SOPHOS
Security made simple.

Propuesta de Reglamento de protección de datos de la UE

Próximos requisitos de confidencialidad de datos y cómo cumplirlos

Las cosas han cambiado mucho desde 1995, la última vez que se aprobó una ley europea importante sobre el tema de la protección de datos (Directiva 95/46/CE sobre protección de datos). Por ejemplo, los dispositivos móviles están en todas partes, y es bastante frecuente llevar dos o incluso tres a la vez. Mientras tanto, los datos corporativos sensibles se mueven fuera del perímetro de seguridad tradicional de la empresa. Los empleados se envían a sí mismos documentos por correo electrónico, acceden a datos desde smartphones y tabletas personales, y almacenan datos en la nube. En la actualidad es muy común que se produzcan importantes filtraciones de datos que ponen a los clientes en riesgo de robo de identidad y pérdidas financieras, y a las empresas en riesgo de perder a sus clientes y la lealtad de los inversores. Este monográfico contiene información sobre las implicaciones que tendrán para las empresas globales las nuevas propuestas de **reforma del Reglamento General de Protección de Datos aplicable** a toda la UE.

Al igual que la mayoría de los estados en los EE.UU., muchos países de la Unión Europea (UE) han implementado su propia legislación de protección de datos para reflejar esta nueva realidad de disolución del perímetro de la red. Las normas europeas de protección de datos varían mucho de país a país, tal y como ocurre en EE.UU. entre diferentes estados Esto, sumado a la proliferación de datos en nuevos tipos de medios y tecnologías, está impulsando la necesidad de modernizar y homogeneizar el Reglamento General de Protección de Datos de la UE.

Durante dos años, la UE ha estado trabajando en nuevas propuestas de reforma del Reglamento General de Protección de Datos que establecerán un marco a escala de la Unión para reemplazar el mosaico existente de legislaciones específicas de cada país. El objetivo es reforzar los derechos de privacidad de los ciudadanos de la UE, recuperar la confianza en las actividades en la red y mejorar la protección de los datos de los clientes, al exigir a las empresas la adopción de nuevos procesos y controles de protección de datos. En el momento de escribir esto, las propuestas constan de 91 artículos[1]. Al igual que cualquier legislación, la reforma pendiente del Reglamento General de Protección de Datos puede ser confusa. Nuestro objetivo con este monográfico no es educar a los lectores sobre el conjunto de la ley, sino centrarnos en la necesidad de proteger la confidencialidad de los datos, ya que su incumplimiento conlleva un conjunto de multas muy severo. Para obtener más información acerca de la iniciativa de la reforma, visite los recursos enumerados en el apéndice de este documento.

La Unión Europea (UE) es una asociación económica y política única entre 28 países europeos que juntos abarcan gran parte del continente. Si bien cada país tiene su propia cultura y legislación, la UE tiene el objetivo de hacer que sus instituciones de gobierno sean más transparentes y democráticas. Una forma de lograr este objetivo es la creación de un marco de leyes o directivas europeas que sustituya parcial o totalmente a las leyes nacionales.

Elementos fundamentales de la reforma

Las propuestas de reforma de los Reglamentos generales de protección de datos establecieron un nuevo récord con 3.999 enmiendas[2] en su trayectoria hacia convertirse en una ley. Tras el largo proceso de revisión, el Parlamento Europeo demostró su firme compromiso con el tema de la protección de datos y la reforma en una votación casi unánime de 621 votos a favor, 10 en contra y 22 abstenciones en marzo de 2014.[3] A pesar de que ahora tiene que pasar por una nueva ronda de revisión y un proceso de aprobación por parte del Consejo de la Unión Europea, es muy probable que la futura legislación sea similar a las propuestas que vemos hoy.

He aquí algunos ejemplos de lo que dice la propuesta sobre la protección de datos sensibles.

