1. INTRODUCCIÓN A LA PROTECCIÓN DE DATOS PERSONALES: CONCEPTOS CLAVE, MARCO REGULATORIO Y ALCANCE

¿Qué son los datos personales? ¿La dirección de correo electrónico de una persona? ¿Su número de teléfono? ¿El número de identificación? ¿Una imagen de una persona capturada por una cámara? ¿La cartera de una persona que ha sido robada? ¿Una persona que ha presentado una queja o reclamación ante un Ayuntamiento? Todos ellos son datos personales. Una idea importante es que los datos de identificación de una persona son datos personales, pero no solo en los casos mencionados.

Los datos personales son cualquier información relativa a una persona física identificada o identificable. ¿Y cuándo se identifica a un individuo? Cuando aparezca un nombre y apellido, un número de teléfono móvil, un número de documento de identidad, o cualquier otro dato que identifique a una persona.

Un dato personal es también información que se refiere a una persona no identificada, pero que se puede identificar, es decir, que es identificable. ¿Y cuándo es una persona identificable? Cuando se puede determinar una identidad a partir de cualquier elemento, como un código de identificación o un número de empleado, o un trabajo de una sola persona, como un secretario del ayuntamiento o un auditor.

Otros conceptos clave en el ámbito de la protección de datos son:

- Tratamiento de datos personales: es toda operación sobre datos personales, ya sea por procedimientos automatizados o no. Por lo tanto, también es un tratamiento cuando una persona presenta una instancia en papel. La recolección de datos personales se considera su captura, pero también su consulta, uso o difusión, incluida su destrucción, por lo que cuando se eliminen datos personales, debe hacerse de forma segura. En definitiva, un tratamiento es cualquier acción que se realice con datos de carácter personal.

- Responsable del tratamiento: es la persona, empresa o entidad que decide los fines y medios del tratamiento. Así, el responsable es quien decide iniciar la recogida y tratamiento de los datos personales por considerarlos necesarios para determinadas finalidades.

- Encargado del tratamiento: es la persona, empresa o entidad que trata datos personales por cuenta del responsable del tratamiento.

- Categorías especiales de datos: son los tipos de datos personales a los que la normativa de protección de datos otorga la máxima protección. Este grupo incluye datos relacionados con el origen étnico o racial, opiniones políticas, religión, afiliación sindical, datos genéticos o biométricos, datos de salud o datos relacionados con la vida sexual o la orientación sexual. En relación con estas categorías especiales de datos, existe una prohibición general de tratamiento, y solo es posible tratarlos en casos muy específicos.

El derecho a la protección de datos personales se rige por el 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 los mismos. y

El proyecto REthinkWASTE ha recibido financiación del Programa LIFE de la Unión Europea.
El contenido de esta publicación es responsabilidad exclusiva de ARC y no refleja necesariamente la opinión de la Unión Europea.

deroga la Directiva 95/46/CE, también conocida como Reglamento General de Protección de Datos (RGPD). El RGPD es obligatorio en todos los estados de la Unión Europea desde mayo de 2018.

En relación con el ámbito de aplicación, el RGPD se aplica al tratamiento total o parcialmente automatizado de datos personales; y también, al tratamiento no automatizado de los datos de carácter personal contenidos en un fichero o destinados a ser incluidos en el mismo. Un tratamiento automatizado de datos es aquel que se realiza a través de medios electrónicos. Este sería el caso de los documentos digitales que una persona guarda en su computadora. Por el contrario, el procesamiento no automatizado se realiza en papel.

Sin embargo, esta regla no se aplica en los siguientes casos:

- Actividades no cubiertas por el Derecho de la UE, como la seguridad nacional o la política exterior.
- Tratamientos realizados por un particular en el ejercicio de actividades exclusivamente personales o domésticas (por ejemplo, al enviar un WhatsApp a un amigo).
- El tratamiento de datos relativos a personas fallecidas.

Al margen de estas exclusiones, la normativa en materia de protección de datos personales no se aplica tampoco al tratamiento de datos relativos a personas jurídicas. Por tanto, un Ayuntamiento, una empresa o una asociación de vecinos no tiene Derecho de Protección de Datos Personales.

Desde un ámbito territorial, el RGPD establece que se aplica a los siguientes tratamientos de datos personales:

1. Los realizados en las actividades del encargado o del responsable establecido en la UE, aunque el tratamiento tenga lugar fuera de la Unión.
2. Los relacionados con interesados que se encuentren en la UE, realizados por un encargado o responsable del tratamiento fuera de la UE, si el tratamiento está relacionado con el suministro de bienes o servicios a interesados de la UE o si el tratamiento está vinculado al control del comportamiento de las personas que se encuentran en la UE, aunque dicho comportamiento tenga lugar en la Unión.
3. Y el último caso está relacionado con el tratamiento de datos realizado por una persona no establecida en la UE, pero en un lugar donde se aplica la ley de los estados miembros de la UE.

