DESlock+
protege tu información

NUEVA Regulación General de Protección de Datos en la UE: Guía rápida para su aplicación

En 2016 se actualiza la Directiva de Protección de Datos de 1995 con nuevas regulaciones para toda la UE

ESET ENJOY SAFER TECHNOLOGY

La Regulación General de Protección de Datos (GDPR, en inglés) es una reforma exhaustiva de la regulación de protección de datos de 1995, que está siendo desarrollada para fortalecer y unificar los derechos de privacidad en internet y la protección de datos para los ciudadanos de la Unión Europea (UE), y al mismo tiempo reestructurar las obligaciones de protección de datos de las empresas que proveen servicios a los ciudadanos de la UE mediante una única Regulación en vez de 28 leyes nacionales diferentes.

La propuesta inicial para la GDPR fue publicada el 25 de enero de 2012 con el objetivo de que entrara en vigor a principios de 2016.

El Comisario de libertades civiles, justicia y asuntos internos (LIBE) del Parlamento Europeo votó de forma positiva el resultado de las negociaciones entre el Parlamento Europeo, la Comisión Europea y el Consejo Europeo con una entrada en vigor estimada de estas medidas en primavera de 2016. A diferencia de una Directiva, **una Regulación no requiere ninguna legislación adicional de gobiernos nacionales y su aplicación está programada para que dé comienzo en la primera mitad de 2018.**

¿CUÁLES SON LOS CAMBIOS?

Los cambios clave de la reforma incluyen:

- **El derecho a saber cuándo fueron hackeados los datos de alguien:** las empresas y organizaciones deben notificar a la autoridad de supervisión nacional las filtraciones de información que ponen a los individuos en riesgo y comunicar al sujeto responsable de la información las infracciones de alto riesgo tan pronto como sea posible para que los usuarios puedan tomar las medidas oportunas.
- **Una aplicación más fuerte de las reglas:** las autoridades de protección de datos podrán multar a las empresas que no cumplan las reglas de la UE con hasta el 2% de su facturación anual global.
- **Un continente, una ley:** una única ley paneuropea para la protección de datos, que sustituye el mosaico actual de leyes nacionales. Las empresas deberán atenderse a una sola ley, no 28. Los beneficios se estiman en 2,3 mil millones de euros por año.
- **Comunicación inmediata de las infracciones:** las organizaciones deben notificar a la autoridad nacional las infracciones graves en materia de protección de datos tan pronto como sea posible (si es posible en menos de 24 horas).
- **Para empresas activas en el mercado de la UE con servicios a ciudadanos de la UE:** Las reglas de la UE deben aplicarse si la información personal se maneja en el extranjero por empresas que están activas en el mercado de la UE y ofrecen sus servicios a los ciudadanos de la UE.
- **Protección de datos por diseño y por defecto:** La "Protección de datos por diseño" y "Protección de datos por defecto" son ahora elementos esenciales en las reglas de protección de datos de la UE. Los sistemas protección de datos se integrarán en los productos y servicios desde las primeras fases de desarrollo, y la configuración predeterminada de la privacidad será la norma a seguir.

Al hacer de la protección de datos un elemento clave y esencial del marco regulatorio de la UE, es obligatorio para las empresas la protección adecuada de información sensible, definida como:

"cualquier información relacionada con una persona natural identificada o identificable, de ahora en adelante referida como el 'sujeto de la información'; una persona identificable es una persona que puede ser identificada directa o indirectamente, en particular en lo referido a un número de identificación o a uno o más factores específicos a su identidad física, fisiológica, mental, económica, cultural o social."

Esta amplia definición de información personal **cubre fácilmente los archivos más simples relacionados incluso indirectamente con clientes, empleados, alumnos y cualquier otro archivo relacionado con un individuo.**

¿QUÉ DICE LA REGULACIÓN ACERCA DE LA PROTECCIÓN DE DATOS?