El **Artículo 30**[5] aborda la seguridad del tratamiento de datos:

1. *El controlador y el encargado de tratar los datos deberán aplicar las medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad acorde con los riesgos que presente el tratamiento, teniendo en cuenta los resultados de una evaluación de impacto sobre la protección de datos (con arreglo al Artículo 33), teniendo en cuenta la tecnología avanzada necesaria y el coste de su implementación.*

1a. *Una vez comprobada la tecnología avanzada y el coste de su implementación, esta política de seguridad deberá incluir:*
(a) la capacidad de garantizar que se valida la integridad de los datos personales;
(b) la capacidad para garantizar de forma continua la confidencialidad, integridad, disponibilidad y capacidad de recuperación de los sistemas y servicios de procesamiento de datos personales;
(c) la capacidad de restaurar la disponibilidad y el acceso a los datos en tiempo y forma en el caso de un incidente físico o técnico.

2. *Las medidas a las que se hace referencia en el párrafo 1 deberán, como mínimo:*
   (a) garantizar que únicamente el personal autorizado puede acceder a los datos de carácter personal para fines legales;
   (b) proteger los datos personales almacenados o transmitidos frente a la destrucción accidental o ilícita, la pérdida accidental o alteración, y el almacenamiento, tratamiento, acceso o divulgación no autorizado o ilegal; y
   (c) garantizar la implementación de una política de seguridad con respecto al tratamiento de datos personales.

En pocas palabras, el artículo obliga a las organizaciones a desplegar controles técnicos avanzados que protejan los datos. El artículo no especifica las tecnologías que se deben utilizar para esos controles, pero se reserva, en un tercer apartado, el derecho a un "Consejo Europeo de Protección de Datos" para especificar en un tiempo futuro "lo que constituye la tecnología avanzada, para sectores específicos y en situaciones específicas, de tratamiento de datos".

En caso de producirse una filtración de datos, el **Artículo 31**[6] de las propuestas especifica que la empresa está obligada a notificárselo inmediatamente a la autoridad supervisora. Sin embargo, la empresa puede o no estar obligada a informar a las personas cuyos datos se han filtrado. El **Artículo 32**[7] establece que:

1. *Cuando es probable que la filtración de datos afecte negativamente a la protección de los datos personales, la privacidad, los derechos o los intereses legítimos del interesado, el controlador, después de la notificación prevista en el Artículo 31, comunicará la filtración de datos personales al interesado sin demora injustificada.*
2. *(...)*
3. *No será necesario comunicar una filtración de datos personales al interesado, si el controlador demuestra (a satisfacción de la autoridad de supervisión), que tiene implementadas las medidas de protección tecnológica apropiadas y que estas medidas se aplicaron a los datos afectados por la filtración de los datos personales. Unas medidas de protección de estas características harán que los datos sean incomprensibles para cualquier persona que no esté autorizada a acceder a ellos.*

Si, en el momento de la pérdida, los datos están protegidos de manera tal que sean ininteligibles (y por lo tanto, inútiles para una parte no autorizada) – *y* la empresa puede demostrar esto a la autoridad de control, entonces no estará obligada a revelar la filtración a las personas cuyos datos se han perdido o robado.

Si una empresa no hace cualquiera de estas cosas – adoptar políticas internas e implementar las medidas adecuadas para garantizar y demostrar el cumplimiento normativo, o notificar a la autoridad de control o al interesado una filtración de datos, siempre que sea necesario – entonces el **Artículo 79**[8] sobre las sanciones administrativas establece que la autoridad de control podrá imponer al menos una de las siguientes sanciones:

a) *una advertencia por escrito en el caso de ser el primer incumplimiento y/o no intencionado*
b) *auditorías de protección de datos regulares y periódicas*
a) *una multa de hasta 100 millones de euros o hasta el 5% del volumen de negocios mundial anual en el caso de una empresa, lo que sea mayor.*

En resumen: Si no implementa la tecnología adecuada para proteger los datos sensibles, entonces probablemente tenga que pagar – directamente a la autoridad de supervisión e indirectamente por daños a la reputación, y la pérdida de la buena voluntad y la confianza de los clientes. Sin embargo, las empresas que cifran sus datos protegen a sus clientes – y a ellas mismas.

Terminología de las propuestas de protección de datos

Datos personales
cualquier información relacionada con la vida privada, profesional o pública de una persona. Puede ser un nombre, una foto, una dirección de correo electrónico, datos bancarios, sus publicaciones en las redes sociales, información médica o la dirección IP de su ordenador.