El proyecto REthinkWASTE ha recibido financiación del Programa LIFE de la Unión Europea.
El contenido de esta publicación es responsabilidad exclusiva de ARC y no refleja necesariamente la opinión de la Unión Europea.

2. PRINCIPIOS RELATIVOS AL TRATAMIENTO DE DATOS PERSONALES

Los principios relativos al tratamiento de datos personales se establecen en el artículo 5 del Reglamento Europeo y son los siguientes:

- El principio de licitud implica que los datos personales solo pueden ser tratados si existe al menos una base legal que permita el tratamiento. Esto se abordará en la siguiente sección.
- El principio de lealtad prohíbe la recogida de datos personales por medios fraudulentos, desleales o ilegales. Un ejemplo de recogida desleal de datos sería una encuesta de satisfacción del usuario sobre la calidad del servicio de recogida selectiva, que asegura que se hace de forma anónima, pero resulta que esto no es cierto, y que pueden vincular las respuestas a la persona que la realiza la encuesta.
- El principio de transparencia exige que los interesados sean informados de lo que se hará con sus datos en el momento de la recogida.
- El principio de limitación de la finalidad implica que los datos deben ser recabados para fines determinados, explícitos y legítimos, y que no deben ser tratados fraudulentamente de forma incompatible con dichos fines. Es decir, los datos recopilados con un propósito, no pueden usarse para nada más. Sin embargo, el procesamiento posterior de datos personales no se considera incompatible con fines de archivo de interés público, investigación científica e histórica o estadística.
- El principio de minimización de datos exige que los datos personales tratados sean adecuados, pertinentes y limitados a los fines para los que son tratados. En otras palabras, solo se deben recoger y tratar los datos que sean necesarios para la finalidad correspondiente, por lo que es necesario evitar el tratamiento de datos que sería desproporcionado.
- El principio de exactitud exige el tratamiento de datos personales exactos y actualizados. También es necesario suprimir o rectificar sin demora los datos personales que sean inexactos u obsoletos.
- El principio de limitación del plazo de conservación implica que la conservación de los datos de forma que se pueda identificar a las personas, sólo debe mantenerse durante el tiempo necesario para los fines perseguidos. Pasado este plazo, sólo podrán conservarse con fines de investigación, estadísticos o de archivo de interés público.
- El principio de integridad y confidencialidad obliga a garantizar la seguridad adecuada, mediante la aplicación de medidas técnicas u organizativas apropiadas, para evitar que los datos sean conocidos por personas no autorizadas, o se pierdan. En relación con este principio, se impone a todo el personal un deber de confidencialidad.
- El principio de responsabilidad proactiva o “accountability” obliga al responsable del tratamiento a ser consciente, diligente y proactivo en relación con todo tratamiento de datos

El proyecto REthinkWASTE ha recibido financiación del Programa LIFE de la Unión Europea.
El contenido de esta publicación es responsabilidad exclusiva de ARC y no refleja necesariamente la opinión de la Unión Europea.

personales. Por tanto, el responsable del tratamiento tiene el deber de asegurarse de que se cumplen todos los deberes impuestos por la normativa de protección de datos. Y no sólo debe cumplir, sino que debe tener capacidad para demostrarlo.

El proyecto REthinkWASTE ha recibido financiación del Programa LIFE de la Unión Europea.
El contenido de esta publicación es responsabilidad exclusiva de ARC y no refleja necesariamente la opinión de la Unión Europea.

3. LEGALIDAD DEL TRATAMIENTO DE DATOS

Para que el tratamiento de datos personales sea lícito, es necesario contar con al menos una de las bases legales establecidas en el artículo 6 del RGPD, las cuales se detallan a continuación.

- Uno de los motivos o bases legales que permiten el tratamiento de datos es el consentimiento del interesado, que para ser considerado válido debe ser libre, específico, informado e inequívoco (Artículo 6.1.a RGPD). El consentimiento sería la base jurídica que legitimaría la incorporación de un modelo de asesoramiento personalizado a través de una plataforma de mensajería instantánea digital (KAYT). Si se realiza la elaboración de perfiles, este consentimiento debe ser explícito. La creación de perfiles se trata en la siguiente sección.

- Para la ejecución de un contrato o la aplicación de medidas precontractuales a la instancia del interesado (artículo 6.1.b RGPD). Esto permitiría tratar los datos de contacto de representantes de empresas contratadas por una entidad local o de las presentadas en una licitación.

- El tratamiento también es lícito cuando es necesario para cumplir con una obligación legal (artículo 6.1.c RGPD).

- Cuando el tratamiento sea necesario para proteger intereses vitales (artículo 6.1.d RGPD). Se trata de una base jurídica subsidiaria, que sólo interviene si no es posible acudir a ninguna de las demás bases jurídicas y en situaciones en las que el interesado no está física o jurídicamente capacitado para prestar el consentimiento o cuando el tratamiento de datos es necesario en emergencias humanitarias causadas por desastres naturales o provocados por el hombre, o control de epidemias.

