e) ordenar al responsable del tratamiento que comunique al interesado las violaciones de la seguridad de los datos personales;
   f) imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición;
   g) ordenar la rectificación o supresión de datos personales o la limitación de tratamiento con arreglo a los artículos 16, 17 y 18 y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales con arreglo a al artículo 17, apartado 2, y al artículo 19;
   h) retirar una certificación u ordenar al organismo de certificación que retire una certificación emitida con arreglo a los artículos 42 y 43, u ordenar al organismo de certificación que no se emita una certificación si no se cumplen o dejan de cumplirse los requisitos para la certificación;
   i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;
   j) ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

3. Cada autoridad de control dispondrá de todos los poderes de autorización y consultivos indicados a continuación:
   a) asesorar al responsable del tratamiento conforme al procedimiento de consulta previa contemplado en el artículo 36;
   b) emitir, por iniciativa propia o previa solicitud, dictámenes destinados al Parlamento nacional, al Gobierno del Estado miembro o, con arreglo al Derecho de los Estados miembros, a otras instituciones y organismos, así como al público, sobre cualquier asunto relacionado con la protección de los datos personales;
   c) autorizar el tratamiento a que se refiere el artículo 36, apartado 5, si el Derecho del Estado miembro requiere tal autorización previa;
   d) emitir un dictamen y aprobar proyectos de códigos de conducta de conformidad con lo dispuesto en el artículo 40, apartado 5;
   e) acreditar los organismos de certificación con arreglo al artículo 43;
   f) expedir certificaciones y aprobar criterios de certificación con arreglo al artículo 42, apartado 5;
   g) adoptar las cláusulas tipo de protección de datos contempladas en el artículo 28, apartado 8, y el artículo 46, apartado 2, letra d);
   h) autorizar las cláusulas contractuales indicadas en el artículo 46, apartado 3, letra a);
   i) autorizar los acuerdos administrativos contemplados en el artículo 46, apartado 3, letra b);
   j) aprobar normas corporativas vinculantes de conformidad con lo dispuesto en el artículo 47.
4. El ejercicio de los poderes conferidos a la autoridad de control en virtud del presente artículo estará sujeto a las garantías adecuadas, incluida la tutela judicial efectiva y al respeto de las garantías procesales, establecidas en el Derecho de la Unión y de los Estados miembros de conformidad con la Carta.
5. Cada Estado miembro dispondrá por ley que su autoridad de control esté facultada para poner en conocimiento de las autoridades judiciales las infracciones del presente Reglamento y, si procede, para iniciar o ejercitar de otro modo acciones judiciales, con el fin de hacer cumplir lo dispuesto en el mismo.
6. Cada Estado miembro podrá establecer por ley que su autoridad de control tenga otros poderes además de los indicadas en los apartados 1, 2 y 3. El ejercicio de dichos poderes no será obstáculo a la aplicación efectiva del capítulo VII.

Artículo 59 Informe de actividad

Cada autoridad de control elaborará un informe anual de sus actividades, que podrá incluir una lista de tipos de infracciones notificadas y de tipos de medidas adoptadas de conformidad con el artículo 58, apartado 2. Los informes se transmitirán al Parlamento nacional, al Gobierno y a las demás autoridades designadas en virtud del Derecho de los Estados miembros. Se pondrán a disposición del público, de la Comisión y del Comité.

CAPÍTULO VII. Cooperación y coherencia

Sección 1. Cooperación y coherencia

Artículo 60 Cooperación entre la autoridad de control principal y las demás autoridades de control interesadas

1. La autoridad de control principal cooperará con las demás autoridades de control interesadas de acuerdo con el presente artículo, esforzándose por llegar a un consenso. La autoridad de control principal y las autoridades de control interesadas se intercambiarán toda información pertinente.

2. La autoridad de control principal podrá solicitar en cualquier momento a otras autoridades de control interesadas que presten asistencia mutua con arreglo al artículo 61, y podrá llevar a cabo operaciones conjuntas con arreglo al artículo 62, en particular para realizar investigaciones o supervisar la aplicación de una medida relativa a un responsable o un encargado del tratamiento establecido en otro Estado miembro.
3. La autoridad de control principal comunicará sin dilación a las demás autoridades de control interesadas la información pertinente a este respecto. Transmitirá sin dilación un proyecto de decisión a las demás autoridades de control interesadas para obtener su dictamen al respecto y tendrá debidamente en cuenta sus puntos de vista.
4. En caso de que cualquiera de las autoridades de control interesadas formule una objeción pertinente y motivada acerca del proyecto de decisión en un plazo de cuatro semanas a partir de la consulta con arreglo al apartado 3 del presente artículo, la autoridad de control principal someterá el asunto, en caso de que no siga lo indicado en la objeción pertinente y motivada o estime que dicha objeción no es pertinente o no está motivada, al mecanismo de coherencia contemplado en el artículo 63.
5. En caso de que la autoridad de control principal prevea seguir lo indicado en la objeción pertinente y motivada recibida, presentará a dictamen de las demás autoridades de control interesadas un proyecto de decisión revisado. Dicho proyecto de decisión revisado se someterá al procedimiento indicado en el apartado 4 en un plazo de dos semanas.
6. En caso de que ninguna otra autoridad de control interesada haya presentado objeciones al proyecto de decisión transmitido por la autoridad de control principal en el plazo indicado en los apartados 4 y 5, se considerará que la autoridad de control principal y las autoridades de control interesadas están de acuerdo con dicho proyecto de decisión y estarán vinculadas por este.
7. La autoridad de control principal adoptará y notificará la decisión al establecimiento principal o al establecimiento único del responsable o el encargado del tratamiento, según proceda, e informará de la decisión a las autoridades de control interesadas y al Comité, incluyendo un resumen de los hechos pertinentes y la motivación. La autoridad de control ante la que se haya presentado una reclamación informará de la decisión al reclamante.
8. No obstante lo dispuesto en el apartado 7, cuando se desestime o rechace una reclamación, la autoridad de control ante la que se haya presentado adoptará la decisión, la notificará al reclamante e informará de ello al responsable del tratamiento.
9. En caso de que la autoridad de control principal y las autoridades de control interesadas acuerden desestimar o rechazar determinadas partes de una reclamación y atender otras partes de ella, se adoptará una decisión separada para cada una de esas partes del asunto. La autoridad de control principal adoptará la decisión respecto de la parte referida a acciones en relación con el responsable del tratamiento, la notificará al establecimiento principal o al único establecimiento del responsable o del encargado en el territorio de su Estado miembro, e informará de ello al reclamante, mientras que la autoridad de control del reclamante adoptará la decisión respecto de la parte relativa a la desestimación o rechazo de dicha reclamación, la notificará a dicho reclamante e informará de ello al responsable o al encargado.
10. Tras recibir la notificación de la decisión de la autoridad de control principal con arreglo a los apartados 7 y 9, el responsable o el encargado del tratamiento adoptará las medidas necesarias para garantizar el cumplimiento de la decisión en lo tocante a las actividades de tratamiento en el contexto de todos sus establecimientos en la Unión. El responsable o el encargado notificarán las medidas adoptadas para dar cumplimiento a dicha decisión a la autoridad de control principal, que a su vez informará a las autoridades de control interesadas.
11. En circunstancias excepcionales, cuando una autoridad de control interesada tenga motivos para considerar que es urgente intervenir para proteger los intereses de los interesados, se aplicará el procedimiento de urgencia a que se refiere el artículo 66.

12. La autoridad de control principal y las demás autoridades de control interesadas se facilitarán recíprocamente la información requerida en el marco del presente artículo por medios electrónicos, utilizando un formulario normalizado.

