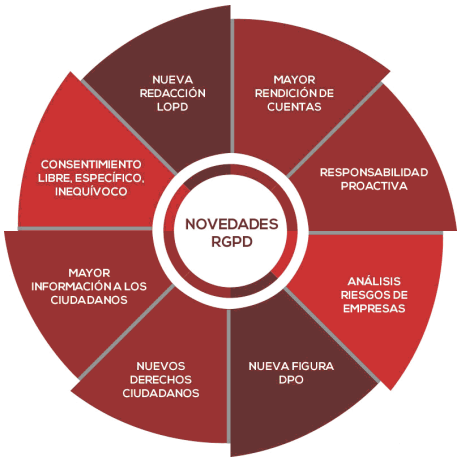
Principales modificaciones con el nuevo Reglamento Europeo de Protección de Datos



¿Qué empresas estarán obligadas a cumplir con el RGPD?

Este Reglamento se aplica todas aquellas **entidades** que traten datos de carácter personal que se encuentren dentro de la Unión Europea.

También se aplicaran a **responsables y encargados** no establecidos en la UE siempre que traten datos como consecuencia de una oferta de bienes o servicios destinados a **ciudadanos de la Unión.**

Nuevas obligaciones

Este Reglamento supone un mayor compromiso de las empresas y organizaciones con la Protección de Datos.

Rendición de cuentas

Se amplia la información que se les debe dar a los interesados en relación con el tratamiento de sus datos así como a sus derechos en esta materia.

Se incorpora el concepto de **privacidad desde el diseño**, lo cual se traduce en que la elaboración de los procedimientos empresariales se tiene que realizar teniendo en cuenta la protección de datos desde un primer momento.

Notificación de violaciones de seguridad

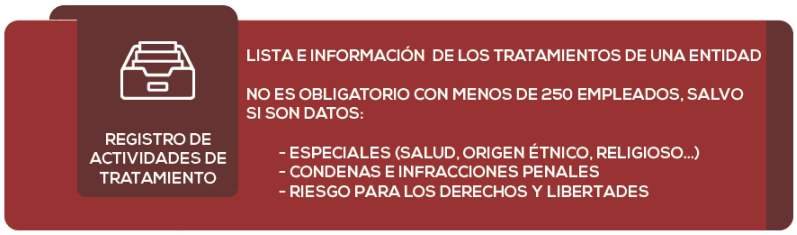
La nueva normativa exige que las violaciones en la seguridad que puedan afectar a los datos personales sean notificadas en un plazo máximo de **72 horas** a la Autoridad de Control correspondiente (Agencia Española de Protección de Datos).

Si además si en esa violación se pueden ver afectado datos de carácter sensible y con gran repercusión a los afectados, también se lo deberá notificar a estos mismos.

Registro de las actividades de tratamiento

La nueva normativa, elimina la obligación de registrar los ficheros ante la Autoridad de Control correspondiente.

No obstante obliga a llevar un registro interno de todos los tratamientos de datos personales que lleva a cabo la entidad, siempre que esta tenga **más de 250 empleados** o cuando se traten, no de forma ocasional, **datos sensibles**.



Responsabilidad proactiva

También llamado Accountability.

Esta responsabilidad activa se refiere a la necesidad de **prevención** por parte de las organizaciones que manejan datos personales.

Las empresas y entidades deben adoptar medidas que garanticen de manera suficiente que están en condiciones de cumplir con las reglas, derechos y garantías que el Reglamento establece.

El RGPD entiende que actuar únicamente cuando ya ha tenido lugar la infracción no es suficiente como estrategia, debido a que esa infracción puede ocasionar daños a los interesados que puede ser muy complicado compensar o reparar.

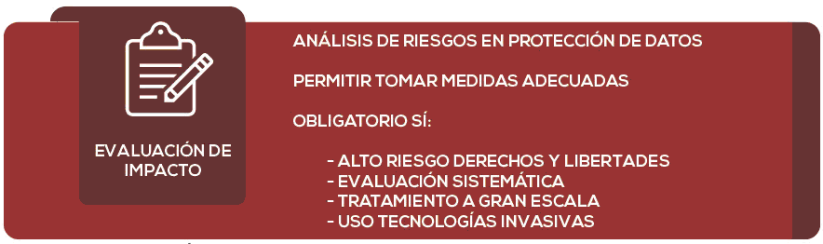
Para ello todas las organizaciones que tratan datos deben efectuar un **análisis de riesgo** de sus tratamientos para poder establecer **qué medidas han de aplicar y cómo hacerlo.**

Estos análisis pueden ser procedimientos sencillos en entidades que no llevan a cabo más que unos pocos tratamientos elementales que no supongan, por ejemplo, datos especialmente protegidos, o trabajos más complejos, en entidades que desarrollen muchos tratamientos, que afecten a gran número de personas o que por sus características requieren de una valoración cuidadosa de sus riesgos.

