

REGLAMENTO EUROPEO DE PROTECCION DE DATOS

El 10 de noviembre de 2017 el Consejo de Ministros aprobó la remisión a las Cortes Generales el Proyecto de Ley Orgánica de Protección de Datos.

La razón fue que el Reglamento General de Protección de Datos (RGPD) había entrado en vigor en mayo de 2016 y **será aplicable a partir del 25 de mayo de 2018, por ello** hasta ese día, continúa vigente la LOPD de 1999 y su reglamento.

Al ser un "Reglamento de la Unión Europea", no necesita trasposición a la normativa nacional, se aplica directamente en toda la Unión Europea, por ello a partir del 24 de mayo del 2018 las empresas e instituciones deberán realizar un análisis de riesgo de sus tratamientos de datos personales y planificar su establecimiento.

Novedades de la nueva legislación

La figura más novedosa es la del Delegado de Protección de Datos (DPD) con el que deberán contar muchas empresas e instituciones, también se regula el derecho al olvido, el registro de las actividades de tratamiento, la información a los interesados de las violaciones de seguridad, la responsabilidad proactiva o el principio de portabilidad es lo más significativo.

Delegado de Protección de Datos



Es una nueva figura, especialista en derecho de protección de datos, que informa y asesora, figura que se crea al lado del responsable y del encargado del tratamiento.

No están obligados a tener delegado de protección de datos, empresas como las PYMES y otras cuya actividad no consista en el tratamiento masivo de datos personales que estén especialmente protegidos.

Esta figura la vemos en instituciones hospitalarias.

Aplicación en Empresas u organizaciones

Las pequeñas empresas y profesionales, actúan como **responsables y encargados del tratamiento** de datos personales, no necesitan el Delegado de Protección de Datos, pero si el resto de novedades que a continuación desgranaremos. **Si los Colegios Profesionales.**

La información al interesado y derechos

El responsable del tratamiento informará al interesado en el momento de solicitar los datos sobre:

- la identidad datos del **responsable**
- identificar la **base legal** (legitimación) y los fines del tratamiento
- el **plazo durante el cual se conservarán los datos**
- también sobre el **derecho a presentar una reclamación ante la autoridad de control.**
- derechos de **acceder, rectificar y suprimir los datos**

La **información debe ser concisa, transparente, inteligible y de fácil acceso, con lenguaje claro y sencillo.** La información se facilitará por escrito y si procede por medios electrónicos (art. 12).



La información deberá facilitarse cuando se obtengan del interesado (arts. 13 y 14).

Modo de obtener el consentimiento

El consentimiento debe ser **"inequívoco"**, deberá ser realizado con un lenguaje sencillo y claro, de forma concisa, transparente, inteligible. El consentimiento debe ser verificable.

Consentimiento de menores

Los menores podrán dar su consentimiento a partir de los 13 años, en la actualidad la LOPD señala los 14 años (art. 8.1).

Responsabilidad proactiva

El principio de responsabilidad proactiva significa que el responsable del tratamiento aplicará las medidas técnicas y organizativas (documentando el tratamiento de datos).

Las empresas (los Colegios Profesionales) deben adoptar medidas que aseguren razonablemente que están en condiciones de cumplir con los principios, derechos y garantías que establece el Reglamento sobre la **protección de datos por defecto**, diseñando medidas para garantizar se traten únicamente los datos necesarios para el fin específico del tratamiento, mantenimiento un registro de tratamientos, realización de evaluaciones de impacto sobre la protección de datos, nombramiento, si procede, de un Delegado de Protección de Datos (DPD) con las funciones de informar, asesorar, supervisar y cooperar actuando como punto de contacto con la autoridad de control (art. 39).

Medidas de seguridad



El RGPD señala que los responsables y encargados establecerán las medidas técnico organizativas apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos detectados en el análisis previo, por lo que **desaparecen los tres niveles de cumplimentación (básico, medio y alto)**, ya que con el nuevo Reglamento se señala que deberá realizarse un análisis del riesgo y *"...se aplicarán medidas técnico y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo"*.

Notificación de "quiebras" en seguridad

Notificación a la AEPD y al interesado de aquellas brechas de seguridad que se produzcan, o sea en situaciones de riesgo, por ejemplo la pérdida de un ordenador portátil, borrado accidental de algunos registros. En estos casos se deberá notificar a los afectados para que puedan tomar medidas.

Desaparece la obligación de registrar los ficheros a la AEPD

Si bien deberán tener un Registro interno de actividades de tratamiento las empresas con más de 250 empleados y quienes realicen tratamientos que puedan entrañar riesgos para los derechos y libertades de las personas.

Los responsables y encargados del tratamiento que los realicen habitualmente o sistemáticamente, deberán llevar con carácter interno un inventario o registro de tratamientos.

El tratamiento de datos sobre el origen étnico, religión, afiliación sindical, datos genéticos,



biométricos, datos relativos a la salud y orientación sexual

El art. 9 del Reglamento señala la prohibición del tratamiento de los datos señalados a excepción que el tratamiento sea necesario para la defensa de reclamaciones y cuando lo sean para finalidades médicas: por ejemplo la evaluación de la capacidad laboral, el diagnóstico médico, la prestación de asistencia sanitaria y social o en virtud de un contrato profesional sanitario de acuerdo con el apartado 3 del mismo artículo que se refiere al profesional sujeto al deber de secreto profesional.

Otros derechos

Derecho de **acceso** (art. 15). Facilitados al informar

Derecho de **rectificación** (art. 16). Facilitados al informar

Derecho a la **supresión** y **Derecho al olvido** (art. 17) y obtener de los responsables del tratamiento que los datos personales sean suprimidos cuando no sean necesarios para la finalidad con la que fueron recogidos.

Derecho a la **portabilidad** (art. 20)

Derecho de **oposición** (art. 21)

Las Evaluaciones del Impacto de Protección de Datos (EIPD)

La obligación de realizar evaluaciones del impacto será cuando se utilicen nuevas tecnologías que entrañen riesgo.

Consideraciones de los profesionales sanitarios

Información de datos personales

-es una cesión consentida, por ejemplo cuando el paciente autoriza al facultativo a informar a la familia de su situación médica.



-en ocasiones se da una colisión de derechos, por ejemplo cuando el facultativo revela el secreto de una enfermedad infecciosa contagiosa a la familia, contra la opinión del paciente (es un derecho preferente, de mayor valor social)

La Historia Clínica

Los facultativos como responsables de protección de datos deben cuidar

- consentimiento a su apertura y datos personales de salud
- los accesos deben quedar registrados
- el ordenado debe quedar cerrado al finalizar los registros
- no enviar datos de salud por correo electrónico
- destrucción de documentos con datos personales
- cierre con llave de los armarios con documentación clínica
- no dejar a la vista las historias clínicas

Col·legi Oficial de Podòlegs

Listas Robinson

Son listas de exclusión publicitaria, conocidas como Listas Robinson, creadas para tratar el acoso publicitario mediante SPAM

Gabinet Jurídic

Col·legi de Podòlegs