Artículo 61 Asistencia mutua

1. Las autoridades de control se facilitarán información útil y se prestarán asistencia mutua a fin de aplicar el presente Reglamento de manera coherente, y tomarán medidas para asegurar una efectiva cooperación entre ellas. La asistencia mutua abarcará, en particular, las solicitudes de información y las medidas de control, como las solicitudes para llevar a cabo autorizaciones y consultas previas, inspecciones e investigaciones.
2. Cada autoridad de control adoptará todas las medidas oportunas requeridas para responder a una solicitud de otra autoridad de control sin dilación indebida y a más tardar en el plazo de un mes a partir de la solicitud. Dichas medidas podrán incluir, en particular, la transmisión de información pertinente sobre el desarrollo de una investigación.
3. Las solicitudes de asistencia deberán contener toda la información necesaria, entre otras cosas respecto de la finalidad y los motivos de la solicitud. La información que se intercambie se utilizará únicamente para el fin para el que haya sido solicitada.
4. La autoridad de control requerida no podrá negarse a responder a una solicitud, salvo si:
   a) no es competente en relación con el objeto de la solicitud o con las medidas cuya ejecución se solicita, o
   b) el hecho de responder a la solicitud infringiría el presente Reglamento o el Derecho de la Unión o de los Estados miembros que se aplique a la autoridad de control a la que se dirigió la solicitud.
5. La autoridad de control requerida informará a la autoridad de control requirente de los resultados obtenidos o, en su caso, de los progresos registrados o de las medidas adoptadas para responder a su solicitud. La autoridad de control requerida explicará los motivos de su negativa a responder a una solicitud al amparo del apartado 4.
6. Como norma general, las autoridades de control requeridas facilitarán la información solicitada por otras autoridades de control por medios electrónicos, utilizando un formato normalizado.
7. Las autoridades de control requeridas no cobrarán tasa alguna por las medidas adoptadas a raíz de una solicitud de asistencia mutua. Las autoridades de control podrán convenir normas de indemnización recíproca por gastos específicos derivados de la prestación de asistencia mutua en circunstancias excepcionales.
8. Cuando una autoridad de control no facilite la información mencionada en el apartado 5 del presente artículo en el plazo de un mes a partir de la recepción de la solicitud de otra autoridad de control, la autoridad de control requirente podrá adoptar una medida provisional en el territorio de su Estado miembro de conformidad con lo dispuesto en el artículo 55, apartado 1. En ese caso, se supondrá que existe la necesidad urgente contemplada en el artículo 66, apartado 1, que exige una decisión urgente y vinculante del Comité en virtud del artículo 66, apartado 2.
9. La Comisión podrá, mediante actos de ejecución, especificar el formato y los procedimientos de asistencia mutua contemplados en el presente artículo, así como las modalidades del intercambio de información por medios electrónicos entre las autoridades de control y entre las autoridades de control y el Comité, en especial el formato normalizado mencionado en el apartado 6 del presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

Artículo 62 Operaciones conjuntas de las autoridades de control

1. Las autoridades de control realizarán, en su caso, operaciones conjuntas, incluidas investigaciones conjuntas y medidas de ejecución conjuntas, en las que participen miembros o personal de las autoridades de control de otros Estados miembros.
2. Si el responsable o el encargado del tratamiento tiene establecimientos en varios Estados miembros o si es probable que un número significativo de interesados en más de un Estado miembro se vean sustancialmente afectados por las operaciones de tratamiento, una autoridad de control de cada uno de esos Estados miembros tendrá derecho a participar en operaciones conjuntas. La autoridad de control que sea competente en virtud del artículo 56, apartados 1 o 4, invitará a la autoridad de control de cada uno de dichos Estados miembros a participar en las operaciones conjuntas y responderá sin dilación a la solicitud de participación presentada por una autoridad de control.
3. Una autoridad de control podrá, con arreglo al Derecho de su Estado miembro y con la autorización de la autoridad de control de origen, conferir poderes, incluidos poderes de investigación, a los miembros o al personal de la autoridad de control de origen que participen en operaciones conjuntas, o aceptar, en la medida en que lo permita el Derecho del Estado miembro de la autoridad de control de acogida, que los miembros o el personal de la autoridad de control de origen ejerzan sus poderes de investigación de conformidad con el Derecho del Estado miembro de la autoridad de control de origen. Dichos poderes de investigación solo podrán ejercerse bajo la orientación y en presencia de miembros o personal de la autoridad de control de acogida. Los miembros o el personal de la autoridad de control de origen estarán sujetos al Derecho del Estado miembro de la autoridad de control de acogida.
4. Cuando participe, de conformidad con el apartado 1, personal de la autoridad de control de origen en operaciones en otro Estado miembro, el Estado miembro de la autoridad de control de acogida asumirá la responsabilidad de acuerdo con el Derecho del Estado miembro en cuyo territorio se desarrollen las operaciones, por los daños y perjuicios que haya causado dicho personal en el transcurso de las mismas.
5. El Estado miembro en cuyo territorio se causaron los daños y perjuicios asumirá su reparación en las condiciones aplicables a los daños y perjuicios causados por su propio personal. El Estado miembro de la autoridad de control de origen cuyo personal haya causado daños y perjuicios a cualquier persona en el territorio de otro Estado miembro le restituirá íntegramente los importes que este último haya abonado a los derechohabientes.
6. Sin perjuicio del ejercicio de sus derechos frente a terceros y habida cuenta de la excepción establecida en el apartado 5, los Estados miembros renunciarán, en el caso contemplado en el apartado 1, a solicitar de otro Estado miembro el reembolso del importe de los daños y perjuicios mencionados en el apartado 4.
7. Cuando se prevea una operación conjunta y una autoridad de control no cumpla en el plazo de un mes con la obligación establecida en el apartado 2, segunda frase, del presente artículo, las demás autoridades de control podrán adoptar una medida provisional en el territorio de su Estado miembro de conformidad con el artículo 55. En ese caso, se presumirá la existencia de una necesidad urgente a tenor del artículo 66, apartado 1, y se requerirá dictamen o decisión vinculante urgente del Comité en virtud del artículo 66, apartado 2.

Sección 2. Coherencia

Artículo 63 Mecanismo de coherencia

A fin de contribuir a la aplicación coherente del presente Reglamento en toda la Unión, las autoridades de control cooperarán entre sí y, en su caso, con la Comisión, en el marco del mecanismo de coherencia establecido en la presente sección.

Artículo 64 Dictamen del Comité

1. El Comité emitirá un dictamen siempre que una autoridad de control competente proyecte adoptar alguna de las medidas enumeradas a continuación. A tal fin, la autoridad de control competente comunicará el proyecto de decisión al Comité, cuando la decisión:
   a) tenga por objeto adoptar una lista de las operaciones de tratamiento supeditadas al requisito de la evaluación de impacto relativa a la protección de datos de conformidad con el artículo 35, apartado 4;
   b) afecte a un asunto de conformidad con el artículo 40, apartado 7, cuyo objeto sea determinar si un proyecto de código de conducta o una modificación o ampliación de un código de conducta es conforme con el presente Reglamento;
   c) tenga por objeto aprobar los requisitos para la acreditación de un organismo con arreglo al artículo 41, apartado 3, de un organismo de certificación conforme al artículo 43, apartado 3, o los criterios aplicables a la certificación a que se refiere el artículo 42, apartado 5;
   d) tenga por objeto determinar las cláusulas tipo de protección de datos contempladas en el artículo 46, apartado 2, letra d), y el artículo 28, apartado 8;
   e) tenga por objeto autorizar las cláusulas contractuales a que se refiere el artículo 46, apartado 3, letra a);
   f) tenga por objeto la aprobación de normas corporativas vinculantes a tenor del artículo 47.
2. Cualquier autoridad de control, el presidente del Comité o la Comisión podrán solicitar que cualquier asunto de aplicación general o que surta efecto en más de un Estado miembro sea examinado por el Comité a efectos de dictamen, en particular cuando una autoridad de control competente incumpla las obligaciones relativas a la asistencia mutua con arreglo al artículo 61 o las operaciones conjuntas con arreglo al artículo 62.
3. En los casos a que se refieren los apartados 1 y 2, el Comité emitirá dictamen sobre el asunto que le haya sido presentado siempre que no haya emitido ya un dictamen sobre el mismo asunto. Dicho dictamen se adoptará en el plazo de ocho semanas por mayoría simple de los miembros del Comité. Dicho plazo podrá prorrogarse seis semanas más, teniendo en cuenta la complejidad del asunto. Por lo que respecta al proyecto de decisión a que se refiere el apartado 1 y distribuido a los miembros del Comité con arreglo al apartado 5, todo miembro que no haya presentado objeciones dentro de un plazo razonable indicado por el presidente se considerará conforme con el proyecto de decisión.
4. Las autoridades de control y la Comisión comunicarán sin dilación por vía electrónica al Comité, utilizando un formato normalizado, toda información útil, en particular, cuando proceda, un resumen de los hechos, el proyecto de decisión, los motivos por los que es necesaria tal medida, y las opiniones de otras autoridades de control interesadas.
5. La Presidencia del Comité informará sin dilación indebida por medios electrónicos:
   a) a los miembros del Comité y a la Comisión de cualquier información pertinente que le haya sido comunicada, utilizando un formato normalizado. La secretaría del Comité facilitará, de ser necesario, traducciones de la información que sea pertinente, y
   b) a la autoridad de control contemplada, en su caso, en los apartados 1 y 2 y a la Comisión del dictamen, y lo publicará.
6. La autoridad de control competente a que se refiere el apartado 1 no adoptará su proyecto de decisión a tenor del apartado 1 en el plazo mencionado en el apartado 3.
7. La autoridad de control competente a que se refiere el apartado 1 tendrá en cuenta en la mayor medida posible el dictamen del Comité y, en el plazo de dos semanas desde la recepción del dictamen, comunicará por medios electrónicos al presidente del Comité si va a mantener o modificar su proyecto de decisión y, si lo hubiera, el proyecto de decisión modificado, utilizando un formato normalizado.