La sección 2 de la seguridad de la información en su artículo 30, la seguridad del tratamiento de datos, establece:

1. Teniendo en cuenta el estado inicial y los costes de implementación, así como la naturaleza, enfoque, contexto y objetivos del proceso de datos y el riesgo de variar la probabilidad y severidad de los derechos y libertades de los individuos, el controlador y agente de tratamiento implementará medidas técnicas y de organización apropiadas para garantizar un nivel de seguridad proporcional al riesgo, incluyendo entre otros, como apropiados:

a) La creación de pseudónimos y **el cifrado de la información** personal;

b) La habilidad de garantizar la confidencialidad, integridad, disponibilidad y adaptación constante de sistemas y servicios de tratamiento de información personal;

c) La habilidad de restaurar la disponibilidad y acceso a la información en un tiempo oportuno en caso de incidencia física o técnica;

d) Un proceso para probar y evaluar de forma regular la efectividad de medidas técnicas y de organización para garantizar la seguridad del tratamiento de datos.

El Artículo 30 **elimina cualquier duda sobre si los sistemas y el almacenamiento en instalaciones seguras deberían ser cifrados.** La tecnología es un medio muy conocido de protección de la información que es vulnerable al robo o pérdida. Esto también sirve para planes de recuperación efectivos en caso de desastres y para los sistemas de recuperación y administración de claves.

El Artículo 28 de la Regulación requiere que los archivos deban guardarse incluyendo una descripción general de las medidas de seguridad a nivel técnico y organizacional llevadas a cabo, como se establece en el Artículo 30, lo cual implica que **las organizaciones necesitan archivos y pruebas de que los sistemas son seguros y que la información cifrada es recuperable después de un incidente técnico.**

¿CUÁLES SON LAS REGLAS PARA LA NOTIFICACIÓN EN CASO DE FILTRACIÓN DE INFORMACIÓN?

El Artículo 31 detalla cómo realizar la Notificación de la filtración de información a las autoridades de supervisión y requiere que, en caso de filtración de información, se notifique a la autoridad de Supervisión donde sea factible, antes de 72 horas después tras haber detectado la filtración. Cualquier notificación posterior a 72 horas debe ir acompañada de una justificación razonada del retraso.

El Artículo 32 detalla aspectos sobre la comunicación de una filtración de información personal al sujeto de la información y establece que:

Cuando la filtración de información personal implique un alto riesgo para los derechos y libertades de los individuos, el controlador comunicará la filtración de información personal al sujeto en cuestión sin demora indebida.

Sin embargo, establece que:

No se requerirá la comunicación al sujeto de la información referido en el párrafo 1 si:

a) **El controlador ha implementado medidas de protección técnicas y organizacionales apropiadas,** y si estas medidas fueron aplicadas a la información afectada por la filtración de información personal, en particular aquellas que dejan la información ininteligible a cualquier persona que no esté autorizada a acceder a ella, tales como el cifrado; o

b) El controlador ha tomado las medidas subsiguientes que garanticen que el alto riesgo para los derechos y libertades de los sujetos de la información referidos en el párrafo 1 no es probable que se materialice;

c) **Pudiera suponer un esfuerzo desproporcionado.** En tal caso habrá una comunicación pública o una medida similar por la cual se informe a los sujetos de la información de una forma igualmente efectiva.

Los estudios demuestran que cuanto antes se informa de una filtración de información, más dañinas son las consecuencias para la organización en cuestión. De nuevo, **el cifrado se considera de forma clara como una medida de protección suficiente** para excluir esto y las consecuencias para la reputación corporativa.

¿CÓMO DISUADE LA REGULACIÓN A LOS INFRACTORES?

El punto seis del Artículo 79 sobre sanciones administrativas establece que:

La autoridad de supervisión impondrá una **multa de hasta 1.000.000 de € o,** en caso de tratarse de una empresa, **hasta el 2% de su facturación anual a nivel mundial**, a cualquiera que de forma intencionada o por negligencia:

> Nota (e): **no adopte políticas internas o no implemente las políticas adecuadas** para garantizar y demostrar el cumplimiento de las medidas establecidas en los Artículos 22, 23 y 30;
>
> Nota (h): **no alerte o notifique una filtración de información personal o no notifique la filtración completamente o en un tiempo oportuno** a la autoridad supervisora o al sujeto implicado en la información conforme a los Artículos 31 y 32;

Este claro intento de penalizar y disuadir a los infractores entrará en vigor a lo largo de los próximos dos años, por lo que es momento de actuar *ahora*.

