REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

D. Rafael Hidalgo Romero
Presidente del Colegio Oficial de Graduados Sociales de Sevilla

Dª. Ana Gómez Hernández
Presidenta de ASNALA

D. Federico Martínez Martín
Director Zona Sur Mass Market|Asesorías, Wolters Kluwer

Wolters Kluwer

COLEGIO OFICIAL DE GRADUADOS SOCIALES DE SEVILLA

asnala
Asociación Nacional de Laboralistas

GRUPO A3 SATEL

REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

Dª. Eva Mª. Blázquez Agudo

Profesora Titular de Derecho del Trabajo y de la Seguridad Social

Universidad Carlos III

SOLUCIONES WOLTERS KLUWER PARA GESTIONAR EL RGPD

D. Felipe Fernández Cantalejo

Director Comercial Andalucía Occidental

A3Satel

Wolters Kluwer

COLEGIO OFICIAL DE GRADUADOS SOCIALES DE SEVILLA

asnal6 Asociación Nacional de Laboralistas

GRUPO A3 SATEL

Wolters Kluwer
COLEGIO OFICIAL DE GRADUADOS SOCIALES DE SEVILLA
asnala
Asociación Nacional de Laboralistas
GRUPO A3 SATEL

Nuevo Reglamento de Protección de Datos

Eva M. Blázquez Agudo

13/06/2018

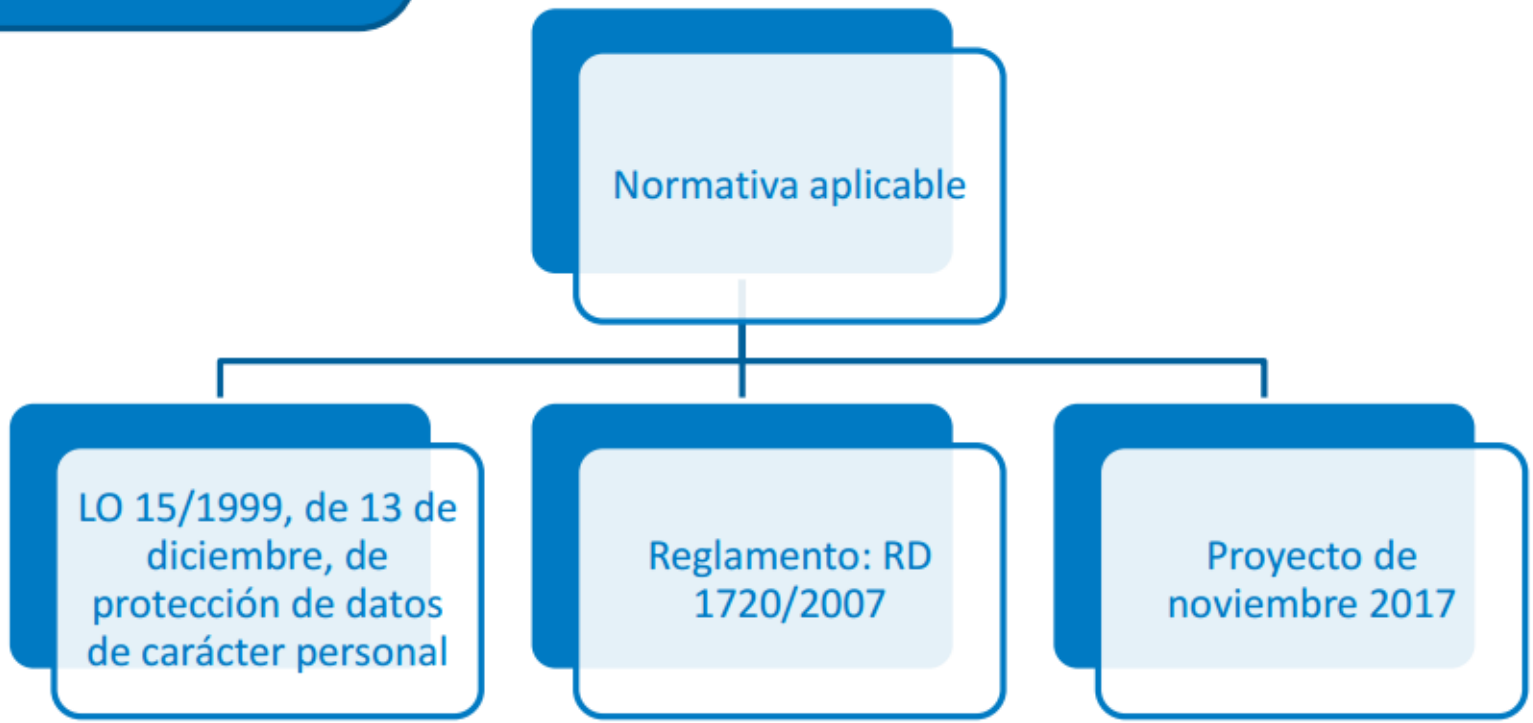