Controladores de datos
deciden sobre las condiciones, la finalidad y forma en la que se procesan los datos personales. Pueden ser personas físicas, empresas o autoridades públicas. Algunos ejemplos de personas físicas pueden ser médicos, farmacéuticos y políticos, que conservan datos sobre sus pacientes, clientes y electores.

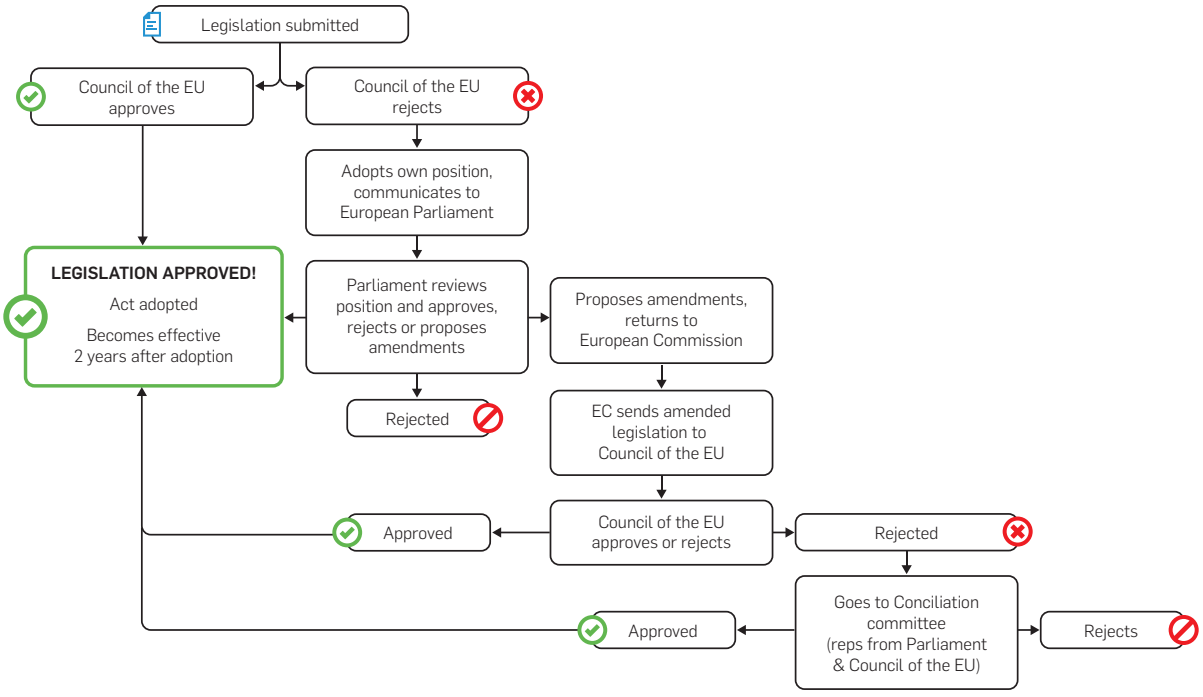
Procesadores de datos
procesan la información personal bajo la autoridad de los controladores de datos, pero no toman decisiones sobre las condiciones, la finalidad y los medios del tratamiento (subcontratistas). Por ejemplo, las empresas especializadas en el pago de nóminas, así como las empresas de contabilidad y estudios de mercado pueden procesar información personal en nombre de otros (por ejemplo, otras empresas o autoridades públicas, que serían los controladores de datos en tales casos). Sin embargo, si deciden sobre las condiciones, la finalidad o actúan más allá de las instrucciones de los controladores, se convierten en controladores para esa actividad de tratamiento específica.

Interesado
Los datos personales se utilizan para identificar a una persona natural. Esa persona es el "interesado".[4]

Proceso de adopción para que la propuesta se convierta en ley

El proceso de promulgación de una ley para toda la Unión es muy largo y puede durar varios años. Las tres instituciones de la Unión Europea – la Comisión Europea, el Parlamento Europeo y el Consejo de la Unión Europea – deben ponerse de acuerdo sobre la legislación antes de que pueda convertirse en una ley activa. El proceso está impulsado por la Comisión Europea, que también es responsable de proponer nueva legislación. En el Parlamento Europeo, el trabajo legislativo sobre el intercambio de información y la protección de datos, está dirigido por la Comisión de Libertades Civiles, Justicia y Asuntos de Interior (LIBE). En el Consejo de la Unión Europea (también llamado Consejo de Ministros), esa responsabilidad recae en el grupo de trabajo DAPIX.