Algunos países ya han empezado a trabajar; el senado Holandés aprobó una propuesta de ley en mayo de 2015 para enmendar su Ley de Protección de Datos con antelación y prevaleciendo la GDPR, haciendo que Holanda pase de ser uno de los países con una legislación más débil a uno de los más severos en esta materia. La regulación se aplicará en todos los 28 estados miembros a mediados de 2018.

¿QUÉ MEDIDAS DEBERÍAN TOMARSE AHORA?

La regulación requiere que todas las empresas adopten un nuevo conjunto de procedimientos y políticas enfocadas a otorgar a los ciudadanos un mayor control sobre los archivos con información personal. Esto implicará la creación de nuevos procesos y manuales, reciclar a los empleados y actualizar los sistemas para adoptar estos nuevos procedimientos. Otros pasos implican medidas prácticas como **utilizar el cifrado donde la información pudiera estar expuesta a riesgos.**

La pérdida o robo de un portátil o dispositivo de almacenamiento USB no tiene porqué implicar sanción alguna si estos han sido cifrados con un producto avalado. DESlock lleva años cifrando portátiles, dispositivos extraíbles, correos electrónicos y archivos de empresas de todos los tamaños. Nuestro producto protege todos los sistemas Windows desde XP a Windows 10 y móviles iOS desde la Versión 7. DESlock cumple con la norma FIPS-140-2 de nivel 1. Además, nuestro sistema de administración de claves y el servidor de administración único son objeto de patentes a nivel mundial.

Contacta con ESET España: **ventas@eset.es o en el telf. 96.291.33.48,** o con tu distribuidor más cercano para más información o para solicitar una demo del producto.

Uno de los requisitos clave de la GDPR de la UE es que la información personal esté cifrada. Donde quiera que se utilice el cifrado como medida técnica, la información debe poder ser restaurada rápidamente después de una incidencia y los archivos deben guardarse para probar que los sistemas son seguros y recuperables.

DESlock está diseñado para afrontar estos requisitos de forma simple y efectiva.

Objetivo	DESlock+
Protege la información almacenada en la empresa	Todas las versiones comerciales de DESlock+ incluyen el cifrado de archivos, carpetas y dispositivos extraíbles por defecto para garantizar la protección de la información en el equipo.
Protege la información en tránsito	DESlock+ Pro incluye el cifrado de todo el disco y de dispositivos extraíbles USB y medios ópticos para garantizar la seguridad de la información que sale de la empresa.
Protege la información para los empleados fuera de la oficina o desde casa	Las licencias comerciales de DESlock+ permiten su instalación en otro ordenador. DESlock+ Go además añade cifrado portable a cualquier dispositivo de almacenamiento USB.
Protege la transferencia de datos entre distintas sedes corporativas	Todas las versiones de DESlock+ incluyen: - Plugin para Outlook - Cifrado de documentos adjuntos - Portapapeles para cualquier sistema El cifrado de medios ópticos permite la transferencia segura de la información almacenada en CDs o DVDs.
Bloquea / limita el acceso a determinada información	La tecnología de compartición de claves única y patentada hace que sea simple instalar y administrar equipos y grupos de trabajo complejos y con múltiples niveles de jerarquía.
Permite el acceso a información segura cuando se solicita	DESlock+ Enterprise Server está diseñado para una administración remota de los usuarios mediante una conexión a internet segura. Las claves pueden ser distribuidas y eliminadas de forma centralizada rápidamente.
Permite el almacenamiento seguro de información personal	DESlock+ está certificado con FIPS-140-2 y utiliza algoritmos y métodos de cifrado estándar fiables que han sido aprobados.
Garantiza la destrucción de información inservible	La herramienta DESlock+ Destructor de Documentos elimina toda la información deseada con el estándar DoD-5220.22-M garantizando que ésta será completamente irrecuperable.

Información General

Detalles del Reglamento
http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf (bota.me/GDPR)

Borrador del compromiso
http://www.statewatch.org/news/2015/dec/eu-council-dp-dir-leas-draft-final-compromise-15174-15.pdf (bota.me/Borrador)