Kit Digital – Formación RGPD

Información Confidencial propiedad de acens

Kit Digital: Formación sobre RGPD

DATOS PERSONALES

¿QUÉ ES UN DATO PERSONAL?

Un dato personal es toda información sobre una persona física identificada o identificable, como pueden ser nombre, apellidos, DNI, teléfono, email, dirección postal, datos físicos, datos económicos, datos culturales/sociales de personas, etc. El concepto de dato personal es muy amplio.

¿DÓNDE SE REGULA EL TRATAMIENTO DE DATOS PERSONALES?

El tratamiento de datos personales se regula a nivel europeo en el Reglamento General de Protección de Datos (RGPD) y en España por la Ley de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPD-GDD).

¿QUÉ SE ENTIENDE POR TRATAMIENTO?

Un tratamiento de datos personales es 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.

PARTES DEL TRATAMIENTO DE DATOS

Interesado

Persona física a la que concierne la información, titular de los derechos.

Responsable

Persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento de datos personales. Es el destinatario principal de deberes y obligaciones del RGPD.

Encargado

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

¿QUIÉN VELA POR LA PROTECCIÓN DE LOS DATOS PERSONALES?

En España, principalmente la Agencia Española de Protección de Datos (AEPD).

La AEPD tiene un amplio elenco de funciones y poderes, incluidos investigación y sanción.

Sanciones

La AEPD es también la encargada de imponer sanciones. Las multas administrativas pueden llegar, en los casos más graves, a los 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.

¿CUÁNDO PUEDO TRATAR DATOS PERSONALES DE INTERESADOS?

Necesitas una base jurídica. Hay seis: consentimiento; contrato o medidas contractuales; obligación legal; interés vital, misión en interés público o en ejercicio de poderes públicos; interés legítimo.

Las más importantes como responsable son las siguientes:

Consentimiento

El interesado puede dar su consentimiento para uno o varios fines específicos. El consentimiento tiene que ser:

a) Libre. El RGPD prohíbe supeditar un contrato a la prestación del servicio a consentimiento para tratar datos no necesarios;
b) Específico. 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, deforma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo.
c) Inequívoco. Tiene que ser una clara acción afirmativa. No es válido el consentimiento tácito (por ejemplo, con casillas premarcadas).
d) Informado. Es necesario informar como mínimo de la identidad del responsable y de los fines del tratamiento, esta información se tiene que dar de manera previa.

El responsable es quien debe ser capaz de demostrar el consentimiento, por lo que tiene que documentar que este consentimiento se otorgó.

Contrato o medidas contractuales

Se da cuando 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.

Obligación legal

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

En sí misma no es una base: hay que remitirse a una norma del Derecho de la UE o de un Estado. Se exige que la finalidad esté determinada en la norma que establece la base jurídica. La LOPDGDD exige que se prevea en una norma con rango de ley.

Interés legítimo

El interés legítimo entra en juego cuando el tratamiento es necesario para la satisfacción e intereses legítimos perseguidos por el responsable 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.

Estos intereses pueden ser no sólo jurídicos, sino también económicos, sociales o morales, del responsable o de un tercero.

Exige ponderar los intereses y derechos que concurren y determinar cuál prevalece. Hay que realizar un juicio de ponderación, atendiendo a las circunstancias concurrentes en el caso y decidir, justificando razonadamente, conforme a criterios de proporcionalidad, cuál prevalece.

Si se utiliza esta base, se ha de informar al afectado sobre el interés concreto. Si el afectado ejerce su derecho de oposición, hay que hacer una nueva ponderación, solo se mantiene si se acreditan motivos legítimos imperiosos prevalentes.

¿QUÉ DERECHOS PUEDEN EJERCER LOS INTERESADOS?

El responsable debe facilitar el ejercicio a los interesados, respondiendo sin dilación y a más tardar en un mes (prorrogable otros dos por la complejidad de la petición, informando al interesado). El ejercicio de los derechos tiene carácter gratuito.

Si se tienen dudas razonables sobre la identidad del interesado, se podrá solicitar que facilite información adicional.

Acceso

En el derecho de acceso el interesado busca confirmación de si el responsable está tratando o no sus datos. El responsable facilitará una copia de estos datos.

Como información complementaria, se incluye fines, categoría de datos, destinatarios a los que se comunican, plazo de conservación, información sobre derechos de interesados, información sobre el origen, la exigencia de decisiones automatizadas, e información sobre transferencias internacionales y garantías.