Wolters Kluwer

COLEGIO OFICIAL DE GRADUADOS SOCIALES DE SEVILLA

asnal6 Asociación Nacional de Laboralistas

GRUPO A3 SATEL

Reglamento Europeo de Protección de Datos
(entra en vigor en mayo 2018)



RGPD

¿Debe el legislador plantearse establecer norma concreta?

Aplicación directa

Exposición de motivos y articulado: duplicidad

Estados miembros pueden complementar ciertas cuestiones

ELEMENTOS BÁSICOS DE LA PROTECCIÓN DE DATOS

CONCEPTO Dato personal

Definición

- Cualquier información correspondientes a las personas físicas
- Donde quedan identificadas o identificables

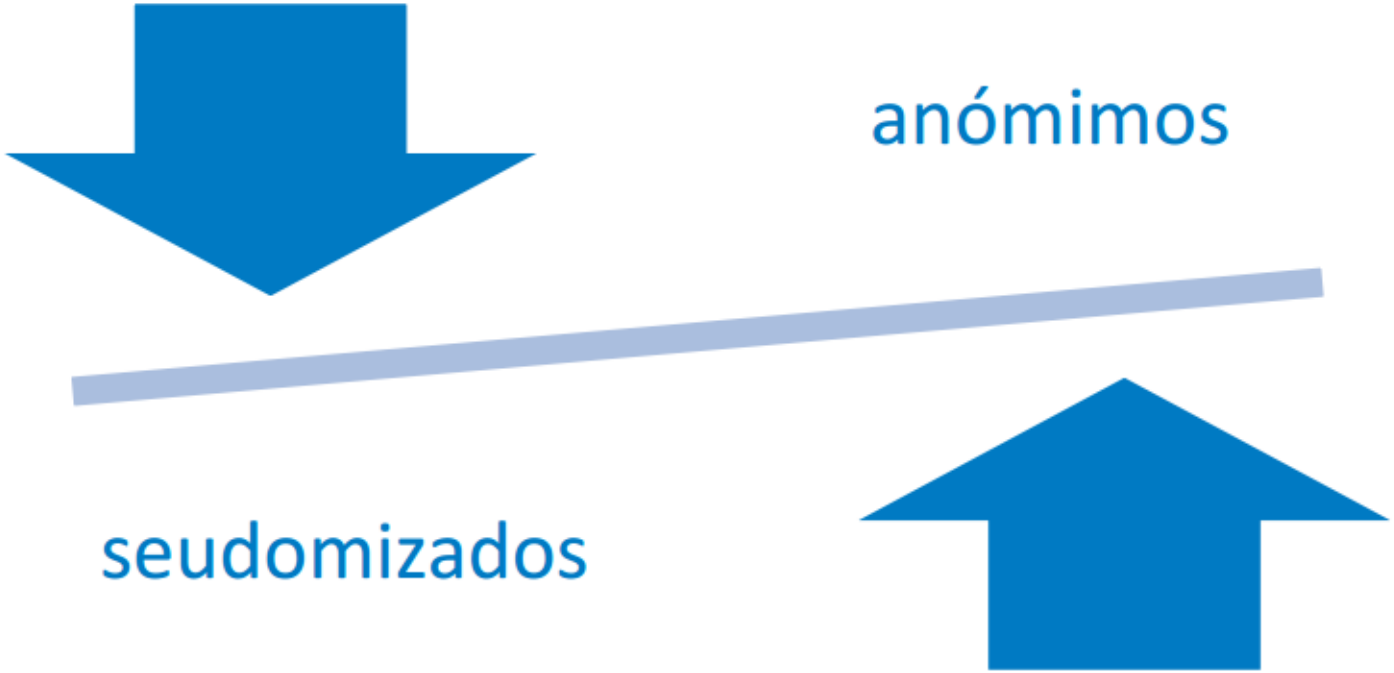
Tipos

- Información numérica, alfabética, gráfica, fotográfica, acústica

Exclusión expresa

- Simple relación de datos donde nombre, apellidos, puestos de trabajo, teléfono, fax y dirección postal o mail

Hacia los datos seudomizados



Seudonimización: medida de seguridad

La técnica de la seudonimización: sustitución de un atributo por otro en un registro, lo que lleva a dificultar su identificación, pero sin garantizar que se trata de datos anónimos.