- Otra base jurídica que legitima el tratamiento es cuando sea necesario para el cumplimiento de una misión de interés público o en el ejercicio de facultades oficiales conferidas al responsable del tratamiento (artículo 6.1.e RGPD). Esta es la base legal que ampara la mayor parte del tratamiento de datos que realizan las entidades del sector público, e incluiría la prestación del servicio de recogida de residuos que permita la individualización de los usuarios, la incorporación de un sistema de pago por generación (PAYT) o las tareas de vigilancia, control e inspección. En este último punto, es importante destacar la importancia de detallar todas estas funciones en la correspondiente normativa municipal del ente local, detallando las normas que atribuyen estas competencias a los entes locales y, al mismo tiempo, especificando qué agentes las llevarán a cabo fuera y de qué manera. Esto determinará los perfiles de usuarios que pueden tratar los datos y el tratamiento específico que pueden realizar.

- También se considera lícito el tratamiento cuando sea necesario para satisfacer intereses legítimos del responsable del tratamiento o de un tercero (artículo 6.1.f RGPD). Por ejemplo, una empresa que graba llamadas telefónicas de atención al cliente. No obstante, esta base jurídica del interés legítimo no se aplica a las administraciones públicas en el ejercicio de sus funciones.

El proyecto REthinkWASTE ha recibido financiación del Programa LIFE de la Unión Europea.
El contenido de esta publicación es responsabilidad exclusiva de ARC y no refleja necesariamente la opinión de la Unión Europea.

4. ELABORACIÓN DE PERFILES

La elaboración de perfiles es el procesamiento de datos para evaluar ciertos aspectos personales de un individuo; en particular, para analizar o predecir aspectos de las preferencias personales, intereses, confiabilidad, comportamiento, ubicación o movimientos de ese sujeto. Por ejemplo, cuando navegas por Internet, ciertas cookies rastrean lo que la persona está navegando para determinar cuáles son sus preferencias y mostrarle anuncios personalizados.

La gestión del cobro de residuos de pago por generación (PAYT) puede conducir al desarrollo de perfiles de comportamiento de las personas que utilizan el servicio de recolección de residuos. En concreto, el análisis de los datos generados en la prestación del servicio, asociados a la persona que utiliza el servicio a través de la dirección, permiten establecer las rutinas o preferencias de las personas afectadas en el uso del servicio. Es decir, te permite evaluar ciertos aspectos de tu comportamiento.

Estos perfiles pueden llegar a tener efectos significativos, e incluso efectos jurídicos, si se aplica un sistema de reparto (por ejemplo, determinando si se aplica o no una bonificación) o si los datos obtenidos se utilizan para controlar cómo se desechan los residuos. depositados (por ejemplo, si se penaliza una mala recogida de separación). En tales casos, estos efectos deberían ser necesarios para celebrar o ejecutar un contrato entre el titular de los datos y un controlador; que esté previsto por la legislación de la UE o de los Estados miembros; o en base al consentimiento explícito.

El proyecto REthinkWASTE ha recibido financiación del Programa LIFE de la Unión Europea.
El contenido de esta publicación es responsabilidad exclusiva de ARC y no refleja necesariamente la opinión de la Unión Europea.

5. CONTRATOS DE TRATAMIENTO DE DATOS

Cuando un Ayuntamiento (Responsable del Tratamiento) utiliza una empresa (Encargado del Tratamiento) para la prestación del servicio de recogida de residuos, desde la perspectiva de la normativa de protección de datos, esta relación debe estar regulada por un contrato u otro acto jurídico, como por ejemplo un acuerdo de colaboración que deberá respetar el contenido mínimo determinado en el artículo 28.3 del Reglamento Europeo de Protección de Datos, refiriéndose, entre otros, a:

a) El objeto, la duración, la naturaleza y la finalidad del tratamiento.

b) El tipo de datos personales y las categorías de personas interesadas.

c) Las obligaciones y derechos del responsable del Tratamiento.

d) Las instrucciones del responsable del Tratamiento.

El Procesador de datos puede confiar ciertas actividades a un sub-encargado. Para ello, deberá suscribirse un contrato entre ellos con las mismas obligaciones en materia de protección de datos estipuladas en el contrato inicial suscrito con el Responsable del Tratamiento. Además, es imprescindible que el Responsable del Tratamiento autorice al Encargado del Tratamiento a contratar un sub-encargado.

Por ejemplo, una empresa que gestiona el servicio de recogida de residuos (encargado del tratamiento), que contrata a otra empresa (sub-encargado del tratamiento) para el suministro de la tecnología necesaria para un nuevo modelo de recogida de residuos, lo que significa que la empresa contratada tiene acceso a los datos de los usuarios del servicio.

