FORMACIÓN LOPD (Actualización RGPD 2018)

Objetivo del curso:

Actualizar los principales cambios en el Nuevo Reglamento Europeo de Protección de Datos.

Formato de la formación:

PRESENCIAL	E-LEARNING
LOPD/RGPD 2018	Nuevo Reglamento General de Protección de Datos
Práctica	Teórica
Específica	Genérica
3h	

Temario:

Principales cambios en el Nuevo Reglamento Europeo de Protección de Datos.

El Reglamento impondrá sanciones muy elevadas por incumplir estas obligaciones. Las violaciones graves tendrán multas de hasta 10 millones de euros o el 2% de la facturación mundial. Las violaciones muy graves tendrán una sanción de hasta 20 millones o el 4% de la facturación mundial.

1. No sustituye a la LOPD

No sustituye a la actual LOPD, el Nuevo Reglamento Europeo unifica el reglamento a todo el territorio Europeo adecuando la normativa a la Unión Europea. La fecha máxima, según el nuevo RGPD, es el mes de mayo de 2018.

2. ¿A qué empresas se aplica el nuevo RGPD?

Este Reglamento se aplica a responsables o encargados de tratamientos de datos de carácter personal establecidos en la Unión Europea, y también a responsables y encargados no establecidos en la UE siempre que traten datos como consecuencia de una oferta de bienes o servicios destinados a los ciudadanos de la UE.

Estas organizaciones y empresas deben designar un DPO (Delegado de Protección de Datos), oficialmente si son empresas de más de 250 trabajadores y de facto si son empresas más pequeñas.

3. ¿Cómo afecta a los ciudadanos y qué herramientas tienen para proteger sus datos personales?

Supone una garantía adicional para los ciudadanos ya que el Reglamento es aplicable a empresas que, hasta ahora, podrían estar tratando datos de personas físicas de países europeos y, cuando menos se rigen por normativas de otras regiones o países que no ofrecen el mismo nivel de protección que la normativa europea.

Se introducen nuevos elementos, entre ellos el derecho de olvido y el derecho de portabilidad, que aumentan la capacidad de decisión y control de los ciudadanos sobres los datos personales que faciliten a terceros.

- **Derecho al olvido**

Es el derecho que tienen los ciudadanos a solicitar y conseguir de los encargados que sus datos personales sean suprimidos cuando estos ya no sean necesarios por el fin que van a ser conseguidos, cuando se haya revocado el consentimiento o cuando estos se hayan obtenido de forma ilegal.

- **Derecho a la portabilidad**

Implica que el interesado que haya proporcionado sus datos a un responsable que los está tratando de forma digitalizada podrá pedir recuperar estos datos en un formato que le permita trasladarlos a otro responsable.

4. Nuevas obligaciones de las empresas

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

Todas las organizaciones que tratan datos han de efectuar un análisis de riesgo de sus tratamientos para poder establecer qué mesuras se deben aplicar y cómo hacerlo.

Estos análisis pueden ser procedimientos sencillos en entidades que realizan tratamientos elementales, pero pueden llegar a ser tratamientos muy complejos en empresas que o bien tratan un gran nombre de datos o que requieren una valoración especial de sus riesgos.

- **¿Cómo tenemos que obtener el consentimiento?**

El Reglamento pide que el consentimiento, con carácter general, sea libre, informado, específico y unívoco.

Las empresas tendrán que revisar la forma en la que obtienen y guarden el consentimiento. Actualmente estas prácticas se realizan por omisión, y que son aceptables en la actual normativa, pero que dejaran de serlo cuando el Reglamento entre en vigor. Tendrán que ser de forma proactiva y clara. El consentimiento tiene que ser verificable.

- **¿Se tienen que revisar los avisos de privacidad?**

El Reglamento prevé que se incluyan una serie de informaciones que anteriormente no eran obligatorias, entre ellas, se tendrá que explicar la procedencia legal para tratar los datos, los periodos de retención de estos y que los interesados puedan dirigir sus requerimientos a las Autoridades.

- **¿En qué consiste el sistema de ventanilla única?**

La ventanilla única supone que los responsables establecidos a diferentes países o que, aún que solo estén establecidos a un país pero afecte a otros, tengan una única autoridad de protección de datos.

- **¿Qué se entiende por Responsabilidad Activa según el RGPD?**

Esta responsabilidad activa se refiere a la necesidad de **PREVENCIÓN** por parte de las organizaciones que utilicen datos personales. Las empresas y entidades tendrán que adoptar medidas que sean garantía de manera suficiente que están en condiciones de cumplir con las reglas, derechos y garantías que el Reglamento establece. El Reglamento entiende que actuar únicamente cuando ya se ha producido la infracción puede producir daños a los interesados y **NO** es suficiente como estrategia, debido a la infracción puede producir daños a los interesados que pueden ser de difícil compensación o reparación.

Se establece una serie de medidas que son:

- Protección de datos des del principio
- Protección de datos por regla general
- Medidas de seguridad
- Establecer un registro de tratamientos
- Realización de un análisis del impacto
- Nombramiento de un Delegado si es necesario
- Comunicación de infracciones o fugas
- Promoción de códigos de conducta y procedimientos.

Para poder alcanzar todos estos cambios trabajaremos los puntos más importantes que son:

Consentimiento

Al no permitir el consentimiento tácito, el Reglamento obliga a todas las empresas a revisar el conjunto de cláusulas y a volverlas a hacer. Es necesario comunicar de una forma nueva, clara y simple. El consentimiento debe ser revocable en cualquier momento. Las empresas se han de asegurar que los datos no solo se utilizarán para los fines que van a ser recogidos.

Análisis de riesgos

El estudio de riesgos es una tasca primordial que se tiene que tener pensado para todos los procedimientos en los que existen un riesgo de la protección de datos. Esto permitirá crear procesos de auditoria para los ya existentes y todos los que puedan devenir en un futuro.

Comunicación de fugas o intentos de acceso

Se tendrán que comunicar los fallos de seguridad a la Agencia Española de Protección de Datos (AGPD) en un plazo máximo de 72 horas. Tiene que existir un sistema efectivo para que esto se pueda hacer y para comunicar a los afectados si existe un riego de sus derechos.

DPO

El delegado de protección de datos es una figura esencial en el reglamento. Tendrá que identificar los riesgos y buscar soluciones para estos. Las empresas deberán tener un delegado interno o externo, y otorgarle TOTAL independencia y poner a su disposición las herramientas que necesite cuando las solicite.