RGPD se aplica, ya que hay posibilidad de identificar a una persona, cuando se ponen en relación con otros.

Valorar medios que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física; así como los costes y el tiempo necesarios para tal identificación,

Lo más adecuado parece ser mantener las dos variables de forma separada, es decir, que los datos seudonimizados no se pongan en contacto con la información adicional que puede llevar a la identificación de las personas.

Los datos personales de categorías especiales

¿Cuáles son?

- Datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, así como 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.

Con consentimiento expreso del interesado

- Se pueden tratar los datos genéticos y datos biométricos, datos relativos a la salud o datos relativos a la vida sexual de una persona física.
- El RGPD: cada país de incluir nuevas condiciones a los efectos de tratar dichos datos genéticos, biométricos o relativos a la salud.
- Nunca se podrá tratar, aún con consentimiento: datos tengan como finalidad identificar ideología, afiliación sindical, religión, orientación sexual o creencias y origen racial o étnico.

Otras opciones de licitud de tratamiento

- Cuando sea 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

Principios aplicables

- Principios de licitud y transparencia
- Principio de minimización del dato
- Principio de la limitación de la finalidad del tratamiento
- Principio de la exactitud de los datos, que se vincula al derecho de los interesados de rectificación
- Principio de la limitación de la conservación de los datos recogidos
- Principio de la integridad y confidencialidad
- Principio de la responsabilidad proactiva

Los límites territoriales de aplicación del RGPD

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.

- Establecimiento; implica el ejercicio efectivo y real de una actividad mediante una instalación estable, pudiendo adoptar la forma de simple sucursal o empresa filial
- Así, cualquier centro de trabajo que se encuentre situada en la Unión Europea.
- Todo ello matizado con la determinación de dónde se encuentra el establecimiento principal dentro de la Unión Europea a los efectos de determinar quién es la autoridad de control y qué norma supletoriamente se aplica.

Tratamiento de datos personales de interesados que residan en la Unión, aunque el responsable o encargado no se encuentre en la Unión, cuando las actividades de tratamiento estén relacionadas con:

- a) La oferta de bienes o servicios a dichos interesados en la Unión
- b) El control de su comportamiento, en la medida en que este tenga lugar en la Unión.

Trasferencia de datos a terceros países I (reglas RGPD + acuerdos internacionales)

Principio general de transferencia:

- Solo si el responsable y encargado del tratamiento cumplen todas las condiciones señaladas en el propio Reglamento
- País de trasferencia tiene que tener un nivel de protección adecuado, (evaluación cada 4 años).

Trasferencia de datos a terceros países II (reglas RGPD + acuerdos internacionales)

En caso de que no exista evaluación, posible el envío de los datos si el encargado o responsable del tratamiento ofrece garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas

Situaciones excepcionales (sin evaluación, ni garantías)

- Cuando transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento
- Cuando sea necesaria para la ejecución de medidas precontractuales adoptadas a solicitud del interesado
- Cando 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.

EL CONSENTIMIENTO DE LOS INTERESADOS

Licitud del tratamiento

En general

- Necesario consentimiento de titular de datos personales para su tratamiento

Excepciones

Principio de finalidad de recogida de datos en la empresa

Finalidad justificada	Cancelación	No posible para finalidades incompatibles
• Finalidad determinada • Manifestarse de forma concreta	• Se deben cancelar cuando han dejado de ser necesarios para la finalidad señalada	• ¿Finalidad distinta? • Relación contrato de trabajo • Casualidad

Notas del consentimiento

Declaración o clara acción afirmativa del afectado.

No se admiten consentimientos por omisión, ni tácitos.

Consentimiento positivo con base en principio de trasparencia

Manifestación de voluntad libre, específica, informada e inequívoca de aceptación del tratamiento

Posibilidad de revocación en cualquier momento

El consentimiento debe darse para todas las actividades de tratamiento realizadas con mismos fines. No es válido para fines incompatibles

(valoración posterior por responsable del tratamiento)

Tratamientos sin necesidad de consentimiento (I)

Por protección de intereses vitales del interesado o de otra persona física.