Rectificación

Corrección de datos inexactos.

Supresión

Cuando no sean necesarios para los fines; se retire el consentimiento, o hayan sido tratados ilícitamente.

Si se han cedido a terceros, el responsable deberá adoptar medidas razonables para comunicar la solicitud de supresión.

Hay excepciones a este derecho: libertad de expresión, obligación legal, ejercicio de reclamaciones…

Oposición

Se puede dar en dos situaciones:

1) En tratamientos basados en cumplimiento de obligación legal o interés legítimo, por motivos relacionados con su situación particular.
2) En tratamiento con fines de mercadotecnia directa (publicidad), en cualquier momento sin alegar motivos.

Limitación del tratamiento

Es el marcado de los datos personales conservados con el fin de limitar su tratamiento en el futuro.

El interesado tendrá derecho a la limitación cuando se cumpla alguna de las siguientes condiciones:

a) 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.

Derecho a no ser objeto de decisiones individuales automatizadas, incluida la elaboración de perfiles

Derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado que produzca efectos jurídicos o le afecte significativamente de modo similar.

Portabilidad de los datos

Es el derecho a recibir los datos personales en un formato estructurado de uso común y lectura mecánica y a transmitirlos a otro responsable.

¿CUÁLES SON LAS OBLIGACIONES DE LOS RESPONSABLES Y ENCARGADOS?

Registro de actividades del tratamiento

Cada responsable y cada encargado, debe llevar un registro de actividades de datos. Este registro debe constar por escrito y estar a disposición de las autoridades de control.

Medidas técnicas y organizativas

Se deben aplicar las medidas técnicas y organizativas apropiadas para garantizar y poder demostrar que los tratamientos son conformes con el RGPD.

a) Privacy by design: privacidad desde el diseño

Se deben abordar las cuestiones de privacidad desde el diseño del producto o servicio y mantenerlas actualizadas a lo largo de todo el ciclo de vida. La AEPD ha elaborado una Guía de Privacidad desde el Diseño.

b) Privacy by default: privacidad por defecto
Se debe garantizar que por defecto sólo se traten los datos necesarios para cada uno de los fines y que no sean accesibles a un número indeterminado de personas sin la intervención del afectado. La AEPD ha elaborado una Guía de Protección de Datos por Defecto.

Medidas de seguridad

Se deben aplicar las medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad adecuado al riesgo.

Se debe tener en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como 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, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.

Se debe hacer siempre una evaluación sobre análisis de riesgo y documentarla.

Evaluaciones de impacto (PIAs)

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.

La Agencia Española de Protección de Datos ha realizado una documento sobre la gestión del riesgo y evaluación de impacto en tratamientos de datos personales. También puede ser útil EVALÚA RIESGO RGPD, un prototipo de herramienta que facilita la evaluación del nivel de riesgo de los tratamientos.

Notificaciones de las violaciones de seguridad

Implica 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. Tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida.

El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias.

La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación. Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales.

La Agencia Española de Protección de datos ha publicado una Guía para la notificación de brechas de datos personales.

Deber de información

El responsable del tratamiento debe informar a las personas interesadas sobre las circunstancias relativas al tratamiento de sus datos. Esta información se debe poner a disposición de los interesados en el momento en que se recopilan sus datos, previamente a la recogida o registro.

Se debe informar sobre responsable del tratamiento, finalidad del tratamiento, legitimación, derechos de las personas interesadas, procedencia d ellos datos, etc.

Se recomienda dar la información por capas:

1) Primera capa. Información básica, de resumida, en el mismo momento y en el mismo medio en el que se recojan los datos. Se remite a la información adicional en un segundo nivel. La forma de presentación preferente es en forma de tabla, debe presentarte como “Información básica sobre protección de datos”.
2) Segunda capa. La información que se presente en la segunda capa ha de completar con todos los detalles la información resumida, así como añadir información adicional, requerida por el RGPD y que no estaba presente en la primera capa.

La AEPD ha publicado una Guía para el cumplimiento del deber de informar.

Delegado de Protección de Datos (DPD/DPO)

Es obligatorio para el responsable y el encargado cuando las actividades de tratamiento requieren una observación habitual y sistemática de personas a gran escala, cuando se realicen tratamientos a gran escala de categorías especiales de datos y cuando lo exija el derecho de la UE o de los Estados. Fuera de estos casos, es opcional.