8. Cuando la autoridad de control competente a que se refiere el apartado 1 informe al presidente del Comité, en el plazo mencionado en el apartado 7 del presente artículo, de que no prevé seguir el dictamen del Comité, en todo o en parte, alegando los motivos correspondientes, se aplicará el artículo 65, apartado 1.

Artículo 65 Resolución de conflictos por el Comité

1. Con el fin de garantizar una aplicación correcta y coherente del presente Reglamento en casos concretos, el Comité adoptará una decisión vinculante en los siguientes casos:
   a) cuando, en un caso mencionado en el artículo 60, apartado 4, una autoridad de control interesada haya manifestado una objeción pertinente y motivada a un proyecto de decisión de la autoridad de control principal y esta no haya seguido la objeción o haya rechazado dicha objeción por no ser pertinente o no estar motivada. La decisión vinculante afectará a todos los asuntos a que se refiera la objeción pertinente y motivada, en particular si hay infracción del presente Reglamento;
   b) cuando haya puntos de vista enfrentados sobre cuál de las autoridades de control interesadas es competente para el establecimiento principal;
   c) cuando una autoridad de control competente no solicite dictamen al Comité en los casos contemplados en el artículo 64, apartado 1, o no siga el dictamen del Comité emitido en virtud del artículo 64. En tal caso, cualquier autoridad de control interesada, o la Comisión, lo pondrá en conocimiento del Comité.
2. La decisión a que se refiere el apartado 1 se adoptará en el plazo de un mes a partir de la remisión del asunto, por mayoría de dos tercios de los miembros del Comité. Este plazo podrá prorrogarse un mes más, habida cuenta de la complejidad del asunto. La decisión que menciona el apartado 1 estará motivada y será dirigida a la autoridad de control principal y a todas las autoridades de control interesadas, y será vinculante para ellas.
3. Cuando el Comité no haya podido adoptar una decisión en los plazos mencionados en el apartado 2, adoptará su decisión en un plazo de dos semanas tras la expiración del segundo mes a que se refiere el apartado 2, por mayoría simple de sus miembros. En caso de empate, decidirá el voto del presidente.
4. Las autoridades de control interesadas no adoptarán decisión alguna sobre el asunto presentado al Comité en virtud del apartado 1 durante los plazos de tiempo a que se refieren los apartados 2 y 3.
5. El presidente del Comité notificará sin dilación indebida la decisión contemplada en el apartado 1 a las autoridades de control interesadas. También informará de ello a la Comisión. La decisión se publicará en el sitio web del Comité sin demora, una vez que la autoridad de control haya notificado la decisión definitiva a que se refiere el apartado 6.
6. La autoridad de control principal o, en su caso, la autoridad de control ante la que se presentó la reclamación adoptará su decisión definitiva sobre la base de la decisión contemplada en el apartado 1 del presente artículo, sin dilación indebida y a más tardar un mes tras la notificación de la decisión del Comité. La autoridad de control principal o, en su caso, la autoridad de control ante la que se presentó la reclamación informará al Comité de la fecha de notificación de su decisión definitiva al responsable o al encargado del tratamiento y al interesado, respectivamente. La decisión definitiva de las autoridades de control interesadas será adoptada en los términos establecidos en el artículo 60, apartados 7, 8 y 9. La decisión definitiva hará referencia a la decisión contemplada en el apartado 1 del presente artículo y especificará que esta última decisión se publicará en el sitio web del Comité con arreglo al apartado 5 del presente artículo. La decisión definitiva llevará adjunta la decisión contemplada en el apartado 1 del presente artículo.

Artículo 66 Procedimiento de urgencia

1. En circunstancias excepcionales, cuando una autoridad de control interesada considere que es urgente intervenir para proteger los derechos y las libertades de interesados, podrá, como excepción al mecanismo de coherencia contemplado en los artículos 63, 64 y 65, o al procedimiento mencionado en el artículo 60, adoptar inmediatamente medidas provisionales destinadas a producir efectos jurídicos en su propio territorio, con un periodo de validez determinado que no podrá ser superior a tres meses. La autoridad de control comunicará sin dilación dichas medidas, junto con los motivos de su adopción, a las demás autoridades de control interesadas, al Comité y a la Comisión.
2. Cuando una autoridad de control haya adoptado una medida de conformidad con el apartado 1, y considere que deben adoptarse urgentemente medidas definitivas, podrá solicitar con carácter urgente un dictamen o una decisión vinculante urgente del Comité, motivando dicha solicitud de dictamen o decisión.
3. Cualquier autoridad de control podrá solicitar, motivando su solicitud, y, en particular, la urgencia de la intervención, un dictamen urgente o una decisión vinculante urgente, según el caso, del Comité, cuando una autoridad de control competente no haya tomado una medida apropiada en una situación en la que sea urgente intervenir a fin de proteger los derechos y las libertades de los interesados.
4. No obstante lo dispuesto en el artículo 64, apartado 3, y en el artículo 65, apartado 2, los dictámenes urgentes o decisiones vinculantes urgentes contemplados en los apartados 2 y 3 del presente artículo se adoptarán en el plazo de dos semanas por mayoría simple de los miembros del Comité.

Artículo 67 Intercambio de información

La Comisión podrá adoptar actos de ejecución de ámbito general para especificar las modalidades de intercambio de información por medios electrónicos entre las autoridades de control, y entre dichas autoridades y el Comité, en especial el formato normalizado contemplado en el artículo 64.

Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

Sección 3. Comité europeo de protección de datos

Artículo 68 Comité Europeo de Protección de Datos

1. Se crea el Comité Europeo de Protección de Datos («Comité»), como organismo de la Unión, que gozará de personalidad jurídica.
2. El Comité estará representado por su presidente.
3. El Comité estará compuesto por el director de una autoridad de control de cada Estado miembro y por el Supervisor Europeo de Protección de Datos o sus representantes respectivos.
4. Cuando en un Estado miembro estén encargados de controlar la aplicación de las disposiciones del presente Reglamento varias autoridades de control, se nombrará a un representante común de conformidad con el Derecho de ese Estado miembro.
5. La Comisión tendrá derecho a participar en las actividades y reuniones del Comité, sin derecho a voto. La Comisión designará un representante. El presidente del Comité comunicará a la Comisión las actividades del Comité.
6. En los casos a que se refiere el artículo 65, el Supervisor Europeo de Protección de Datos sólo tendrá derecho a voto en las decisiones relativas a los principios y normas aplicables a las instituciones, órganos y organismos de la Unión que correspondan en cuanto al fondo a las contempladas en el presente Reglamento.

Artículo 69 Independencia

1. El Comité actuará con total independencia en el desempeño de sus funciones o el ejercicio de sus competencias con arreglo a los artículos 70 y 71.
2. Sin perjuicio de las solicitudes de la Comisión contempladas en el artículo 70, apartados 1 y 2, el Comité no solicitará ni admitirá instrucciones de nadie en el desempeño de sus funciones o el ejercicio de sus competencias.

Artículo 70 Funciones del Comité

1. El Comité garantizará la aplicación coherente del presente Reglamento. A tal efecto, el Comité, a iniciativa propia o, en su caso, a instancia de la Comisión, en particular:
   a) supervisará y garantizará la correcta aplicación del presente Reglamento en los casos contemplados en los artículos 64 y 65, sin perjuicio de las funciones de las autoridades de control nacionales;
   b) asesorará a la Comisión sobre toda cuestión relativa a la protección de datos personales en la Unión, en particular sobre cualquier propuesta de modificación del presente Reglamento;
   c) asesorará a la Comisión sobre el formato y los procedimientos para intercambiar información entre los responsables, los encargados y las autoridades de control en relación con las normas corporativas vinculantes;
   d) emitirá directrices, recomendaciones y buenas prácticas relativas a los procedimientos para la supresión de vínculos, copias o réplicas de los datos personales procedentes de servicios de comunicación a disposición pública a que se refiere el artículo 17, apartado 2;
   e) examinará, a iniciativa propia, a instancia de uno de sus miembros o de la Comisión, cualquier cuestión relativa a la aplicación del presente Reglamento, y emitirá directrices, recomendaciones y buenas prácticas a fin de promover la aplicación coherente del presente Reglamento;
   f) emitirá directrices, recomendaciones y buenas prácticas de conformidad con la letra e) del presente apartado a fin de especificar más los criterios y requisitos de las decisiones basadas en perfiles en virtud del artículo 22, apartado 2;
   g) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado a fin de constatar las violaciones de la seguridad de los datos y determinar la dilación indebida a tenor del artículo 33, apartados 1 y 2, y con respecto a las circunstancias particulares en las que el responsable o el encargado del tratamiento debe notificar la violación de la seguridad de los datos personales;
   h) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado con respecto a las circunstancias en las que sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas a tenor del artículo 34, apartado 1;
   i) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado con el fin de especificar en mayor medida los criterios y requisitos para las transferencias de datos personales basadas en normas corporativas vinculantes a las que se hayan adherido los responsables del tratamiento y en normas corporativas vinculantes a las que se hayan adherido los encargados del tratamiento y en requisitos adicionales necesarios para garantizar la protección de los datos personales de los interesados a que se refiere el artículo 47;
   j) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado a fin de especificar en mayor medida los criterios y requisitos de las transferencias de datos personales sobre la base del artículo 49, apartado 1;
   k) formulará directrices para las autoridades de control, relativas a la aplicación de las medidas a que se refiere el artículo 58, apartados 1, 2 y 3, y la fijación de multas administrativas de conformidad con el artículo 83;
   l) examinará la aplicación práctica de las directrices, recomendaciones y buenas prácticas;

m) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado a fin de establecer procedimientos comunes de información procedente de personas físicas sobre infracciones del presente Reglamento en virtud del artículo 54, apartado 2;

n) alentará la elaboración de códigos de conducta y el establecimiento de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos de conformidad con los artículos 40 y 42;

o) aprobará los criterios de certificación en virtud del artículo 42, apartado 5, y llevará un registro público de los mecanismos de certificación y sellos y marcas de protección de datos en virtud del artículo 42, apartado 8, y de los responsables o los encargados del tratamiento certificados establecidos en terceros países en virtud del artículo 42, apartado 7;

p) aprobará los requisitos contemplados en el artículo 43, apartado 3, con miras a la acreditación de los organismos de certificación a los que se refiere el artículo 43;

q) facilitará a la Comisión un dictamen sobre los requisitos de certificación contemplados en el artículo 43, apartado 8;

r) facilitará a la Comisión un dictamen sobre los iconos a que se refiere el artículo 12, apartado 7;

s) facilitará a la Comisión un dictamen para evaluar la adecuación del nivel de protección en un tercer país u organización internacional, en particular para evaluar si un tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o una organización internacional, ya no garantizan un nivel de protección adecuado. A tal fin, la Comisión facilitará al Comité toda la documentación necesaria, incluida la correspondencia con el gobierno del tercer país, que se refiera a dicho tercer país, territorio o específico o a dicha organización internacional;

t) emitirá dictámenes sobre los proyectos de decisión de las autoridades de control en virtud del mecanismo de coherencia mencionado en el artículo 64, apartado 1, sobre los asuntos presentados en virtud del artículo 64, apartado 2, y sobre las decisiones vinculantes en virtud del artículo 65, incluidos los casos mencionados en el artículo 66;

u) promoverá la cooperación y los intercambios bilaterales y multilaterales efectivos de información y de buenas prácticas entre las autoridades de control;

v) promoverá programas de formación comunes y facilitará intercambios de personal entre las autoridades de control y, cuando proceda, con las autoridades de control de terceros países o con organizaciones internacionales;

w) promoverá el intercambio de conocimientos y documentación sobre legislación y prácticas en materia de protección de datos con las autoridades de control encargadas de la protección de datos a escala mundial;

x) emitirá dictámenes sobre los códigos de conducta elaborados a escala de la Unión de conformidad con el artículo 40, apartado 9, y

y) llevará un registro electrónico, de acceso público, de las decisiones adoptadas por las autoridades de control y los tribunales sobre los asuntos tratados en el marco del mecanismo de coherencia.

2. Cuando la Comisión solicite asesoramiento del Comité podrá señalar un plazo teniendo en cuenta la urgencia del asunto.

3. El Comité transmitirá sus dictámenes, directrices, recomendaciones y buenas prácticas a la Comisión y al Comité contemplado en el artículo 93, y los hará públicos.

4. Cuando proceda, el Comité consultará a las partes interesadas y les dará la oportunidad de presentar sus comentarios en un plazo razonable. Sin perjuicio de lo dispuesto en el artículo 76, el Comité publicará los resultados del procedimiento de consulta.

Artículo 71 Informes

1. El Comité elaborará un informe anual en materia de protección de las personas físicas en lo que respecta al tratamiento en la Unión y, si procede, en terceros países y organizaciones internacionales. El informe se hará público y se transmitirá al Parlamento Europeo, al Consejo y a la Comisión.
2. El informe anual incluirá un examen de la aplicación práctica de las directrices, recomendaciones y buenas prácticas indicadas en el artículo 70, apartado 1, letra l), así como de las decisiones vinculantes indicadas en el artículo 65.

Artículo 72 Procedimiento

1. El Comité tomará sus decisiones por mayoría simple de sus miembros, salvo que el presente Reglamento disponga otra cosa.
2. El Comité adoptará su reglamento interno por mayoría de dos tercios de sus miembros y organizará sus disposiciones de funcionamiento.

Artículo 73 Presidencia

1. El Comité elegirá por mayoría simple de entre sus miembros un presidente y dos vicepresidentes.
2. El mandato del presidente y de los vicepresidentes será de cinco años de duración y podrá renovarse una vez.

Artículo 74 Funciones del presidente

1. El presidente desempeñará las siguientes funciones:
   a) convocar las reuniones del Comité y preparar su orden del día;
   b) notificar las decisiones adoptadas por el Comité con arreglo al artículo 65 a la autoridad de control principal y a las autoridades de control interesadas;
   c) garantizar el ejercicio puntual de las funciones del Comité, en particular en relación con el mecanismo de coherencia a que se refiere el artículo 63.
2. El Comité determinará la distribución de funciones entre el presidente y los vicepresidentes en su reglamento interno.

Artículo 75 Secretaría

1. El Comité contará con una secretaría, de la que se hará cargo el Supervisor Europeo de Protección de Datos.
2. La secretaría ejercerá sus funciones siguiendo exclusivamente las instrucciones del presidente del Comité.
3. El personal del Supervisor Europeo de Protección de Datos que participe en el desempeño de las funciones conferidas al Comité por el presente Reglamento dependerá de un superior jerárquico distinto del personal que desempeñe las funciones conferidas al Supervisor Europeo de Protección de Datos.
4. El Comité, en consulta con el Supervisor Europeo de Protección de Datos, elaborará y publicará, si procede, un memorando de entendimiento para la puesta en práctica del presente artículo, que determinará los términos de su cooperación y que será aplicable al personal del Supervisor Europeo de Protección de Datos que participe en el desempeño de las funciones conferidas al Comité por el presente Reglamento.
5. La secretaría prestará apoyo analítico, administrativo y logístico al Comité.
6. La secretaría será responsable, en particular, de:
   a) los asuntos corrientes del Comité;
   b) la comunicación entre los miembros del Comité, su presidente y la Comisión;

c) la comunicación con otras instituciones y con el público;

d) la utilización de medios electrónicos para la comunicación interna y externa;

e) la traducción de la información pertinente;

f) la preparación y el seguimiento de las reuniones del Comité;

g) la preparación, redacción y publicación de dictámenes, decisiones relativas a solución de diferencias entre autoridades de control y otros textos adoptados por el Comité.

Artículo 76 Confidencialidad

1. Los debates del Comité serán confidenciales cuando el mismo lo considere necesario, tal como establezca su reglamento interno.
2. El acceso a los documentos presentados a los miembros del Comité, los expertos y los representantes de terceras partes se regirá por el Reglamento (CE) n.o 1049/2001 del Parlamento Europeo y del Consejo.

CAPÍTULO VIII. Recursos, responsabilidad y sanciones

Artículo 77 Derecho a presentar una reclamación ante una autoridad de control

1. Sin perjuicio de cualquier otro recurso administrativo o acción judicial, todo interesado tendrá derecho a presentar una reclamación ante una autoridad de control, en particular en el Estado miembro en el que tenga su residencia habitual, lugar de trabajo o lugar de la supuesta infracción, si considera que el tratamiento de datos personales que le conciernen infringe el presente Reglamento.
2. La autoridad de control ante la que se haya presentado la reclamación informará al reclamante sobre el curso y el resultado de la reclamación, inclusive sobre la posibilidad de acceder a la tutela judicial en virtud del artículo 78.

Artículo 78 Derecho a la tutela judicial efectiva contra una autoridad de control

1. Sin perjuicio de cualquier otro recurso administrativo o extrajudicial, toda persona física o jurídica tendrá derecho a la tutela judicial efectiva contra una decisión jurídicamente vinculante de una autoridad de control que le concierna.
2. Sin perjuicio de cualquier otro recurso administrativo o extrajudicial, todo interesado tendrá derecho a la tutela judicial efectiva en caso de que la autoridad de control que sea competente en virtud de los artículos 55 y 56 no dé curso a una reclamación o no informe al interesado en el plazo de tres meses sobre el curso o el resultado de la reclamación presentada en virtud del artículo 77.
3. Las acciones contra una autoridad de control deberán ejercitarse ante los tribunales del Estado miembro en que esté establecida la autoridad de control.
4. Cuando se ejerciten acciones contra una decisión de una autoridad de control que haya sido precedida de un dictamen o una decisión del Comité en el marco del mecanismo de coherencia, la autoridad de control remitirá al tribunal dicho dictamen o decisión.