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,

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,

Interesado no esté capacitado, física o jurídicamente, para dar su consentimiento.

Ámbito actividades a fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, sobre tratamiento sobre miembros actuales o antiguos de tales organismos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos.

Tratamientos sin necesidad de consentimiento (II)

Datos personales que el interesado ha hecho manifiestamente público

Cuando es necesario por razones de un interés público esencial

Cuando es preciso para fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

g)Cuando el tratamiento sea necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial.

g)Cuando el tratamiento se refiera a datos personales que el interesado ha hecho manifiestamente públicos.

g)Cuando se justifique por razones de interés público o salud pública.

LOS SUJETOS DE LA PROTECCIÓN DE DATOS

Responsable y encargado del tratamiento (Deber de secreto y seguridad)

Responsable tratamiento

- Personas física o jurídica que decide sobre finalidad, contenido y uso del tratamiento
- No es necesario que realice el tratamiento de datos
- Ámbito laboral: generalmente el empresario o representante
- Nueva obligación Reglamento Europeo: Evaluación del impacto de operaciones de tratamiento de los datos en supuestos de alto riesgo sobre los derechos y libertades de las personas físicas. Esta obligación se relaciona con la utilización de nuevas tecnologías

Encargado de tratamiento

- Persona física o jurídica que trata los datos personales por cuenta del responsable
- En muchas ocasiones, se realizan por entes especializados. Externalización (responsabilidades concretas y en concreto establecer ciertos elementos en contrato).

Encargado del tratamiento de datos

Puede tener carácter remunerado o no /Puedes ser temporal o indefinido.

a) Persona concreta de la propia empresa que desarrolla estas actividades de acuerdo con su prestación definida en su contrato laboral

b) Externalizar estas funciones mediante la contratación de un tercero especializado en dicho servicios

- En este supuesto el responsable del fichero debe verificar el cumplimiento de toda la normativa relativa a la protección de datos en la actividad del encargado.
- El Reglamento Europeo impone la obligación de la existencia de un contrato entre el responsable y el encargado (se impone unos elementos mínimos en contratación).
- No se aplican normas de acceso a los datos de terceros (no necesario consentimiento expreso)
- No puede subcontratar a la vez con un tercero la realización de sus funciones, salvo que le hubiera autorizado el responsable del fichero.
- Normas subcontratación. Debe ser autorizada por responsable

Nueva figura en reglamento: el delegado de protección de datos

Debe ser nombrado por el responsable y el encargado de tratamiento

Solo obligatorio en ciertos supuestos: ej. en el ámbito de la empresa, si involucrados un gran número de trabajadores

Posible que sea alguien de la propia empresa y, si se trata de un grupo de empresas, puede organizar las actividades una misma persona

Funciones : asesoramiento y supervisión del control de todos los elementos de la protección de datos.

Ser el enlace con la autoridad de control

OBLIGACIONES

LA OBLIGACIÓN DE REGISTRO INTERNO

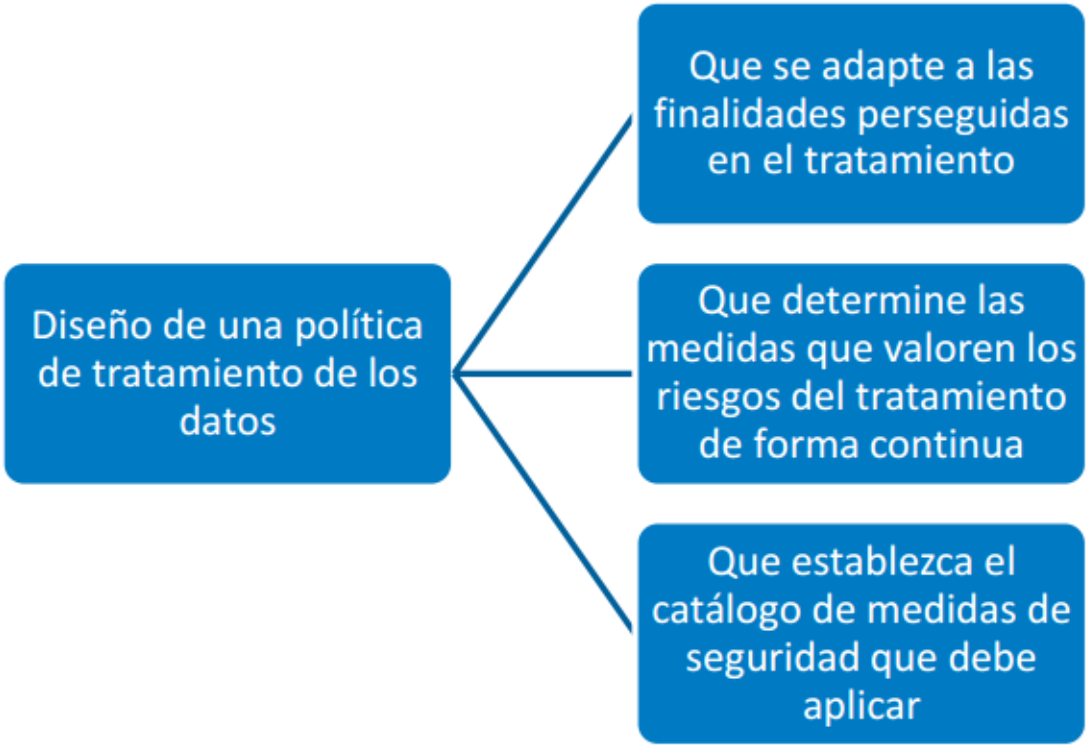
Obligación de dos registros internos:

