ESCURA

IMPLANTACIÓN NUEVO REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

¿Qué es el RGPD?

¿Por qué es obligatorio para las empresas?

Sanciones

La figura del Delegado de Protección de Datos

Metodología

Conclusiones

¿Qué normativas vienen?

1. **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 estos datos y por el que se deroga la Directiva 95/46/CE (**Reglamento General de Protección de Datos**).

2. **Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal.**

1. Reglamento General de Protección de Datos (RGPD)

- El Reglamento Europeo de Protección de Datos unifica y moderniza la normativa europea sobre protección de datos, permitiendo a los ciudadanos tener un mejor control de sus datos personales y a las empresas aprovechar al máximo las oportunidades de un mercado único digital.

- "Será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro **a partir del 25 de Mayo de 2018".**

¿Qué es el Reglamento General de Protección de Datos?

1. **Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal:**

   Se aprobó el 10 de noviembre de 2017 por el Consejo de Ministros y se aplicará a partir del 25 de mayo de 2018.

   Respeta en todo momento el Reglamento General de Protección de Datos y clarifica su contenido.

   Sustituirá la Ley Orgánica de Protección de Datos actual.

¿Qué cambia legalmente?

- Queda derogada la anterior Directiva Europea 95/46/CE.
- Queda derogada la Ley Orgánica 15/99 de Protección de Datos.
- Queda derogado el Real Decreto 1720/2007.
- Entra en vigor el Reglamento General de Protección de Datos UE 2016/679: **25 de Mayo de 2018.**
- No es necesario transponer (será igual en todos los países de la UE).

¿Qué cambia conceptualmente?

LOPD

- Consentimiento Tácito.
- 3 niveles: básico, medio, alto.
- Inscripción pública de ficheros.
- Regulación Externa.
- Medidas de Seguridad establecidas en el RD.
- 4 Derechos: Arco.

RGPD

- Consentimiento Expreso
- 2 niveles: especiales y no especiales.
- Registro Interno de Actividades
- Autorregulación.
- Medidas de Seguridad definidas por la empresa.
- 6 Derechos:

ARCO+olvido+portabilidad

¿Cómo se presta el consentimiento?

LOPD

- Manifestación de voluntad
- Tácito, Contrario o negativo, implícito
- Varios consentimientos en uno
- Silencio Positivo

RGPD

- Manifestación de voluntad expresa (inequívoco)
- No caben los consentimientos tácitos o presuntos
- Cada consentimiento por separado (Privacy by Design).
- Silencio Negativo (Privacy by Default)

¿Por qué es obligatorio para las empresas?

El art. 24 RGPD y art. 30. del Proyecto

- **Todas las empresas deberán nombrar a un Responsable de Protección de Datos**, quien, tras ponderar los riesgos que el tratamiento pueda generar en los derechos de los afectados y, en particular, en su derecho a la protección, se encargará de establecer las medidas técnicas y organizativas a fin de garantizar y poder demostrar que el tratamiento de datos es conforme a la normativa comunitaria.

Sanciones

Art. 45 LOPD

1.- Las infracciones leves serán sancionadas con multa de 900 a 40.000 euros.

2.- Las infracciones graves serán sancionadas con multa de 40.001 a 300.000 euros.

3.- Las infracciones muy graves serán sancionadas con multa de 300.001 a 600.000 euros

Art. 83 RGPD

1.- Multas administrativas de 10.000.000 EUR 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.

2.- Multas administrativas de 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.

¿Qué datos aparecen con el nuevo RGPD ?

En el **art. 9.1 del RGPD** aparece la figura de categoría de datos especiales que la define de la siguiente manera:

"Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y 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"*

¿Qué obligaciones aparecen según el tipo de datos?

Para la categoría de **datos especiales** aparecen las obligaciones de:

- Realización de una **Evaluación de Impacto (EIPD).**
- **Registro** de actividad.
- Nombramiento **Delegado de Protección de Datos.**

¿En qué consiste la Evaluación de Impacto?

Recogido en el **art. 35 del RGPD**, los responsables deberán realizar una EIPD antes de la puesta en macha de aquellos tratamientos que afecten a datos especiales y que puedan conllevar un alto riesgo para los interesados. Deberá realizarse cuando:

1. En base a los datos se generen perfiles sobre cuya base se tomen decisiones que produzcan efectos jurídicos.

2. Cuando se haga tratamientos a gran escala de datos sensibles.

3. Cuando exista observación sistemática a gran escala de una zona de acceso público.

4. Las autoridades de protección de datos están obligadas a confeccionar listas adicionales de tratamientos que requerirán una EIPD.

¿Qué es el Registro de actividad?

Lo encontramos en el **art. 30 del RGPD**:

- Sustituye a la anterior inscripción de ficheros públicos ante la Agencia Española de Protección de Datos.