El proyecto REthinkWASTE ha recibido financiación del Programa LIFE de la Unión Europea.
El contenido de esta publicación es responsabilidad exclusiva de ARC y no refleja necesariamente la opinión de la Unión Europea.

6. EVALUACIÓN DEL IMPACTO DE LA PROTECCIÓN DE DATOS

Las evaluaciones de impacto de protección de datos (EIPD), que deben realizarse antes del procesamiento, no son necesarias para ningún procesamiento de datos personales, pero solo cuando existe un alto riesgo relacionado con los derechos y libertades de las personas, debido a la naturaleza del procesamiento, el alcance y contexto, las finalidades o el uso de las nuevas tecnologías.

El Reglamento Europeo (GDPR) contiene una lista de tratamientos en los que se requiere la EIPD:

a) cuando tenga por objeto la evaluación "sistemática y exhaustiva" de aspectos de la persona realizada de oficio. Por ejemplo, a la hora de perfilar con efectos jurídicos, qué podría pasar en determinados supuestos de uso de inteligencia artificial en el sector público;

b) cuando se trate de categorías especiales de datos a gran escala, como un hospital, o datos relacionados con condenas e infracciones penales; y

c) cuando se realiza una observación sistemática a gran escala de un área de acceso público, como sería el caso de un sistema de videovigilancia en una infraestructura utilizada diariamente por miles de personas.

El listado de casos en los que, según el RGPD, es necesario realizar la EIPD por considerar que se trata de tratamientos de alto riesgo, no tiene el carácter de listado cerrado, y por tanto el RGPD prevé que las autoridades de control puedan publicar la lista de los tipos de tratamientos que requieren una EIPD y la lista de tratamientos en los que no se requiere la EIPD (las listas publicadas por la Autoridad Española de Protección de Datos se pueden consultar aquí).

El contenido mínimo que debe tener la EIPD, en caso de ser necesario, es el siguiente: una descripción del tratamiento, como el ciclo de vida de los datos; el propósito o base legal; la valoración de la necesidad y proporcionalidad del tratamiento; evaluación de riesgos y medidas para minimizarlos; etc.

Si como resultado de la evaluación de impacto, el Responsable del Tratamiento continúa observando un riesgo elevado que no puede ser mitigado o reducido por medios razonables de acuerdo con la tecnología disponible y los costes de la aplicación, deberá consultar a la Autoridad de Control antes de iniciar tal Procesando. La Autoridad de Control deberá advertir al Responsable del Tratamiento, pero también podrá prohibir su tratamiento.

El proyecto REthinkWASTE ha recibido financiación del Programa LIFE de la Unión Europea.
El contenido de esta publicación es responsabilidad exclusiva de ARC y no refleja necesariamente la opinión de la Unión Europea.

7. OTRAS OBLIGACIONES

Además de las obligaciones presentadas hasta ahora, el RGPD impone otras obligaciones al Controlador.

La primera de estas obligaciones son las políticas de protección de datos, para las cuales el RGPD no especifica cuál debe ser su contenido. Estas políticas se configuran como una de las medidas de índole técnica y organizativa a adoptar por el responsable del tratamiento, que debe incluir información sobre los tratamientos de datos que lleva a cabo la organización, así como sus compromisos en relación con la protección de datos (por ejemplo, identificación de los Responsables del tratamiento y Delegado de Protección de Datos, cómo se pueden ejercer los derechos, etc.).

La siguiente obligación es el registro de actividades de tratamiento (RAT). La RAT ha sustituido la anterior obligación de registro de ficheros ante las Autoridades de Control, procedimiento que desapareció con el RGPD. Las entidades del sector público, como los Ayuntamientos, están obligadas a disponer de este Registro.

El RGPD establece el contenido del Registro (fines del tratamiento, categorías de interesados y datos personales, descripción general de las medidas técnicas y organizativas de seguridad, entre otras).

En determinados casos, la obligación de disponer de la RAT, con contenido similar, también es aplicable a los Encargados del Tratamiento, debiendo identificarse también el Responsable del Tratamiento por cuenta del cual trabaja el Encargado del Tratamiento.

La siguiente es una explicación de la protección de datos por diseño y la protección de datos por defecto. En primer lugar, la Protección de Datos desde el Diseño implica tener en cuenta todas las obligaciones y requisitos que impone la normativa de protección de datos, desde el momento en que se diseña un nuevo tratamiento. En particular, requiere la implementación de medidas técnicas y organizativas apropiadas, como la pseudonimización; aplicar de manera efectiva los principios de protección de datos; e integrar las garantías necesarias para cumplir con las obligaciones impuestas por el RGPD y para proteger los derechos de los interesados. Por ejemplo, si una entidad local decide crear un canal electrónico que permita la participación ciudadana, antes de implementarlo debe evaluar si es necesario identificar a los interesados, qué datos se recopilan, cómo garantizar la seguridad de los datos, cómo pueden ejercer sus derechos, etc.

