Información sobre implantación del Reglamento General de Protección de Datos Europeo (RGPD)

Índice

0. Introducción

Todas las **empresas necesitan recoger y tratar datos personales** para el ejercicio de su actividad diaria (de trabajadores, clientes, proveedores, contactos, etc.). Datos que son incorporados en los sistemas informáticos de la empresa.

Si los sistemas en los que se almacenan **datos personales**, son accedidos por alguien no autorizado o se pierde la información contenida en ellos, el **responsable** de esos sistemas se podría encontrar ante una **vulneración de la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD)**, que contempla **sanciones** de hasta **600.000 €**.

Por otra parte, el **25 de mayo de 2018** entra en aplicación el **Reglamento General de Protección de Datos** de Europa, cuyas sanciones ascienden hasta los **20.000.000 €,** si el responsable no ha protegido adecuadamente la seguridad de dichos datos o los ha tratado **sin seguir los principios y requisitos** marcados por la normativa.

Entre las **novedades más importantes** que incorpora el Reglamento General de Protección de Datos podemos destacar las siguientes:

- Se **amplía el deber de información** al interesado.
- Se **amplía** el contenido de los **contratos** de acceso a datos.
- Debe realizarse una **evaluación de riesgos** para determinar las medidas de seguridad que deben implantarse.
- Establece el principio de "**responsabilidad proactiva**", a través del cual, el responsable, además de cumplir, debe **poder demostrarlo**.
- Se deben **notificar las violaciones de la seg**uridad a la Agencia Española de Protección de Datos en el plazo máximo de 72 horas.

1. El Reglamento General de Protección de Datos de Europa

El Reglamento General de Protección de Datos de Europa (RGPD) **regula la recogida, uso, almacenamiento y destrucción de los datos personales.**

El RGPD es de **obligado cumplimiento** para todas las entidades públicas y privadas (empresas, asociaciones, comunidades de propietarios, etc.).

1.1. ¿Qué obligaciones establece el RGPD?

Existen tres momentos fundamentales en el tratamiento de los datos personales, con sus obligaciones legales específicas:

- **En la recogida de los datos:** se debe incluir la cláusula informativa detallando la entidad que recoge los datos, la finalidad de la recogida, la base jurídica para el tratamiento, los plazos de conservación de los datos, la existencia de decisiones automatizadas y su lógica, si existen transferencias de los datos a terceros países, indicando también cómo puede el titular de los datos ejercer los derechos de acceso, rectificación, supresión, limitación del tratamiento y portabilidad de los datos.

- **En el almacenamiento y uso de los datos:** se debe realizar una evaluación de los riesgos a que están sometidos los tratamientos de datos personales e implantar las medidas de seguridad necesarias para garantizar la integridad, confidencialidad y disponibilidad de los datos personales, en función de los riesgos detectados. Debe existir un Registro de Actividades de Tratamiento en el que se detallen los tratamientos de datos personales que se realizan y las medidas de seguridad que están implantadas para proteger dichos tratamientos.

- **En la destrucción:** se deben destruir de forma segura los datos, de forma que no sea posible la recuperación posterior de los mismos.

1.2. ¿Qué acciones debe realizar una entidad para adecuarse al RGPD?

Para adecuarse al RGPD, una entidad debe realizar las siguientes acciones:

1. Elaborar las **cláusulas legales** necesarias, **conforme al RGPD** (no sirven las existentes hasta ahora), para recoger los datos e incorporarlas en los formularios donde se recogen los datos (incluida web). En dichas cláusulas, la información debe proporcionarse en 2 capas.

2. **Realizar una evaluación de los riesgos** a que están sometidos los tratamientos de datos personales, así como una gestión de dichos riesgos para rebajarlos a niveles asumibles por la organización.

3. **Elaborar el Registro de Actividades de Tratamiento,** describiendo los datos que trata, los tratamientos que realiza y las medidas de seguridad que se implantan para preservar la seguridad de los mismos.

4. **Implantar las medidas de seguridad** recogidas en el Registro de Actividades de Tratamiento.

5. Elaborar y dar a firmar los **compromisos de confidencialidad y deber de secreto** a los trabajadores.

6. Elaborar y dar a firmar los **contratos de acceso a datos por cuenta de terceros, conforme al RGPD** (no sirven los existentes hasta ahora), a las entidades externas que acceden o pueden acceder a ellos para prestar un servicio (asesoría fiscal y laboral, mantenimiento informático, prevención, etc.).

7. Elaborar los **protocolos de atención** necesarios para atender correctamente los derechos de los interesados.

8. Elaborar los **protocolos de notificación** de las posibles **violaciones en la seguridad** a la **autoridad de control y a los interesados**.

9. Realizar, en caso de ser necesario, el **Análisis de Impacto relativo a la Protección de Datos** (EIPD) para aquellos tratamientos que lo requieran.