Artículo 79 Derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento

1. Sin perjuicio de los recursos administrativos o extrajudiciales disponibles, incluido el derecho a presentar una reclamación ante una autoridad de control en virtud del artículo 77, todo interesado tendrá derecho a la tutela judicial efectiva cuando considere que sus derechos en virtud del presente Reglamento han sido vulnerados como consecuencia de un tratamiento de sus datos personales.

2. Las acciones contra un responsable o encargado del tratamiento deberán ejercitarse ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento. Alternativamente, tales acciones podrán ejercitarse ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual, a menos que el responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos.

Artículo 80 Representación de los interesados

1. El interesado tendrá derecho a dar mandato a una entidad, organización o asociación sin ánimo de lucro que haya sido correctamente constituida con arreglo al Derecho de un Estado miembro, cuyos objetivos estatutarios sean de interés público y que actúe en el ámbito de la protección de los derechos y libertades de los interesados en materia de protección de sus datos personales, para que presente en su nombre la reclamación, y ejerza en su nombre los derechos contemplados en los artículos 77, 78 y 79, y el derecho a ser indemnizado mencionado en el artículo 82 si así lo establece el Derecho del Estado miembro.
2. Cualquier Estado miembro podrán disponer que cualquier entidad, organización o asociación mencionada en el apartado 1 del presente artículo tenga, con independencia del mandato del interesado, derecho a presentar en ese Estado miembro una reclamación ante la autoridad de control que sea competente en virtud del artículo 77 y a ejercer los derechos contemplados en los artículos 78 y 79, si considera que los derechos del interesado con arreglo al presente Reglamento han sido vulnerados como consecuencia de un tratamiento.

Artículo 81 Suspensión de los procedimientos

1. Cuando un tribunal competente de un Estado miembro tenga información de la pendencia ante un tribunal de otro Estado miembro de un procedimiento relativo a un mismo asunto en relación con el tratamiento por el mismo responsable o encargado, se pondrá en contacto con dicho tribunal de otro Estado miembro para confirmar la existencia de dicho procedimiento.
2. Cuando un procedimiento relativo a un mismo asunto en relación con el tratamiento por el mismo responsable o encargado esté pendiente ante un tribunal de otro Estado miembro, cualquier tribunal competente distinto de aquel ante el que se ejercitó la acción en primer lugar podrá suspender su procedimiento.
3. Cuando dicho procedimiento esté pendiente en primera instancia, cualquier tribunal distinto de aquel ante el que se ejercitó la acción en primer lugar podrá también, a instancia de una de las partes, inhibirse en caso de que el primer tribunal sea competente para su conocimiento y su acumulación sea conforme a Derecho.

Artículo 82 Derecho a indemnización y responsabilidad

1. Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.
2. Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el presente Reglamento. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del presente Reglamento dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable.
3. El responsable o encargado del tratamiento estará exento de responsabilidad en virtud del apartado 2 si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios.
4. Cuando más de un responsable o encargado del tratamiento, o un responsable y un encargado hayan participado en la misma operación de tratamiento y sean, con arreglo a los apartados 2 y

3, responsables de cualquier daño o perjuicio causado por dicho tratamiento, cada responsable o encargado será considerado responsable de todos los daños y perjuicios, a fin de garantizar la indemnización efectiva del interesado.

5. Cuando, de conformidad con el apartado 4, un responsable o encargado del tratamiento haya pagado una indemnización total por el perjuicio ocasionado, dicho responsable o encargado tendrá derecho a reclamar a los demás responsables o encargados que hayan participado en esa misma operación de tratamiento la parte de la indemnización correspondiente a su parte de responsabilidad por los daños y perjuicios causados, de conformidad con las condiciones fijadas en el apartado 2.
6. Las acciones judiciales en ejercicio del derecho a indemnización se presentarán ante los tribunales competentes con arreglo al Derecho del Estado miembro que se indica en el artículo 79, apartado 2.

Artículo 83 Condiciones generales para la imposición de multas administrativas

1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.
2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:
   a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;
   b) la intencionalidad o negligencia en la infracción;
   c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;
   d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;
   e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;
   f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;
   g) las categorías de los datos de carácter personal afectados por la infracción;
   h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;
   i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;
   j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y
   k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.
3. Si un responsable o un encargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones del presente Reglamento, la cuantía total de la multa administrativa no será superior a la cuantía prevista para las infracciones más graves.
4. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de

una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;

b) las obligaciones de los organismos de certificación a tenor de los artículos 42 y 43;

c) las obligaciones de la autoridad de control a tenor del artículo 41, apartado 4.

5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;

b) los derechos de los interesados a tenor de los artículos 12 a 22;

c) las transferencias de datos personales a un destinatario en un tercer país o una organización internacional a tenor de los artículos 44 a 49;

d) toda obligación en virtud del Derecho de los Estados miembros que se adopte con arreglo al capítulo IX;

e) el incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control con arreglo al artículo 58, apartado 2, o el no facilitar acceso en incumplimiento del artículo 58, apartado 1.

6. El incumplimiento de las resoluciones de la autoridad de control a tenor del artículo 58, apartado 2, se sancionará de acuerdo con el apartado 2 del presente artículo con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

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

8. El ejercicio por una autoridad de control de sus poderes en virtud del presente artículo estará sujeto a garantías procesales adecuadas de conformidad con el Derecho de la Unión y de los Estados miembros, entre ellas la tutela judicial efectiva y el respeto de las garantías procesales.

9. Cuando el ordenamiento jurídico de un Estado miembro no establezca multas administrativas, el presente artículo podrá aplicarse de tal modo que la incoación de la multa corresponda a la autoridad de control competente y su imposición a los tribunales nacionales competentes, garantizando al mismo tiempo que estas vías de derecho sean efectivas y tengan un efecto equivalente a las multas administrativas impuestas por las autoridades de control. En cualquier caso, las multas impuestas serán efectivas, proporcionadas y disuasorias. Los Estados miembros de que se trate notificarán a la Comisión las disposiciones legislativas que adopten en virtud del presente apartado a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier ley de modificación o modificación posterior que les sea aplicable.

Artículo 84 Sanciones

1. Los Estados miembros establecerán las normas en materia de otras sanciones aplicables a las infracciones del presente Reglamento, en particular las infracciones que no se sancionen con multas administrativas de conformidad con el artículo 83, y adoptarán todas las medidas necesarias para garantizar su observancia. Dichas sanciones serán efectivas, proporcionadas y disuasorias.

2. Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior que les sea aplicable.

CAPÍTULO IX. Disposiciones relativas a situaciones específicas de tratamiento

Artículo 85 Tratamiento y libertad de expresión y de información

1. Los Estados miembros conciliarán por ley el derecho a la protección de los datos personales en virtud del presente Reglamento con el derecho a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria.
2. Para el tratamiento realizado con fines periodísticos o con fines de expresión académica, artística o literaria, los Estados miembros establecerán exenciones o excepciones de lo dispuesto en los capítulos II (principios), III (derechos del interesado), IV (responsable y encargado del tratamiento), V (transferencia de datos personales a terceros países u organizaciones internacionales), VI (autoridades de control independientes), VII (cooperación y coherencia) y IX (disposiciones relativas a situaciones específicas de tratamiento de datos), si son necesarias para conciliar el derecho a la protección de los datos personales con la libertad de expresión e información.
3. Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 2 y, sin dilación, cualquier modificación posterior, legislativa u otra, de las mismas.

Artículo 86 Tratamiento y acceso del público a documentos oficiales

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

Artículo 87 Tratamiento del número nacional de identificación

Los Estados miembros podrán determinar adicionalmente las condiciones específicas para el tratamiento de un número nacional de identificación o cualquier otro medio de identificación de carácter general. En ese caso, el número nacional de identificación o cualquier otro medio de identificación de carácter general se utilizará únicamente con las garantías adecuadas para los derechos y las libertades del interesado con arreglo al presente Reglamento.

Artículo 88 Tratamiento en el ámbito laboral

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

Artículo 89 Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos

1. El tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo.
2. Cuando se traten datos personales con fines de investigación científica o histórica o estadísticos el Derecho de la Unión o de los Estados miembros podrá establecer excepciones a los derechos contemplados en los artículos 15, 16, 18 y 21, sujetas a las condiciones y garantías indicadas en el apartado 1 del presente artículo, siempre que sea probable que esos derechos imposibiliten u obstaculicen gravemente el logro de los fines científicos y cuanto esas excepciones sean necesarias para alcanzar esos fines.
3. Cuando se traten datos personales con fines de archivo en interés público, el Derecho de le Unión o de los Estados miembros podrá prever excepciones a los derechos contemplados en los artículos 15, 16, 18, 19, 20 y 21, sujetas a las condiciones y garantías citadas en el apartado 1 del presente artículo, siempre que esos derechos puedan imposibilitar u obstaculizar gravemente el logro de los fines científicos y cuanto esas excepciones sean necesarias para alcanzar esos fines.
4. En caso de que el tratamiento a que hacen referencia los apartados 2 y 3 sirva también al mismo tiempo a otro fin, las excepciones solo serán aplicables al tratamiento para los fines mencionados en dichos apartados.