Y, en segundo lugar, la Protección de Datos por Defecto es el principio según el cual una organización (el responsable del tratamiento) se asegura de que solo se traten por defecto (sin la intervención del usuario) los datos estrictamente necesarios para cada finalidad específica del tratamiento. Así, cuando una persona se registra en una red social, la protección de datos por defecto supondría que, sin tener que configurar nada, el perfil debería ser privado. Y al revés, si el usuario quiere que sea público, esta modificación debe realizarla él mismo.

El Reglamento Europeo también exige que se tomen las medidas apropiadas o adecuadas para garantizar la seguridad de los datos. Se debe realizar un análisis de riesgo adecuado para determinar las medidas de seguridad apropiadas.

El proyecto REthinkWASTE ha recibido financiación del Programa LIFE de la Unión Europea.
El contenido de esta publicación es responsabilidad exclusiva de ARC y no refleja necesariamente la opinión de la Unión Europea.

El análisis de riesgos debe tener en cuenta los siguientes elementos: la naturaleza de los datos (p. ej., si se procesan categorías especiales de datos), el número de interesados afectados o la cantidad (volumen de datos), o la variedad del procesamiento (p. ej., si permite perfilar).

El RGPD establece que las medidas de seguridad pueden consistir en:

- Minimizar el procesamiento de datos.
- La pseudonimización o encriptación de los datos.
- La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia continua de los sistemas y servicios de procesamiento, es decir, la capacidad de resistir o recuperarse (por ejemplo, de un ataque de piratas informáticos).
- La capacidad de restaurar la disponibilidad y el acceso a los datos personales rápidamente, en caso de un incidente físico o técnico (por ejemplo, con copias de seguridad).
- Un proceso para verificar, evaluar y evaluar periódicamente la eficacia de las medidas de seguridad. Por ejemplo, esto se lograría mediante auditorías de estas medidas.

Otra obligación es denunciar las violaciones de seguridad. Esta obligación implica que, ante cualquier vulneración o incidente en la seguridad de los datos que se sufra y suponga un riesgo para los derechos y libertades de los interesados, el Ayuntamiento responsable del tratamiento deberá comunicarlo a la Autoridad de Control competente. Esta notificación debe hacerse sin demora, a más tardar 72 horas después del momento de la infracción. Sin embargo, si no es probable que la violación constituya un riesgo para los derechos y libertades de las personas, dicha notificación no es necesaria.

En los casos en que deba ser comunicado a la Autoridad de Control por no poder considerarse improbable el riesgo, si la Entidad Local considera que la violación de la seguridad puede suponer un alto riesgo para los derechos y libertades de las personas, además de comunicarlo a la Autoridad de Control, los interesados en cuestión deben ser notificados y se les deben ofrecer recomendaciones para mitigar los riesgos.

En todo caso, ante cualquier tipo de incidencia que pueda afectar a la seguridad de los datos, incluso en los supuestos que no requieran comunicación a la Autoridad, el órgano local responsable deberá documentar internamente la incidencia, anotando los hechos y las medidas correctoras. adoptado. Esta documentación interna se pondrá a disposición de la Autoridad de Control para que pueda realizar las comprobaciones correspondientes.

Finalmente, la designación de un Delegado de Protección de Datos (DPD) es obligatoria en determinados supuestos, y en todo caso cuando el Responsable del Tratamiento o Encargado del Tratamiento sea una Autoridad u Organismo Público. Por lo tanto, un Ayuntamiento está obligado a tener un DPO. No obstante, se puede designar un mismo DPD para varias entidades.

El DPD es el referente de la organización en materia de protección de datos, que, entre otros requisitos, debe contar con experiencia en esta materia.

Las funciones del DPO se describen en la normativa de protección de datos. Los más relevantes son:

El proyecto REthinkWASTE ha recibido financiación del Programa LIFE de la Unión Europea.
El contenido de esta publicación es responsabilidad exclusiva de ARC y no refleja necesariamente la opinión de la Unión Europea.

- Debe informar y asesorar al Responsable del Tratamiento o Encargado del Tratamiento, así como a sus empleados, sobre las obligaciones que deben cumplir en materia de protección de datos.

- También es responsable de supervisar el cumplimiento de la normativa de protección de datos y de las políticas del Responsable del tratamiento o del Encargado del tratamiento, incluida la asignación de responsabilidades, la sensibilización y formación del personal y las auditorías relacionadas.

El proyecto REthinkWASTE ha recibido financiación del Programa LIFE de la Unión Europea.
El contenido de esta publicación es responsabilidad exclusiva de ARC y no refleja necesariamente la opinión de la Unión Europea.