- Cada responsable llevará un registro de las actividades de tratamiento efectuadas bajo su responsabilidad.
- 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.
- Así, hay una doble actividad de registro: uno sobre las actividades y otro sobre las categorías de actividades.

Obligados todas las empresas

- Excepción: empresas de menos de 250 trabajadores.
- Una excepción a la excepción, si será preciso el registro cuando el tratamiento que realicen pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional o incluya categorías especiales de datos o datos relativos a condenas e infracciones penales.

La nueva responsabilidad proactiva: desde la pasividad a la actividad



Complemento de la responsabilidad proactiva

La evaluación previa del impacto del tratamiento (EIPD) como un deber continuo de reevaluación

- Cuando queden implicado derechos fundamentales y libertades de las personas en el desarrollo del tratamiento de datos personales.
- Cuando se trata muchos datos personales de categorías especiales

Mecanismos de certificación

3.Adhesión a códigos de conducta

3.Medidas de seguridad desde el análisis del riesgo

- 3.Violación de las normas de seguridad

DERECHOS DE LOS INTERESADOS

Características de la información por capas

- Información precisa, expresa e inequívoca
- Existencia de fichero o tratamiento
- Finalidad de recogida datos
- Destinatarios de la información
- Consecuencia de obtención de datos
- Derechos de acceso, rectificación, oposición y cancelación
- Responsable del tratamiento o representante
- BASTA CON TENERLA A SU DISPOSICIÓN (principio trasparencia)

Derechos de los interesados

Derecho de acceso, rectificación, oposición y cancelación a los datos

Deben tener a su disposición impresos informativos (o posibilidad de imprimirlos): obligación del responsable del fichero

Derecho a la portabilidad

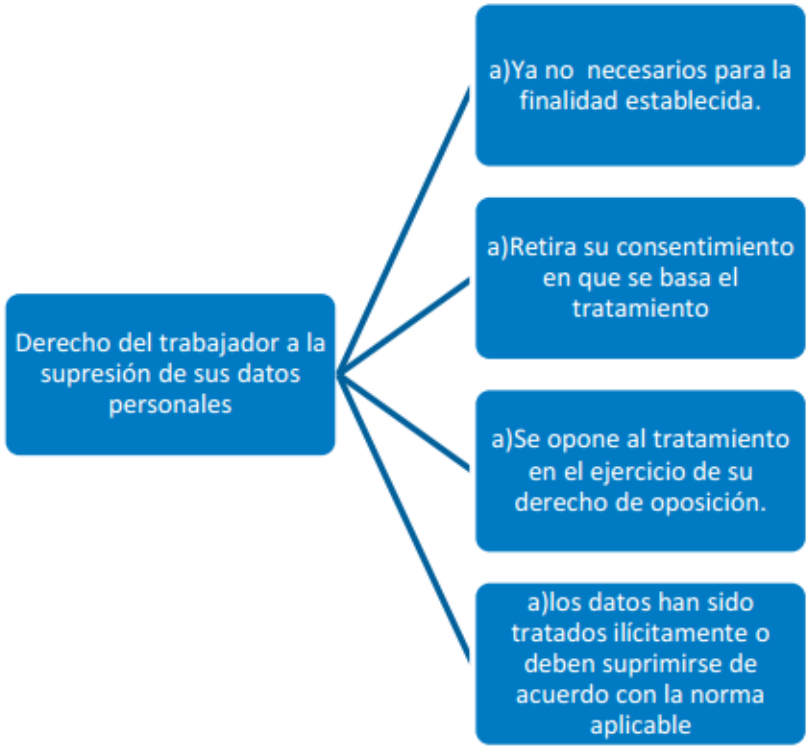
¿En qué consiste?