Artículo 90 Obligaciones de secreto

1. Los Estados miembros podrán adoptar normas específicas para fijar los poderes de las autoridades de control establecidos en el artículo 58, apartado 1, letras e) y f), en relación con los responsables o encargados sujetos, con arreglo al Derecho de la Unión o de los Estados miembros o a las normas establecidas por los organismos nacionales competentes, a una obligación de secreto profesional o a otras obligaciones de secreto equivalentes, cuando sea necesario y proporcionado para conciliar el derecho a la protección de los datos personales con la obligación de secreto. Esas normas solo se aplicarán a los datos personales que el responsable o el encargado del tratamiento hayan recibido como resultado o con ocasión de una actividad cubierta por la citada obligación de secreto.
2. Cada Estado miembro notificará a la Comisión las normas adoptadas de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior de las mismas.

Artículo 91 Normas vigentes sobre protección de datos de las iglesias y asociaciones religiosas

1. Cuando en un Estado miembro iglesias, asociaciones o comunidades religiosas apliquen, en el momento de la entrada en vigor del presente Reglamento, un conjunto de normas relativas a la protección de las personas físicas en lo que respecta al tratamiento, tales normas podrán seguir aplicándose, siempre que sean conformes con el presente Reglamento.
2. Las iglesias y las asociaciones religiosas que apliquen normas generales de conformidad con el apartado 1 del presente artículo estarán sujetas al control de una autoridad de control independiente, que podrá ser específica, siempre que cumpla las condiciones establecidas en el capítulo VI del presente Reglamento.

CAPÍTULO X. Actos delegados y actos de ejecución

Artículo 92 Ejercicio de la delegación

1. Los poderes para adoptar actos delegados otorgados a la Comisión estarán sujetos a las condiciones establecidas en el presente artículo.
2. La delegación de poderes indicada en el artículo 12, apartado 8, y en el artículo 43, apartado 8, se otorgarán a la Comisión por tiempo indefinido a partir del 24 de mayo de 2016.
3. La delegación de poderes mencionada en el artículo 12, apartado 8, y el artículo 43, apartado 8, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto al día siguiente de su publicación en el Diario Oficial de la Unión Europea o en una fecha posterior indicada en la misma. No afectará a la validez de los actos delegados que ya estén en vigor.
4. Tan pronto como la Comisión adopte un acto delegado lo notificará simultáneamente al Parlamento Europeo y al Consejo.
5. Los actos delegados adoptados en virtud del artículo 12, apartado 8, y el artículo 43, apartado 8, entrarán en vigor únicamente si, en un plazo de tres meses desde su notificación al Parlamento Europeo y al Consejo, ni el Parlamento Europeo ni el Consejo formulan objeciones o si, antes del vencimiento de dicho plazo, tanto el uno como el otro informan a la Comisión de que no las formularán. El plazo se ampliará en tres meses a iniciativa del Parlamento Europeo o del Consejo.

Artículo 93 Procedimiento de comité

1. La Comisión estará asistida por un comité. Dicho comité será un comité en el sentido del Reglamento (UE) n.o 182/2011.
2. Cuando se haga referencia al presente apartado, se aplicará el artículo 5 del Reglamento (UE) n.o 182/2011.
3. Cuando se haga referencia al presente apartado, se aplicará el artículo 8 del Reglamento (UE) n.o 182/2011, en relación con su artículo 5.

CAPÍTULO XI. Disposiciones finales

Artículo 94 Derogación de la Directiva 95/46/CE

1. Queda derogada la Directiva 95/46/CE con efecto a partir del 25 de mayo de 2018.
2. Toda referencia a la Directiva derogada se entenderá hecha al presente Reglamento. Toda referencia al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales establecido por el artículo 29 de la Directiva 95/46/CE se entenderá hecha al Comité Europeo de Protección de Datos establecido por el presente Reglamento.

Artículo 95 Relación con la Directiva 2002/58/CE

El presente Reglamento no impondrá obligaciones adicionales a las personas físicas o jurídicas en materia de tratamiento en el marco de la prestación de servicios públicos de comunicaciones electrónicas en redes públicas de comunicación de la Unión en ámbitos en los que estén sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE.

Artículo 96 Relación con acuerdos celebrados anteriormente

Los acuerdos internacionales que impliquen la transferencia de datos personales a terceros países u organizaciones internacionales que hubieren sido celebrados por los Estados miembros antes del 24 de mayo de 2016 y que cumplan lo dispuesto en el Derecho de la Unión aplicable antes de dicha fecha, seguirán en vigor hasta que sean modificados, sustituidos o revocados.

Artículo 97 Informes de la Comisión

1. A más tardar el 25 de mayo de 2020 y posteriormente cada cuatro años, la Comisión presentará al Parlamento Europeo y al Consejo un informe sobre la evaluación y revisión del presente Reglamento. Los informes se harán públicos.
2. En el marco de las evaluaciones y revisiones a que se refiere el apartado 1, la Comisión examinará en particular la aplicación y el funcionamiento de:
   a) el capítulo V sobre la transferencia de datos personales a países terceros u organizaciones internacionales, particularmente respecto de las decisiones adoptadas en virtud del artículo 45, apartado 3, del presente Reglamento, y de las adoptadas sobre la base del artículo 25, apartado 6, de la Directiva 95/46/CE;
   b) el capítulo VII sobre cooperación y coherencia.
3. A los efectos del apartado 1, la Comisión podrá solicitar información a los Estados miembros y a las autoridades de control.
4. Al llevar a cabo las evaluaciones y revisiones indicadas en los apartados 1 y 2, la Comisión tendrá en cuenta las posiciones y conclusiones del Parlamento Europeo, el Consejo y los demás órganos o fuentes pertinentes.
5. La Comisión presentará, en caso necesario, las propuestas oportunas para modificar el presente Reglamento, en particular teniendo en cuenta la evolución de las tecnologías de la información y a la vista de los progresos en la sociedad de la información.

Artículo 98 Revisión de otros actos jurídicos de la Unión en materia de protección de datos

La Comisión presentará, si procede, propuestas legislativas para modificar otros actos jurídicos de la Unión en materia de protección de datos personales, a fin de garantizar la protección uniforme y coherente de las personas físicas en relación con el tratamiento. Se tratará en particular de las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento por parte de las instituciones, órganos, y organismos de la Unión y a la libre circulación de tales datos.

Artículo 99 Entrada en vigor y aplicación

1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea.
2. Será aplicable a partir del 25 de mayo de 2018.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el 27 de abril de 2016.

3 PROTECCIÓN DE DATOS Y ADMINISTRACIÓN LOCAL

Guía Sectorial AEPD

El 4 de diciembre de 2017 se firmó un Protocolo General de Actuación entre la AEPD y la FEMP como marco de la colaboración que ambas entidades venimos manteniendo para lograr la máxima difusión posible de los principios del Reglamento General de Protección de Datos (RGPD) y de las herramientas, guías y publicaciones que puedan ayudar a las entidades locales en su proceso de adaptación a las previsiones del RGPD, que será plenamente aplicable el próximo 25 de mayo.

Conscientes de la gran tarea que hemos de realizar en este ámbito, hemos venido desarrollando diferentes iniciativas como la organización de jornadas formativas e informativas dirigidas a representantes de entidades locales, la colaboración de la AEPD en el Grupo de Trabajo para la implantación del nuevo Reglamento Europeo constituido en el seno de la FEMP, el intercambio de documentos e información, la colaboración en la difusión de herramientas, guías y publicaciones, etc…

Con esta finalidad divulgativa se presenta la Guía de Protección de Datos y Administración Local, en la que la AEPD ha recogido aportaciones realizadas por el mencionado Grupo de Trabajo, y a la que se acompaña el estudio realizado por la FEMP sobre el proceso de adaptación de las entidades locales al RGPD sobre la base de una encuesta realizada a Diputaciones Provinciales, Cabildos y Consejos Insulares, que da buena muestra del punto de partida del que parten las entidades locales en esta materia.

Confiamos en que todo ello sirva a la finalidad esencial que orienta el trabajo de ambas entidades, que no es otra que la de prestar apoyo y facilitar a las entidades locales el proceso de adaptación y cumplimiento de la nueva normativa de protección de datos.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

FEDERACIÓN ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

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

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.

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

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.

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

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.	....

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.

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.

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

· 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.

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

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.

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

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.

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

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.

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

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.

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

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.

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

· **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.

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

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.

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

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.

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

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.