8. DERECHO A SER INFORMADO

El derecho a la información forma parte del núcleo esencial del derecho a la protección de datos personales, ya que permite ejercer la facultad de control o disposición que tienen los sujetos sobre sus datos personales. Este derecho que toda persona tiene de controlar su información personal sólo será efectivo si se informa previamente a los interesados sobre los usos de los datos y otros detalles que se explicarán a continuación.

Con carácter general, corresponde al responsable del tratamiento hacer valer el derecho a la información, aunque si la recogida de datos la realiza el encargado del tratamiento, puede estar previsto en el contrato del responsable del tratamiento que asume la función de informar.

Si los datos se recopilan del mismo interesado, la información debe proporcionarse en el momento de la recopilación. En estos casos, la información que debe facilitarse al interesado en cuestión está contenida en el artículo 13 del RGPD.

Si, por el contrario, los datos no se obtienen del interesado en cuestión, sino de otra fuente (por ejemplo, otra Administración), la información a facilitar está recogida en el artículo 14 del Reglamento Europeo de Protección de Datos, que establece que debe facilitarse en un plazo razonable, pero en todo caso en el plazo máximo de 1 mes desde la recepción de los datos.

El RGPD prevé casos en los que no es necesario informar al interesado en cuestión, como cuando la persona ya tiene la información. O no es necesario informar si los datos no se recopilan directamente del interesado en cuestión, sino de otra fuente, y la comunicación de la información es imposible o implica un esfuerzo desproporcionado, o si la recopilación o transmisión de datos es proporcionada por Derecho de la UE o Derecho de los Estados miembros.

En cuanto al contenido de la información a facilitar, en caso de que los datos se obtengan directamente del interesado, el artículo 13 del Reglamento Europeo obliga al Responsable a informar en el momento de la recogida sobre varias cuestiones: quién es el responsable y cómo contactarlo; los datos de contacto del Delegado de Protección de Datos, las finalidades del tratamiento y su base jurídica; los destinatarios o categoría de destinatarios a los que se pueden comunicar los datos; el período de retención de los datos; la posibilidad de ejercer los derechos establecidos a continuación; el derecho a retirar el consentimiento; el derecho a reclamar ante una Autoridad de Control; etc.

Por lo tanto, si los datos personales se recopilan a través de un formulario, los interesados deben ser informados de todos estos detalles.

Si los datos no se obtuvieron directamente del interesado en cuestión, el artículo 14 del RGPD establece que el interesado también debe ser informado de las categorías de datos en cuestión; y la fuente u origen de los datos personales y, en su caso, si proceden de fuentes de acceso público, como Internet.

El proyecto REthinkWASTE ha recibido financiación del Programa LIFE de la Unión Europea.
El contenido de esta publicación es responsabilidad exclusiva de ARC y no refleja necesariamente la opinión de la Unión Europea.

9. OTROS DERECHOS QUE SE PUEDEN EJERCER: ACCESO, RECTIFICACIÓN, SUPRESIÓN, RESTRINGIR EL TRATAMIENTO, PORTABILIDAD DE DATOS, OPONERSE Y NO SER OBJETO DE DECISIONES AUTOMATIZADAS

El RGPD reconoce los siguientes derechos en relación con el tratamiento de datos personales: derecho de acceso, derecho de rectificación, derecho de supresión, derecho de limitación del tratamiento, derecho a la portabilidad de los datos, derecho de oposición y derecho de no ser objeto de una decisión basada únicamente en el tratamiento automatizado. Estos derechos son personalísimos, por lo que sólo puede ejercerlos el propio titular de los datos, aunque también puede hacerlo a través de un representante legal o voluntario.

El plazo de respuesta a la solicitud de ejercicio de cualquiera de los derechos es de un mes, prorrogable por otros dos meses en caso de ser necesario, teniendo en cuenta la complejidad y el número de solicitudes. Si el Responsable del Tratamiento considera que el derecho ejercido no es adecuado, también deberá responder sin demora y en el plazo máximo de un mes, indicando al interesado las razones por las que el derecho ejercido no es efectivo. Asimismo, deberá ser informado de la posibilidad de tomar las medidas oportunas, en particular para reclamar ante una Autoridad de Control.

Cada uno de estos derechos se aborda a continuación:

- Acceso: La finalidad de este derecho es que cualquier persona sepa que sus datos están siendo tratados por una entidad local. Si una persona ejerce este derecho y el Controlador procesa sus datos personales, se debe proporcionar una copia de los datos que se procesan, así como otra información adicional, que es en gran medida acorde con el contenido del derecho a la información (fines del procesamiento; categorías de datos personales; destinatarios o categorías de destinatarios; plazo de conservación previsto o criterios utilizados para determinarlo, etc.). El derecho a obtener una copia de los datos no puede afectar negativamente a los derechos y libertades de terceros.

- Rectificación: mediante este derecho la persona puede solicitar la modificación de los datos que sean inexactos, o que se completen los que sean incompletos. Cuando se ejerza este derecho, la solicitud de rectificación deberá indicar los datos a que se refiere, y la rectificación a realizar; y deberá acompañarse, en su caso, de la documentación que justifique la inexactitud o lo incompleto de los datos objeto de tratamiento.