El delegado de protección de datos: podrá formar parte de la plantilla o ser externo, puede ser una persona física o jurídica, y debe tener conocimientos especializados en Derecho, práctica en protección de datos y capacidad para desempeñar funciones.

Se deben publicar sus datos de contacto y comunicarlos a la AEPD.
Sus funciones son:

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

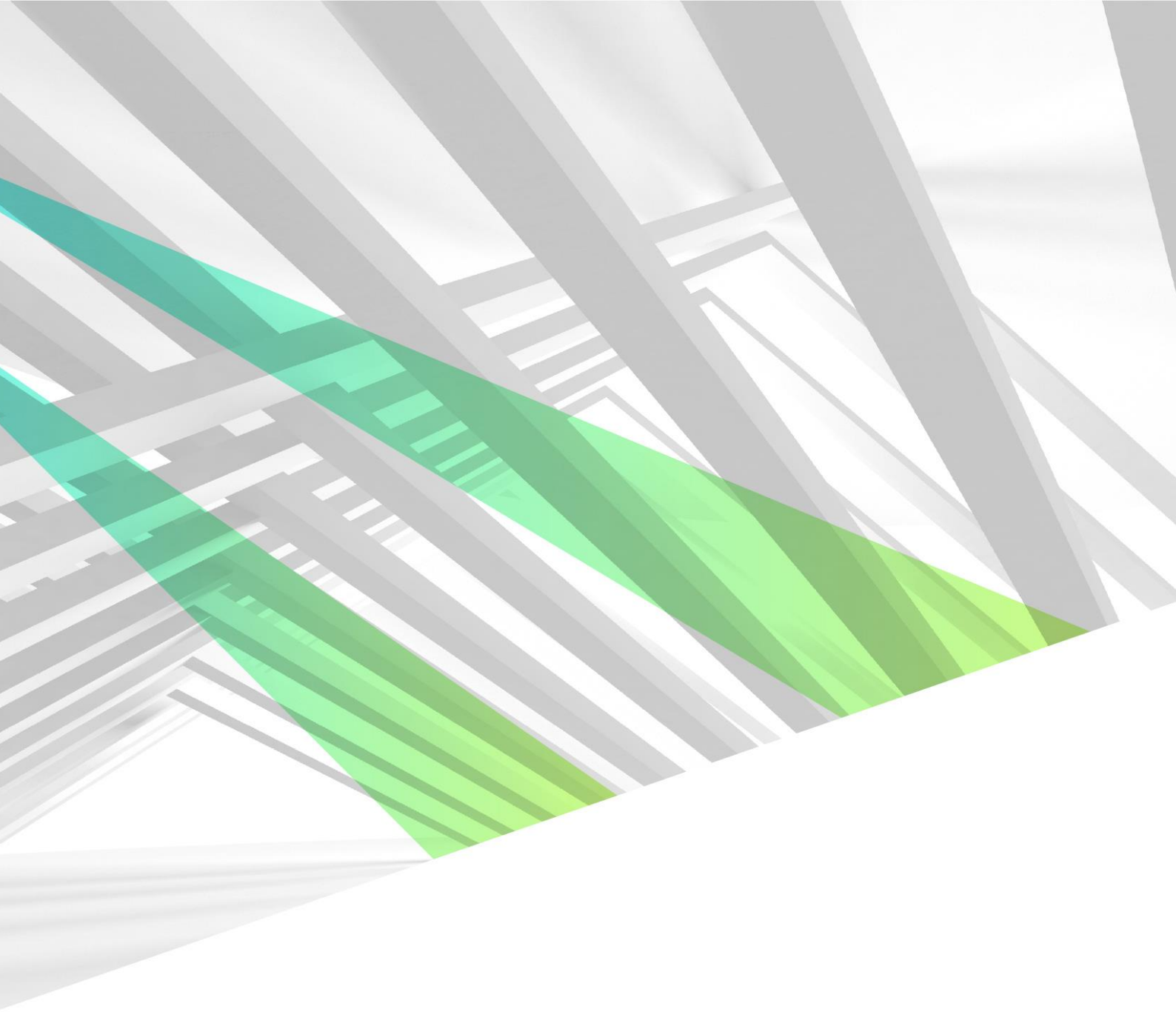
en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

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.



acens
Part of Telefónica Tech

Telefónica Empresas