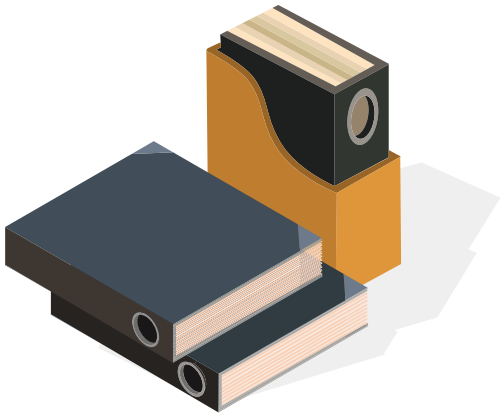
b) Emitir informe, a solicitud de la Administración Pública correspondiente, sobre el traslado total o parcial de las instalaciones e implantación o revisión de sus sistemas de organización y métodos de trabajo.

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.

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

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.

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.*

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

PROTECCIÓN DE DATOS Y ADMINISTRACIÓN LOCAL

GUÍAS SECTORIALES AEPD

Con la colaboración de:

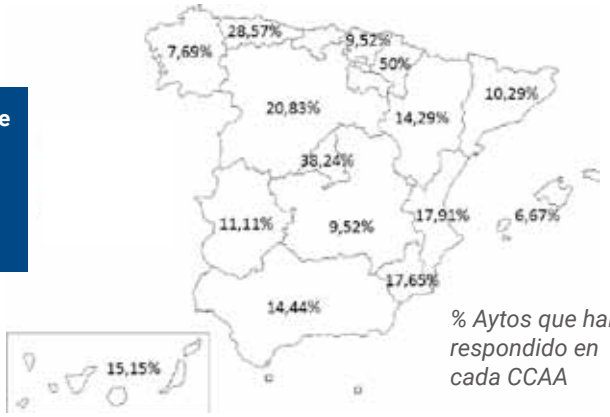
4 DECÁLOGO DE INCUMPLIMIENTOS MÁS FRECUENTES EN LA AA.LL.

ADAPTACIÓN DE LAS EELL AL RGPD: AYUNTAMIENTOS

5

Estudio realizado en Octubre de 2017

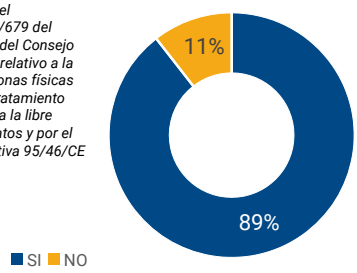
Resultados en Ayuntamientos de más de 20.000 habitantes

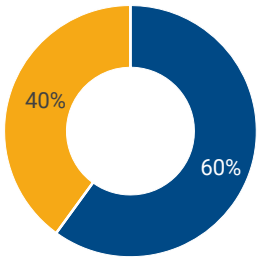


% Aytos que han respondido en cada CCAA

CCAA	Respuestas	Total EELL	Habitantes	% sobre total aytos.
ANDALUCÍA	13	90	5.732.875	14,44
ARAGÓN	1	7	769.145	14,29
ASTURIAS	2	7	729.402	28,57
CANARIAS	5	33	1.659.910	15,15
CANTABRIA	0	5	312.561	0
CASTILLA LA MANCHA	2	21	864.159	9,52
CASTILLA LEÓN	5	24	1.251.420	20,83
CATALUÑA	7	68	5.316.188	10,29
CEUTA	0	1	84.519	0
EXTREMADURA	1	9	443.107	11,11
GALICIA	2	26	1.418.491	7,69
ILLES BALEARS	1	15	787.545	6,67
LA RIOJA	0	2	174.703	0
MADRID	13	34	5.868.028	38,24
MELILLA	0	1	86.026	0
MURCIA	3	17	1.208.497	17,65
NAVARRA	2	4	271.191	50
PAÍS VASCO	2	21	1.402.557	9,52
VALENCIA	12	67	3.598.607	17,91
TOTAL	71	452	31.978.931	15,71

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

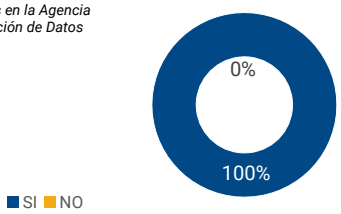




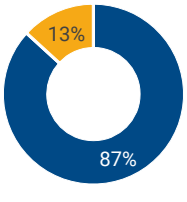
Conoce las implicaciones y cambios que el RGPD establece frente a la actual normativa Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD) y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD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

Dispone el Ayuntamiento de algunas de las siguientes medidas:

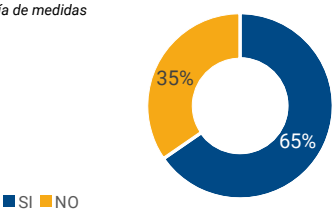
Ficheros declarados en la Agencia Española de Protección de Datos



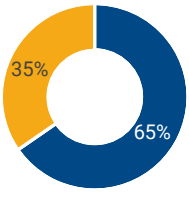
Documento de seguridad



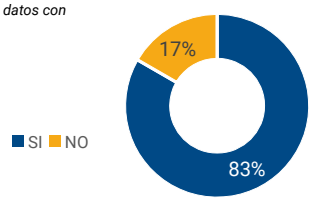
Informes de auditoría de medidas de seguridad



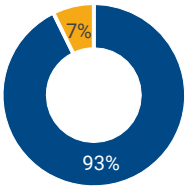
Responsable de seguridad



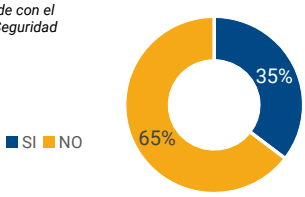
Contratos de acceso a datos con terceros



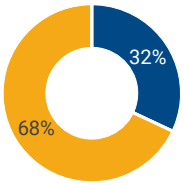
Textos informativos de protección de datos en los formularios de recogida de datos disponibles para los ciudadanos



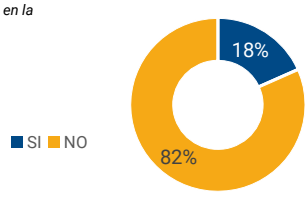
Plan de seguridad acorde con el Esquema Nacional de Seguridad



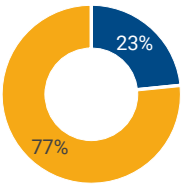
Análisis de riesgos en protección de datos



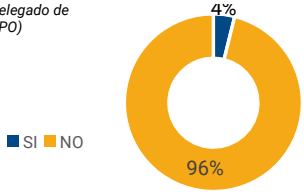
Evaluación de impacto en la protección de datos



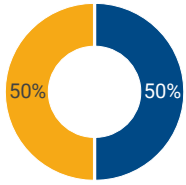
Creación del Registro de las Actividades en relación con los tratamientos de datos de su responsabilidad



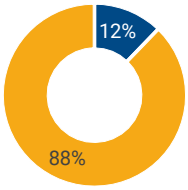
Nombramiento de un Delegado de Protección de Datos (DPO)



Información y transparencia del tratamiento

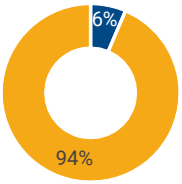


Sustitución de los contratos de acceso a datos por contratos de encargo de tratamiento



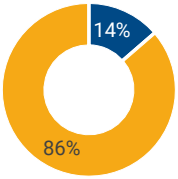
SI NO

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



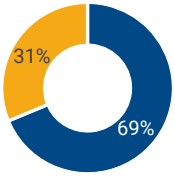
SI NO

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



SI NO

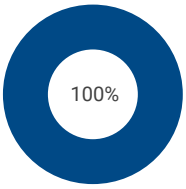
Protocolo para garantizar los derechos de acceso, rectificación, cancelación y oposición



SI NO

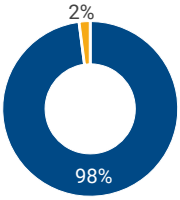
Gestiona el Ayuntamiento alguno de los siguientes recursos, procesos o funciones:

Padrón municipal / Gestión obras públicas, pavimentación vías, urbanismo y vivienda / Actividades culturales y deportivas / Gestión económica del Ayuntamiento / Nóminas de sus empleados públicos / Licencias Servicios sociales y reinserción social / Desarrollo local y promoción empresarial / Nómina / Bolsa de trabajo / Empresas colaboradoras y proveedoras.