- Supresión o derecho al olvido: es el derecho del interesado a que se supriman los datos personales en determinados supuestos: cuando los datos ya no sean necesarios para los fines perseguidos; cuando el interesado en cuestión retire su consentimiento; si el interesado en cuestión se opone al procesamiento y no prevalecen otras razones legítimas para el procesamiento; si los datos han sido procesados ilegalmente; etc. El Reglamento

El proyecto REthinkWASTE ha recibido financiación del Programa LIFE de la Unión Europea.
El contenido de esta publicación es responsabilidad exclusiva de ARC y no refleja necesariamente la opinión de la Unión Europea.

Europeo enumera los casos en los que este derecho no se aplica, considerando que el tratamiento es necesario para ejercer el derecho a la libertad de expresión e información; para cumplir con una obligación legal que requiera el procesamiento de datos, como cuando la legislación de archivo requiere la retención de la documentación que contiene los datos; o para llevar a cabo una tarea realizada en interés público o en el ejercicio de la autoridad oficial conferida a la persona responsable; etc.

- Limitación del tratamiento: permite al interesado exigir que los datos sólo puedan ser utilizados en determinadas circunstancias. En otras palabras, es como suspender el procesamiento de datos, pero no borrarlos. Este derecho podrá solicitarse en los cuatro casos siguientes: cuando el Interesado impugne la exactitud de los datos personales, durante el plazo que permita al responsable verificar la exactitud de los mismos; cuando el tratamiento sea ilícito pero el interesado se oponga a la supresión de los datos y, en lugar de borrarlos, solicite que se limite su uso; cuando el responsable del tratamiento ya no necesite los datos para los fines del tratamiento, pero el interesado los necesite para formular, ejercer o defender reclamaciones; y cuando el interesado en cuestión se haya opuesto al procesamiento sobre la base de una situación particular, mientras se verifica si los motivos legítimos del Controlador prevalecen sobre los del interesado en cuestión.

- Portabilidad de los datos: puede ejercerse si el tratamiento se realiza por medios automatizados; y también, si se basa en el consentimiento del interesado o en la ejecución de un contrato. Por tanto, el derecho a la portabilidad de los datos no entra en juego cuando el tratamiento sea realizado por las Administraciones Públicas para el cumplimiento de una misión de interés público o en el ejercicio de facultades públicas atribuidas al responsable del tratamiento, o en cumplimiento de una obligación legal.

  En los casos en que resulte aplicable este derecho, el interesado podrá solicitar la transferencia de los datos a otro responsable del tratamiento, o también solicitar que los datos facilitados al responsable del tratamiento se le faciliten en un formato estructurado.

- Oposición: en virtud de este derecho se solicita al Responsable el cese de un determinado tratamiento de los datos, y dicha solicitud se basa en motivos relacionados con la situación particular del solicitante, como persona que puede ser víctima de violencia de género, protegida testimonio, etc.

  Este derecho podrá ejercerse cuando el tratamiento, incluida la elaboración de perfiles, se base en el interés público o en el ejercicio de poderes públicos conferidos al Responsable del tratamiento; en el interés legítimo perseguido por el Responsable o por un tercero; o se realice con fines de investigación científica o histórica o con fines estadísticos, salvo que sea necesario para llevar a cabo una misión realizada por razones de interés público. En tales casos, el responsable del tratamiento cesará en el tratamiento, salvo que acredite motivos legítimos que prevalezcan sobre los intereses, derechos y libertades del interesado; o que el tratamiento sea necesario para la formulación, el ejercicio o la defensa de reclamaciones.

- A No ser objeto de una decisiones individuales automatizadas, incluida la elaboración de perfiles: en el caso de las administraciones públicas, estas decisiones pueden darse en supuestos de tratamientos automatizados de los datos personales, como si en la recogida de residuos se establecen sistemas de pago por generación o por participación (tasa justa), en base al principio de “quien contamina paga. Sin embargo, este derecho no existe cuando la decisión automatizada es necesaria para celebrar o ejecutar un contrato entre el interesado en cuestión y un responsable del tratamiento; cuando se basa en el

El proyecto REthinkWASTE ha recibido financiación del Programa LIFE de la Unión Europea.
El contenido de esta publicación es responsabilidad exclusiva de ARC y no refleja necesariamente la opinión de la Unión Europea.

consentimiento explícito del interesado en cuestión; o cuando está autorizado por la legislación de la UE o de los Estados miembros.

Excepto en este último caso, cuando la decisión esté autorizada por una norma de la UE o de un Estado miembro, el interesado tiene derecho a obtener la intervención humana del Responsable del tratamiento, a expresar su punto de vista y a impugnar la decisión.