Un caso especial : Evaluación de impacto de protección de datos

Las Evaluaciones de Impacto son la principal medida de responsabilidad proactiva.

Se trata de un análisis de los riesgos previos que puede acarrear un determinado sistema de información, producto o servicio al derecho a la protección de datos.



Delegado de Protección de Datos

Se trata de una nueva figura de responsabilidad dentro de la entidad.

El DPO, se encargará de la planificación de las medidas de seguridad aplicables a los tratamientos de datos. así como la gestión de los mismos.

Hay que destacar que servirá de enlace entre la empresa y la autoridad de control.

Solo será obligatorio en determinados casos, los cuales encontremos regulados en la nueva LOPD cuando está definitivamente se apruebe.

¿Qué es el Delegado de Protección de Datos?

Una de las principales novedades que implica el Reglamento es la creación de la figura del Delegado de Protección de Datos (*data protection officer*).

El DPO, es en gran medida, la persona encargada informar a la entidad responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos.

También por tanto deberá velar o supervisar el cumplimiento normativo así como de cooperar con la autoridad de control y actuar como punto de contacto entre ésta y la entidad responsable del tratamiento de datos.

Por lo tanto esta claro que la nueva normativa convierte al DPO en una figura muy importante para la empresa.

En consecuencia, para el buen desarrollo de sus funciones (de las cuales hablaremos en el siguiente apartado) se le deberá dotar de los recursos necesarios para llevar a cabo su trabajo con plenas garantías y la suficiente estabilidad.

Se debe destacar también que los **datos de contacto deben ser públicos**, para que interesados y supervisores puedan contactar con él de manera directa y confidencial.

Funciones del DPO

A continuación describo cual es el **objetivo del Delegado de Protección de Datos** son:

Asesoramiento

- Debe informar y asesorar al responsable o al encargado del tratamiento de las obligaciones normativas en protección de datos que les incumban.
- Tiene que asesorar tanto al responsable como al encargado acerca de la evaluación de impacto que realice relativa a la protección de datos.
- Asesorar a los empleados durante el tratamiento de datos.

Supervisión del cumplimiento normativo

- Supervisar el adecuado cumplimiento de las normas sobre protección de datos en la entidad.
- Revisar las políticas internas de privacidad en la organización y su adecuación normativa.
- Asignar responsabilidades entre los miembros de la organización, respecto a las obligaciones en materia de protección de datos.
- Realización de acciones de concienciación internas respecto al cumplimiento efectivo de la normativa.
- Formar al personal que participa en las operaciones de tratamiento de datos.
- Supervisar las evaluaciones de impacto en la protección de datos.
- Control, coordinación y verificación de las medidas de seguridad aplicables.

Cooperación y enlace con la autoridad de control

- Actuar como punto de contacto con la Agencia Española de Protección de Datos para las cuestiones relacionadas con el tratamiento de datos personales, incluyendo la consulta previa.
- Cooperar con la autoridad de control.

Atención a los interesados

- Atender las consultas que los interesados realicen a la entidad, ya sea para cuestiones relativas al tratamiento de sus datos o para el ejercicio de sus derechos.

¿Cuándo es obligatorio contar con un DPO?

No siempre es necesaria la figura de un delegado de protección de datos en nuestra organización.

El artículo 37 del RGPD fija la **obligatoriedad de su designación en estos casos**:

1. Cuando el tratamiento de los datos sea realizado por una autoridad o un organismo público.
2. Si as 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.
3. Si las actividades principales del responsable implican el tratamiento a gran escala de datos especiales o personales referidos a condenas o delitos.

Asimismo el Proyecto de Ley Orgánica de Protección de Datos, en su artículo 34, enumera una serie de entidades en las que será obligatoria la designación de un DPO:

Colegios profesionales

Un **colegio profesional** o **colegio oficial** es una asociación de carácter profesional o gremial integrada por quienes ejercen una profesión liberal y que suelen estar amparados por el Estado.

Centros docentes

Centros que ofrezcan **enseñanzas regladas** (infantil, educación primaria, educación secundaria, bachillerato, formación profesional, enseñanzas artísticas, enseñanzas de idiomas, enseñanzas deportivas, enseñanza de personas adultas y educación especial) y las Universidades públicas y privadas.

Prestadores de servicios de comunicaciones electrónicas

Aquí se incluyen las **compañías telefónicas** y los proveedores de acceso a Internet, siempre y cuando traten a gran escala perfiles.