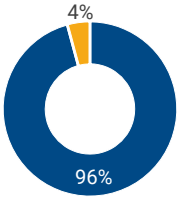
SI NO

Recursos propios de carácter tributario Tráfico vehículos y personas Seguridad en lugares públicos



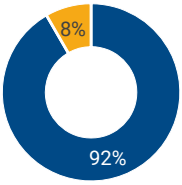
SI NO

Abastos, mataderos, ferias, mercados, defensa de usuarios y consumidores



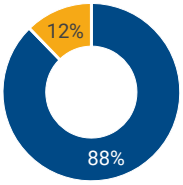
SI NO

Protección civil



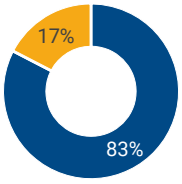
SI NO

Recogida residuos y limpieza diaria / Protección de medioambiente / Cementerios y servicios funerarios



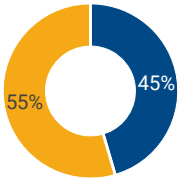
SI NO

Centro de Acceso Público a Internet



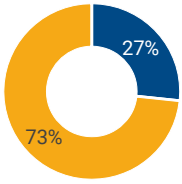
SI NO

Protección y extinción de incendios



SI NO

Atención primaria de la salud



SI NO

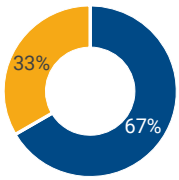
6 ADAPTACIÓN DE LAS EELL AL RGPD: ORGANISMOS SUPRAMUNICIPALES

Estudio realizado en Octubre de 2017

Resultados en Diputaciones Provinciales, Cabildos y Consejos Insulares

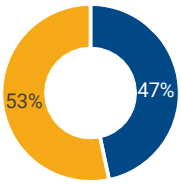
Diputaciones Provinciales, Cabildos y Consejos Insulares participantes y CAST

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



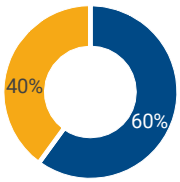
SI NO

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



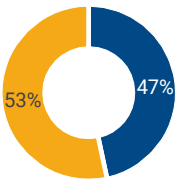
SI NO

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



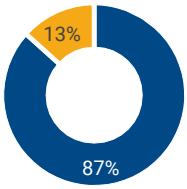
SI NO

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



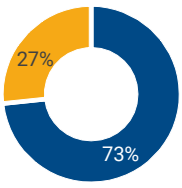
SI NO

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



SI NO

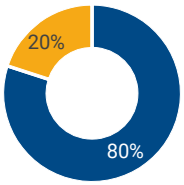
Conoce las implicaciones y cambios que el RGPD establece frente a la actual normativa Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD) y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD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



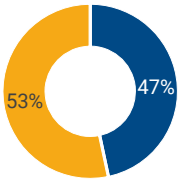
SI NO

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

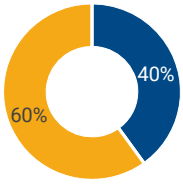
Ficheros declarados en la Agencia Española de Protección de Datos



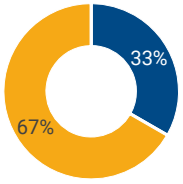
Documento de seguridad.



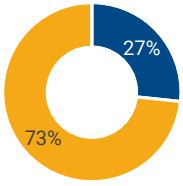
Informes de auditoría de medidas de seguridad.



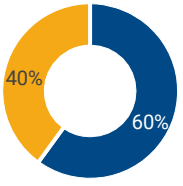
Responsable de seguridad.



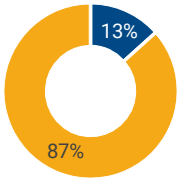
Contratos de acceso a datos con terceros



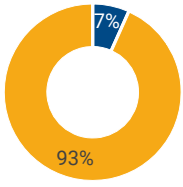
Textos informativos de protección de datos en los formularios de recogida de datos disponibles para los ciudadanos



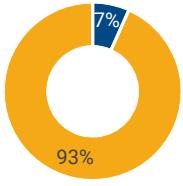
Plan de seguridad acorde con el Esquema Nacional de Seguridad



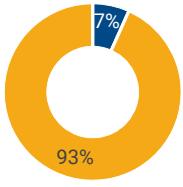
Análisis de riesgos en protección de datos.



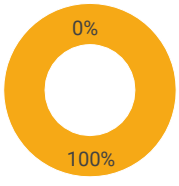
Evaluación de impacto en la protección de datos



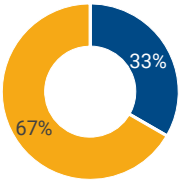
Creación del Registro de las Actividades en relación con los tratamientos de datos de su responsabilidad.



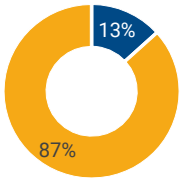
Nombramiento de un Delegado de Protección de Datos (DPO).



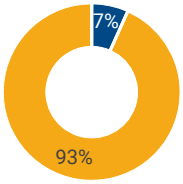
Información y transparencia del tratamiento



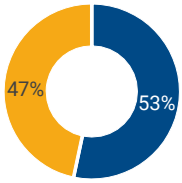
Sustitución de los contratos de acceso a datos por contratos de encargo de tratamiento



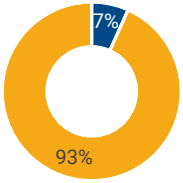
Protocolo de notificación de brechas de seguridad a la Agencia Española de Protección de Datos



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

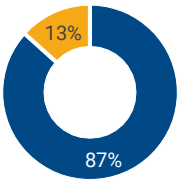


Protocolo para garantizar los derechos de supresión, limitación al tratamiento y portabilidad

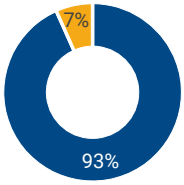


Gestionan los Ayuntamientos de su competencia alguno de los siguientes recursos, procesos o funciones

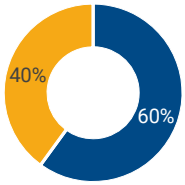
Padrón Municipal / Recursos propios de carácter tributario / Recogida residuos y limpieza diaria / Gestión obras públicas, pavimentación vías, urbanismo y vivienda / Actividades Culturales y Deportivas /



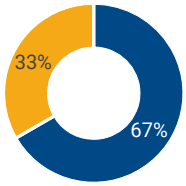
Licencias / Cementerios y servicios funerarios / Gestión económica del Ayuntamiento



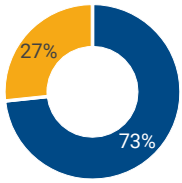
Desarrollo local y promoción empresarial



Bolsa de trabajo

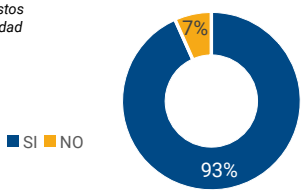


Empresas colaboradoras y proveedoras / Centro de Acceso Público a Internet

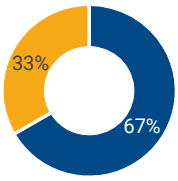


Servicios de titularidad municipal prestados por la Diputación/Cabildo/Consejo que implican tratamientos de datos de carácter personal

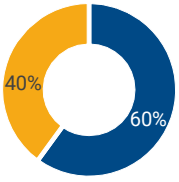
Recaudación de impuestos municipales / Contabilidad



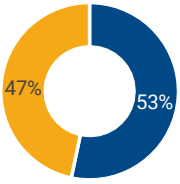
Servicios Sociales / Servicios de administración electrónica / Servicios de copias de seguridad



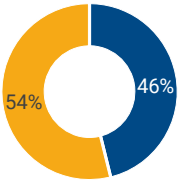
Servicios de micro-informática y asistencia técnica informática / Gestión de actividades deportivas y/o culturales /



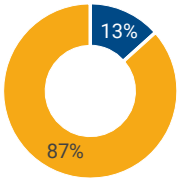
Servicios de urbanismo / Extinción de incendios



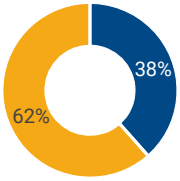
Servicios de agricultura y medio-ambiente



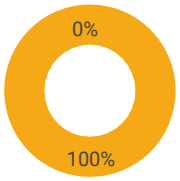
Oficina de atención al consumidor



Gestión de la contratación / Compra centralizada



Gestión de servicios de limpieza



7 GRUPO DE TRABAJO

Coordinador:

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

Integrantes:

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

Responsable FEMP:

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

Invitados:

- Jesús Rubí, Adjunto a la Directora de la Agencia Española de Protección de Datos.
- Rafael García Gozalo, Vocal Asesor Jefe del Departamento Internacional de la Agencia Española de Protección de Datos.

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

El pasado mes de abril se aprobó el Reglamento (UE) 2016/679 del Parlamento y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

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

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

Está publicación ha sido posible gracias al trabajo impulsado desde la Agencia Española de Protección de Datos, de quienes la FEMP ha querido ir de la mano, y consideramos que en ella se pueden encontrar gran parte de las claves necesarias para el cumplimiento normativo, así como tomar conciencia de la situación de partida en la que se encuentran nuestras Administraciones Locales.

FEMP
FEDERACION ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

RED
RED DE ENTIDADES LOCALES POR LA TRANSPARENCIA Y PARTICIPACIÓN CIUDADANA

Depósito Legal: M-18286-2018