El proyecto REthinkWASTE ha recibido financiación del Programa LIFE de la Unión Europea.
El contenido de esta publicación es responsabilidad exclusiva de ARC y no refleja necesariamente la opinión de la Unión Europea.

10. LA AUTORIDAD DE CONTROL Y EL SISTEMA DE GARANTÍAS DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

En caso de incumplimiento de los deberes impuestos por el Reglamento Europeo de Protección de Datos o de los derechos reconocidos a todas las personas, se podrá presentar una reclamación ante la Autoridad de Control competente.

En cuanto al régimen sancionador, el RGPD establece dos listas de infracciones, que pueden ser sancionadas con multas de un máximo de 10 o 20 millones de euros o, en el caso de una empresa, una cantidad equivalente al 2% o 4%, como máximo, de la facturación total anual del año anterior, y entre las dos opciones se deberá elegir la de mayor cuantía.

Sin embargo, en el caso de infracciones cometidas por entidades del sector público, la ley orgánica de protección de datos ha descartado la imposición de multas a entidades del sector público.

Por otro lado, si una persona sufre un daño o perjuicio, material o inmaterial (como el daño moral) como consecuencia de una infracción del Reglamento Europeo, tiene derecho a recibir una indemnización del Responsable del tratamiento o del Encargado del tratamiento por la perjuicios causados.

El proyecto REthinkWASTE ha recibido financiación del Programa LIFE de la Unión Europea.
El contenido de esta publicación es responsabilidad exclusiva de ARC y no refleja necesariamente la opinión de la Unión Europea.

11. TRANSFERENCIAS INTERNACIONALES DE DATOS

Las transferencias internacionales de datos implican el flujo de datos personales desde el territorio de un Estado Miembro hacia destinatarios establecidos en países fuera del Espacio Económico Europeo, lo que sólo podrá realizarse en los siguientes casos:

- En países, territorios o sectores concretos sobre los que la Comisión Europea haya tomado una decisión reconociendo que ofrecen un nivel adecuado de protección.
- Cuando se hayan brindado las garantías adecuadas sobre la protección que los datos recibirán en su destino:
  - ✓ Instrumento vinculante y exigible entre Administraciones u organismos públicos.
  - ✓ Normas societarias vinculantes (NSV).
  - ✓ Cláusulas tipo de protección de datos adoptadas por la Comisión Europea o la Autoridad de Control competente.
  - ✓ Con autorización de la Autoridad de Control, con base en cláusulas contractuales o disposiciones que se incorporen a acuerdos vinculantes entre organismos públicos que contengan derechos exigibles.
  - ✓ Un código de conducta que incorpore compromisos vinculantes y exigibles.
  - ✓ Un mecanismo de certificación que incorpore compromisos vinculantes y exigibles.
- Cuando concurra alguna de las excepciones previstas en el artículo 49 del RGPD que permitan la transferencia de datos sin garantías de adecuada protección, por razones de necesidad vinculadas al interés del titular de los datos o al interés general.

El proyecto REthinkWASTE ha recibido financiación del Programa LIFE de la Unión Europea.
El contenido de esta publicación es responsabilidad exclusiva de ARC y no refleja necesariamente la opinión de la Unión Europea.

12. CONCLUSIONES

Uno de los elementos a tener en cuenta a la hora de implantar un sistema de recogida de residuos es la protección de datos personales. En este punto, cabe señalar que las entidades locales con competencia en la recogida de residuos pueden tratar los datos que sean estrictamente necesarios.

El tratamiento de estos datos es legítimo en el desempeño de una misión de interés público o en el ejercicio de poderes públicos. De esta forma, no es necesario obtener el consentimiento del interesado en la prestación del servicio de recogida de residuos. Cuando la recogida de residuos implique la elaboración de perfiles que afecten a la persona que utiliza el servicio, por ejemplo, si se prevé una bonificación en función de las aportaciones individuales realizadas, se requerirá uno de los siguientes: el consentimiento del interesado, el amparo de la legislación de la UE o de los Estados miembros para tal elaboración de perfiles, o un contrato entre el interesado y un responsable del tratamiento.

También es necesario valorar si, antes de poner en funcionamiento el sistema de recogida de residuos, es necesario realizar una evaluación de impacto en materia de protección de datos, especialmente si existe perfil en los términos establecidos, como es el caso de los sistemas de pago por generación.

Por último, cabe señalar que toda empresa o entidad que preste un servicio a un ente local en el marco de la prestación del servicio de recogida de residuos, lo que implica que pueda tener acceso a datos de carácter personal, tendrá la consideración de Encargado del Tratamiento. En este caso, deberá suscribirse el correspondiente acuerdo o contrato de Encargado del Tratamiento.

El proyecto REthinkWASTE ha recibido financiación del Programa LIFE de la Unión Europea.
El contenido de esta publicación es responsabilidad exclusiva de ARC y no refleja necesariamente la opinión de la Unión Europea.