- Derecho a recibir los datos personales que le incumban, en un formato estructurado, de uso común y lectura mecánica,
- Y transmitirlos a otro responsable del tratamiento.

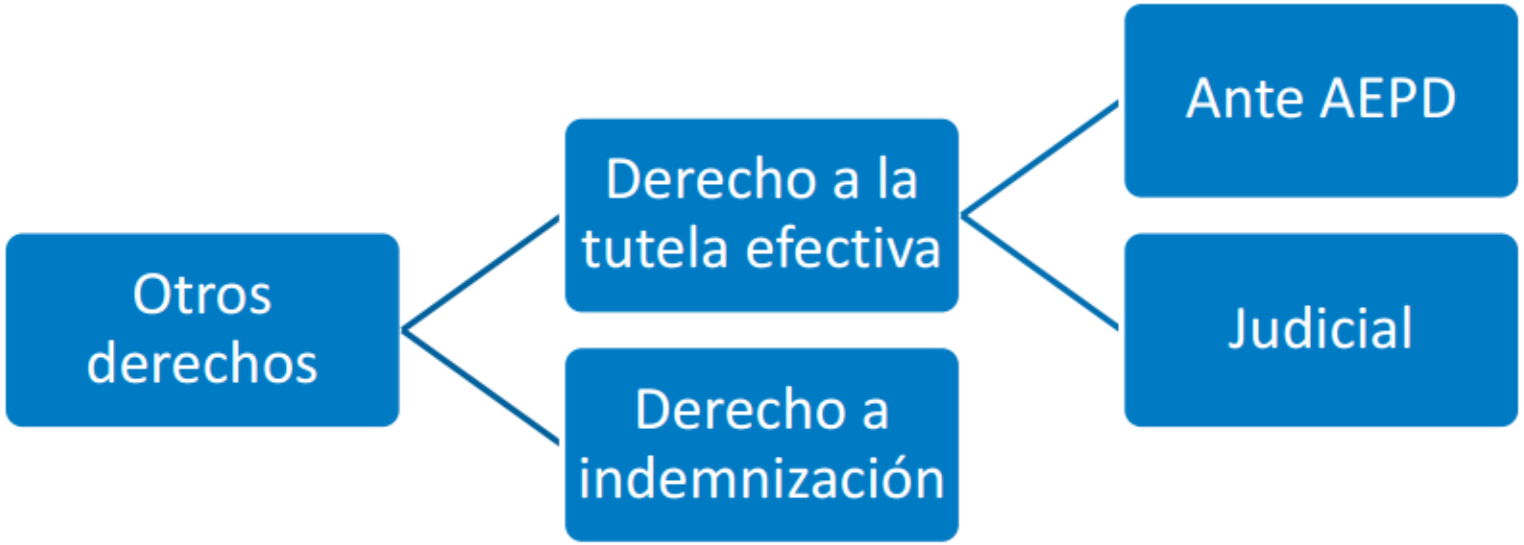
¿Cuándo se puede ejercitar el derecho?

- Sobre datos que el interesado haya facilitado a un responsable del tratamiento,
- Siempre que se encuentren estructurados a través de sistemas interoperable, aunque no necesariamente compatibles.

Derecho de supresión



Otros derechos



Régimen sancionador más duro

Las siguientes infracciones se sancionarán con multas administrativas de diez millones de euros 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:

- En relación a las obligaciones del responsable y del encargado a tenor de los artículos 8 (consentimiento de menores), 11 (cuestiones relativas a datos personales sobre condenas e infracciones penales, 25 a 39 (políticas de diseño, registro de actividades, medidas de seguridad y, en general, las obligaciones de los responsables, encargados y DPD) 42 y 43 (cuestiones relativas a certificaciones)

Las sanciones se podrán aumentar hasta veinte millones de euros, o tratándose de una empresa, una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

- Infracciones del responsable y del encargado relativas al incumplimiento de los principios básicos para el tratamiento; los derechos de los interesados y la trasferencia de datos a un destinatario de un tercer país