Las leyes reformadas de protección de datos fueron propuestas por la Comisión Europea. En octubre de 2013, la Comisión LIBE respaldó el proyecto modificado por una abrumadora mayoría y recibió el mandato de negociar con el Consejo de la Unión Europea. A continuación, esta votación fue confirmada por el Parlamento Europeo en sesión plenaria el 12 de marzo de 2014, de nuevo por una abrumadora mayoría de 621 votos a favor, 10 en contra y 22 abstenciones. Si bien las elecciones en Europa sin duda introducirán retrasos e incertidumbres, la cantidad de trabajo legislativo que ya se ha realizado y el voto casi unánime a favor de este texto en todas las nacionalidades e ideologías políticas son claros indicativos de que esta propuesta ha llegado para quedarse y que el impulso continuará. La propuesta de legislación ahora puede tomar uno de varios caminos antes de convertirse en ley, lo cual podría hacer que se tardase más de un año en pasar por todos los pasos posibles.



¿Quién se ve afectado por la nueva reforma?

El estado de las propuestas de reforma del Reglamento de protección de datos de la UE debe ser de interés mundial, ya que afecta a cualquier empresa que haga negocios con ciudadanos europeos, independientemente de dónde tenga su sede la empresa. Esto es muy similar a muchas leyes de protección de datos de los Estados Unidos. Por ejemplo, una empresa con sede en Francia que haga negocios con clientes estadounidenses en California debe cumplir con la ley de protección de datos de California. Si esa misma empresa también hace negocios con clientes en Massachusetts, entonces también debe cumplir con la ley de protección de datos de Massachusetts, y así sucesivamente. Algunos de los beneficios de la reforma del Reglamento General de Protección de Datos de la UE serán los siguientes:

- Un continente, una ley: las empresas europeas y no europeas ya no tendrán que investigar y conocer los detalles de 28 regulaciones y reglamentos diferentes.
- Proceso unificado: se seguirá el mismo proceso en caso de filtraciones y/o violaciones.
- Se aplicarán las mismas reglas a todas las empresas: independientemente de dónde tengan su sede las empresas, se aplicará el mismo conjunto de reglas al hacer negocios en la UE.

Cómo cumplir con la nueva legislación

Para las muchas empresas que deben cumplir con la legislación sugerida para la reforma del Reglamento general de protección de datos, la mejor manera de prepararse es implementar una estrategia de protección de datos sólida y un proceso que **debe incluir el cifrado** para aumentar la eficacia.

Como se mencionó anteriormente, la ley propuesta no requiere un tipo específico de control técnico aparte de ser "avanzado" y hacer que los datos del cliente sean ininteligibles. Por lo tanto, lo mejor es observar cómo las organizaciones consiguen cumplir con los demás reglamentos destinados a proteger los datos sensibles. La Ley de responsabilidad y transferibilidad de seguros médicos (HIPAA), el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI DSS) y la ley Sarbanes-Oxley (SOX) son algunos ejemplos de reglamentos que requieren controles de protección de datos similares a los de las propuestas para la reforma del Reglamento de protección de datos de la UE. El cifrado es ampliamente aceptado como un medio adecuado para satisfacer estos requisitos, debido a que hace que los datos sean ininteligibles, Si los datos cifrados se pierden o son objeto de robo, son esencialmente inútiles. Nadie puede acceder a los datos reales. Y ese es el quid de las leyes y reglamentos de protección de datos.

Conclusión: Si quiere estar preparado para la reforma del Reglamento General de Protección de Datos, debe empezar a estudiar las tecnologías de cifrado.