1.3. Qué se requiere para cumplir el RGPD

La documentación necesaria para cumplir los requisitos del RGPD es la siguiente:

- **Cláusulas legales** informativas para la recogida de los datos.
- **Contratos de acceso a datos** por cuenta de terceros.
- **Compromisos de confidencialidad** y deber de secreto para los trabajadores.
- **Evaluación de Riesgos.**
- **Registro de Actividades de Tratamiento.**
- **Evaluación de Impacto relativa a la Protección de Datos** (en su caso).
- **Protocolos para atención a los derechos de los interesados.**
- **Protocolos para la notificación de violaciones de la seguridad** a la Autoridad de Control y a los interesados.

Asimismo, es necesario también:

- **Implantar las medidas de seguridad** indicadas en el Registro de Actividades de Tratamiento.
- **Formar adecuadamente a los trabajadores que tratan datos personales.**

2. Nuestra empresa

Leasba Consulting es una empresa **especializada** en **ciberseguridad, seguridad de la información y protección de datos**. Cuenta con una gran experiencia, avalada por los más de **11 años** que lleva prestando servicio en estos ámbitos.

Aunque la **central** está establecida en **León**, damos **servicio a nivel nacional,** de forma directa o a través de acuerdos que tenemos con más de 500 profesionales.

Damos una **importancia fundamental** a la **formación** de nuestros profesionales, los cuales cuentan con las certificaciones más prestigiosas dentro de estos ámbitos (AENOR, EC-Council, APEP, etc.).

Leasba se encuentra registrada en el Catálogo de Empresa y Soluciones de Ciberseguridad de INCIBE, siendo también miembro de la Agrupación Empresarial Innovadora en Ciberseguridad y Tecnologías Avanzadas.

Servicios ofrecidos

Ofrecemos los servicios de **Consultoría**, **Auditoría** y **Formación** dentro de los siguientes ámbitos:

- **Ciberseguridad**
  - Análisis de riesgos
  - Securización de entornos
  - Análisis de vulnerabilidades
  - Pruebas de penetración (hacking ético)
  - Análisis forense de sistemas informáticos
- **Seguridad de la Información**
  - Copia de seguridad externa automatizada
  - Análisis de riesgos
  - Implantación de SGSI (ISO 27001)
  - Planes de continuidad de negocio
- **Protección de datos personales (LOPD) y LSSI**
  - Implantación y cumplimiento
  - Defensa jurídica
  - Software de gestión
  - Adecuación de web a la LSSICE

Consultoría | Auditoría | Formación

3. Confidencialidad y acceso a datos

Toda la información que obtengamos del cliente, **así como los resultados** parciales de cualquier parte del proceso, **permanecen protegidos bajo sistemas de almacenamiento seguro**.

Leasba Consulting firmará un Acuerdo de No Divulgación (NDA) entre las partes para garantizar la confidencialidad de la información involucrada y los hallazgos.

También se firmará un contrato acceso a datos por cuenta terceros para **regular**, **según establece la LOPD**, el posible acceso a datos de carácter personal que podría producirse durante la prestación de nuestros servicios.

4. Servicios ofertados

Los servicios ofertados en la presente propuesta son los siguientes:

- **Consultoría presencial para implantación del RGPD:** incluye la consultoría necesaria para el cumplimiento del Reglamento General de Protección de Datos.

  En dicha consultoría se revisarán, entre otros puntos, los siguientes:

  - **Flujos de información**. Recogida, tratamiento y supresión.
  - **Tratamientos**. Interesados, contenido y sensibilidad.
  - **Encargados** del tratamiento con acceso a datos.
  - **Proveedores** sin acceso a datos personales.
  - **Transferencias** de datos a terceros países.
  - **Análisis de las medidas de seguridad** implantadas.

5. Entregables y formación

Se elaborará y entregará la siguiente documentación para cumplir con los requisitos formales que establece el Reglamento General de Protección de Datos.

- **Cláusulas legales** (para documentación en papel y para la web).
- **Compromisos de confidencialidad con trabajadores**.
- **Contratos de acceso a datos por cuenta de terceros** para los encargados del tratamiento.
- **Contratos de prestación de servicios sin acceso a datos personales.**
- **Evaluación de Riesgos**.
- **Registro de Actividades de Tratamiento**.
- **Carteles informativos**.

6. Metodología y normas

Todas las intervenciones que realizamos se basan en **normas y metodologías vigentes** de referencia dentro del mundo de la seguridad de la información:

- ✓ **LOPD:** Ley Orgánica de Protección de Datos de Carácter Personal.
- ✓ **RGPD:** Reglamento General de Protección de Datos, de ámbito europeo.
- ✓ **LSSICE:** Ley de Servicios de la Información y de Comercio Electrónico.
- ✓ **ISO 27001**: El estándar a nivel mundial en la gestión de la seguridad de la información.
- ✓ **ISO 22301**: El estándar a nivel mundial en la gestión de la continuidad de negocio.
- ✓ **ENS:** Esquema Nacional de Seguridad.

7. Alcance del servicio

- Ámbito nacional.

Parque Tecnológico de León

c/ Julia Morros, 1 – Edificio Usos Comunes, Ofic. 109-115 · 24009 León

Tf. 987 263 832 · 987 7263 047

www.leasba.com · info@leasba.com