Prestadores de servicios de la sociedad de la información

En este caso estaríamos hablando de una tienda online, una red social, etc, cuando **elaboren a gran escala perfiles** de los usuarios del servicio.

Entidades de crédito

Estamos hablando de entidades de crédito como los bancos, las cajas de ahorros, las cooperativas de crédito y el Instituto de Crédito Oficial.

Empresas de fomento de la financiación empresarial

Son aquellas empresas que, sin tener la consideración de entidad de crédito y previa autorización del Ministro de Economía y Competitividad, se dediquen con carácter profesional a la concesión de préstamos y créditos, el arrendamiento financiero o la concesión de avales y garantías.

Entidades aseguradoras

Una compañía de seguros o aseguradora es la empresa especializada en el seguro, cuya actividad económica consiste en producir el servicio de seguridad, cubriendo determinados riesgos económicos (riesgos asegurables) a las unidades económicas de producción y consumo.

Empresas de servicios de inversión

Son las que ofrecen **servicios de inversión bursátiles** y de fondos de ahorro.

Distribuidores y comercializadores de electricidad

En este caso no solo comprendemos a las compañías eléctricas, sino también a las entidades que venden al público esa electricidad.

Organizaciones que evalúan la solvencia patrimonial y crédito

Se incluyen los responsables de los ficheros regulados por la Ley de prevención del blanqueo de capitales y de la financiación del terrorismo.

Empresas de publicidad y prospección comercial

Se incluyen aquellas empresas que se dediquen al marketing elaborando perfiles del consumidor.

Centros sanitarios

En este caso incluimos diversos tipos de centros sanitarios, como hospitales, clínicas estéticas o clínicas dentales, las cuales se encuentra obligados a mantener la historia clínica del paciente.

Emisores de informes comerciales

Empresas cuya actividad principal es la aportación de informes relativos al comercio realizado por persona físicas.

Operadores de juego electrónico

En este caso incluimos a las entidades que ofrecen apuestas deportivas online, así como también juegos de casino.

Empresas de seguridad privada

Quienes desempeñen las actividades reguladas por el Título II de la Ley 5/2014, de 4 de abril, de Seguridad Privada.

Se incluyen en este caso empresas que proporcionan seguridad privada así como también los despachos de detectives privados.

¿Es necesario que estas entidades realicen un curso sobre DPO?

No.

Aunque en las entidades que acabamos de mencionar es obligatorio contar con un DPO, no es necesario que los empleados de la misma realicen cursos específicos de este figura, ya que como veremos en el siguiente apartado, el DPO puede ser externo.

No obstante, si decidimos que un empleado de la entidad debe ser el DPO, y este no cuenta con los requisitos formativos necesarios para que sea considerado dicho **nombramiento responsable**, deberá realizar un **itinerario formativo en una entidad acreditada por la AEPD**, a fin de cumplir los requisitos formativos para poder ejercer de DPO.

Perfil del Delegado de Protección de Datos

En el RGPD, en particular en el artículo 37, en sus puntos 5 y 6, establece que el DPO será designado o contratado según su capacidad para ejercer las atribuciones fijadas.

Por lo tanto para esa designación se deberán tener en cuenta sus cualidades profesionales y, concretamente, de sus **conocimientos en materia de Derecho y protección de datos**.

Ser jurista sería recomendable, no obstante no es obligatorio.

¿Que posición debe tener el DPO en mi empresa?

El DPO podrá ser interno o externo a la empresa.

El representante legal de una entidad, ¿puede ser nombrado DPO de la misma?

No, el representante legal de una entidad no puede ser nombrado DPO de la misma.

Uno de las principales características de DPO es su independencia.

Debe poder ejercer sus funciones sin ninguna limitación y, por supuesto, **sin conflicto de intereses**, que es lo que podría ocurrir si el representante fuera nombrado DPO

¿Siempre se deben cumplir los requisitos para ser nombrado DPO?

En lo casos en los que la empresa esté obligado a contar con uno, deberá cumplir con los requisitos que antes hemos mencionado.

En cambio, en los casos que, de forma voluntaria, se designe a un DPO sin estar obligada la entidad, si bien se regirá por el mismo régimen de independencia y de trabajo, los requisitos técnicos no deberán ser cumplidos, siempre y cuando este DPO voluntario cuente con asesoramiento externo específico en la materia.

El futuro de la Protección de Datos en España

A la vista de los cambios que se están produciendo en este sector como esta nueva normativa europea, nos planteamos cómo va a evolucionar la Protección de Datos en nuestro país.

GESFOR
Gestora de Formación