Cómo Sophos SafeGuard le ayuda a superar con éxito el reto de la protección de datos

La adopción de la tecnología de cifrado ha sido impulsada en gran medida por la necesidad de cumplir con los requisitos legales y reglamentarios. Sin embargo, las empresas que han adoptado el cifrado a menudo se muestran preocupadas por la tecnología. El cifrado se percibe tradicionalmente como un consumidor de recursos que sobrecarga a los equipos de TI y obstaculiza la productividad del usuario. Las tecnologías de cifrado más viejas pueden ralentizar el tiempo de arranque y suponer una molestia para los usuarios. Otras no funcionan con el hardware más reciente o incapacitan los equipos, e inevitablemente los, ya saturados equipos de TI, tienen que dedicarles tiempo.

Sophos SafeGuard Encryption proporciona cifrado sin compromiso. Las versiones modernas de los sistemas operativos Windows y Mac vienen con motores de cifrado incorporados. SafeGuard aprovecha estos motores de cifrado nativos de los sistemas operativos siempre que sea posible para reducir el impacto en el usuario final. El resultado es mayor protección con mayor rendimiento.

También facilitamos el cifrado protegiendo a todos los equipos en todas las plataformas sin interponernos en el camino de los usuarios ni en la manera en la que quieren trabajar. SafeGuard acompaña a los datos para protegerlos en todas partes. Ya sea en la nube, en dispositivos de almacenamiento extraíbles, en archivos de red, o en dispositivos móviles, SafeGuard va allá donde vayan sus datos.

Un cifrado sencillo también significa una implementación y gestión más sencilla para el equipo de TI. Las capacidades de auditoría y presentación de informes son un refuerzo para el cumplimiento normativo, ya que permiten comprobar si un archivo, equipo o dispositivo USB estaba cifrado en el momento en el que se perdió, fue robado o se produjo una filtración. Todas estas características aportarán tranquilidad para las empresas, que se arriesgan a percibir cuantiosas multas en caso de incumplir las leyes de protección de datos.

Sophos es el único proveedor de seguridad que le ofrece funciones de cifrado para los equipos de los usuarios, las carpetas compartidas, los medios extraíbles y los datos almacenados en la nube, tanto para Windows como para Mac. Y disfrutará de toda esta versatilidad con un solo agente y desde una misma consola de administración. Nuestro cifrado certificado bloquea fugas de datos y facilita el cumplimiento de las normativas sin interponerse en su trabajo. Además, le ayuda a ahorrar tiempo, porque la protección de sus datos se administra fácilmente.

Conclusión

El miedo a la vigilancia del gobierno, junto con las noticias sobre filtraciones de datos de perfil alto en los medios de comunicación, hace que cada vez sea mayor la presión y los requisitos para proteger los datos confidenciales de los clientes. Al mismo tiempo, la confianza de los clientes en los negocios se está deteriorando. El Parlamento Europeo, las autoridades de protección de datos y los gobiernos quieren salvaguardar e impulsar la economía europea en línea, por lo que muchas empresas tendrán que poner en práctica procesos y controles técnicos que garanticen la confidencialidad de los datos de los clientes.

El cifrado debe ser parte de esta solución, ya que evitará que usuarios no autorizados puedan leer los datos en caso de pérdida o robo. Sophos SafeGuard Encryption ofrece a las empresas la garantía de disfrutar de la protección que necesitan sin afectar al flujo de trabajo del usuario ni consumir recursos de TI.

Apéndice

1. Propuesta para un REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO,relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos). Comisión Europea, 25 de enero de 2012.

2. Control de calidad sobre la Reforma de la protección de datos de la UE. Parlamento Europeo, 3 de abril de 2013.

3. Comunicado de prensa: El progreso en la reforma de la protección de datos de la UE es ya irreversible tras la votación del Parlamento Europeo. Parlamento Europeo, 12 de marzo de 2014.

4. Control de calidad sobre la Reforma de la protección de datos de la UE. Parlamento Europeo, 3 de abril de 2013.

5-8. INFORME sobre la propuesta para un reglamento del Parlamento Europeo y del Consejo,relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos). Parlamento Europeo, 21 de noviembre de 2013.

Ventas en el Reino Unido e internacionales
Teléfono: +44 8447 671131
Correo electrónico: sales@sophos.com

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en Norteamérica
Teléfono: +1 866 866 2802
Correo electrónico: nasales@sophos.com

Oxford (Reino Unido) | Boston (EE. UU.)

5.14.GH.wpes.simple