- Se registra internamente en la empresa: "***Principio de Responsabilidad Proactiva***"

¿Qué contiene el Registro de actividad?

Debe contener:

- Nombre y datos de contacto de la empresa responsable
- Nombre y datos de contacto de encargados de tratamiento
- Nombre y datos del DPO
- Finalidades para las que se recogen los datos
- Categorías de interesados (relación de los titulares con la empresa)
- Tipos de datos (haciendo mención si son especiales)
- En su caso, transferencias internacionales
- Base legal (motivo por el que tengo los datos)
- Si son datos especiales, documentar evaluación de impacto para el titular.

¿Qué Medidas de Seguridad debe realizar la empresa?

El esquema de medidas de seguridad previsto en el RD 1720/2007 **NO seguirá siendo válido de forma automática.**

- Las medidas se deciden en base al resultado del análisis de riesgos.
- Deben ser aplicadas ANTES del inicio del tratamiento.
- Basadas en mejora continua.
- Las medidas técnicas y organizativas deberán establecerse teniendo en cuenta:

  1. El coste y estado de la técnica
  2. Los costes de aplicación
  3. La naturaleza, el alcance, el contexto y los fines del tratamiento.
  4. Los riesgos para los derechos y libertades de los afectados.

- Se configura como un Sistema de Gestión de la Privacidad basado en el auto aprendizaje y la mejora, lo que obliga al auto análisis del sistema (auditorías).

¿Qué es el Delegado de Protección Datos?

Se encuentra recogido en el **art. 37 del RGPD**:

"El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:

a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

b) las 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,

c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10".

¿Qué funciones tiene el Delegado de Protección Datos?

a) Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de los datos personales de las obligaciones que les incumben en virtud del Reglamento y otras disposiciones sobre protección de datos de la Unión o de los Estados miembros;

b) Supervisar el cumplimiento de lo dispuesto en el Reglamento, en otras disposiciones sobre 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;

¿Qué funciones tiene el Delegado de Protección Datos?

c) Ofrecer el asesoramiento que se le pida acerca de la evaluación de impacto relativa a la protección de datos y supervisar su realización;

d) Cooperar con la autoridad de control;

e) Actuar como punto de contacto de la autoridad de control para las cuestiones relacionadas con el tratamiento de datos personales incluida la consulta previa, y consultar en su caso, sobre cualquier otro asunto.

¿Qué requisitos tiene que tener el Delegado de Protección Datos?

a) Amplia experiencia y conocimiento de la materia y de la interpretación y adecuación práctica para aplicar la normativa sobre protección de datos, incluyendo medidas de seguridad en todos los procesos técnicos y administrativos y de desarrollo de la empresa.

b) Conocimiento concreto de la materia aplicados a los diferentes sectores.

c) Experiencia y capacidad para asistir a la razón social ante inspecciones, requerimientos de las autoridades competentes y cualquier tipo de consulta de los terceros afectados por el tratamiento de datos de la razón social.

d) Habilidades de negociación, formación y empatía para trabajar con representantes de trabajadores, y por supuesto con los propios trabajadores de la empresa.

Metodología

1- Nombramiento del RPD o del DPD.

- La empresa debe nombrar a un Responsable de Protección de Datos (RPD) o un Delegado de Protección de Datos (DPD), según o establecido en el artículo 37 RGPD.

2- Evaluación de riesgos

- El RPD o un DPD realizará una evaluación de riesgos y en su caso (datos especialmente protegidos) una evolución de impacto sobre los riesgos que puedan afectar a la empresa.

Metodología

3- Registro de actividad

- El El RPD o un DPD crea un registro de ficheros internos, junto con las medidas de seguridad necesarias para proteger a la empresa de los riesgos detectados.

4- Medidas de seguridad

- Una vez realizados los procedimientos anteriores, se recopila todo en un único Documento, que deberá regir el comportamiento de los miembros de la organización en materia de Protección de Datos.

Ejemplos de riesgos

Acceso ilícito a información confidencial
Robo físico de información digital o en papel
Envío de información confidencial a terceros sin autorización
Diseño insuficiente de medidas de seguridad
Cadena de custodia de contraseñas deficiente
Fuga accidental de información
Interceptación de documentación
Interceptación, accidental o no, de conversaciones
No cerrar una aplicación informática tras su uso
Divulgación de datos personales de clientes, trabajadores, proveedores…

Conclusiones

Todas las empresas deben cumplir con la norma comunitaria

Cualquier empresa debe elaborar y cumplir políticas adaptadas sobre protección de datos

El servicio que se ofrece debe adaptarse a las necesidades requeridas por la Ley

Deben analizarse los procesos sensibles y crear los programas organizativos adaptados a cada situación

Las fases para la implantación de las políticas de protección de datos se basan en una metodología y en la participación de la empresa

Las sanciones que se pueden imponer en caso de incumplimiento pueden llegar hasta el 4% de la facturación de la empresa