G DATA Whitepaper

El nuevo Reglamento de Protección de Datos de la UE (GDPR) – Lo que las empresas deben saber

G DATA Software AG | Septiembre 2017

Introducción

La protección de datos es mucho más que una obligación y el nuevo Reglamento General de Protección de Datos de la UE (GDPR) está en la agenda de todas las empresas europeas, con independencia de su tamaño o la naturaleza de su negocio. Las organizaciones tienen de plazo hasta el 25 de mayo de 2018 para adaptarse a la nueva situación jurídica y proteger eficazmente los datos de sus clientes. Los incumplimientos del nuevo Reglamento se castigarán con penas bastante serias, por lo que es imprescindible actuar. Se deberá informar a los empleados y comprobar los flujos de trabajo y las herramientas para garantizar que los datos de clientes se traten de acuerdo con la ley. También en el área TI habrá que adoptar un número considerable de medidas. En el presente informe encontrará las exigencias más importantes que establece el nuevo GDPR y se le informa de cómo una solución integral de seguridad TI puede ayudarle a cumplirlo.

1. ¿Qué es el Reglamento General de Protección de Datos?

El Reglamento General de Protección de Datos de la UE (GDPR) fue aprobado por el Parlamento Europeo en abril de 2016 y regula la modernización y armonización a nivel europeo de leyes de protección de datos, siendo su principal objetivo garantizar la protección de los datos personales conforme a los siguientes principios[1]:

- licitud, lealtad y transparencia
- limitación a la finalidad
- minimización de datos
- exactitud
- limitación del plazo de conservación
- integridad y confidencialidad

El Reglamento sustituye a la ya anticuada Data Protection Directive (DPD) del año 1995. A diferencia de la DPD, el GDPR no «sólo» es una directiva, sino de una ley. Esto significa que el Reglamento no requiere implementación separada por parte de los estados miembros de la UE, por lo que la entrada en vigor se estableció ya para el 24 de mayo de 2016. Se concedió un período de transición hasta el 25 de mayo de 2018 para que las empresas pudieran adaptarse a la nueva legalidad y aplicar las especificaciones del GDPR. Si no lo hacen, se les puede imponer elevadas multas en caso de fallo en la protección de datos.

[1] Artículo 5 del GDPR. Encontrará el texto íntegro en http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

2. ¿A qué empresas afecta el GDPR?

El Reglamento General de Protección de Datos regula la protección de datos personales por lo que afecta a todas las empresas que traten datos personales de particulares en la Unión Europea. El artículo 4 del texto legislativo contiene la siguiente definición para especificar los datos a los que se refiere la ley:

«A efectos del presente Reglamento se entenderá por 'datos personales' toda información sobre una persona física identificada o identificable; se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona».

Nos encontramos ante una definición bastante amplia. Los datos típicos recopilados por las empresas y protegidos por el GDPR son el nombre, la dirección, la dirección de correo electrónico u también la dirección IP. En el contexto empresarial a menudo se trata de datos de clientes que se procesan, por ejemplo, en un sistema CRM. Sin embargo, el GDPR protege también los datos empleados sólo para fines de marketing o recopilados a modo de "captura accesoria", como p. ej. una dirección IP en un log.

3. ¿Qué derechos reconoce el GDPR a los clientes?

El GDPR establece los requisitos que las empresas deben cumplir al tratar datos personales. Muchas medidas ya se definieron en la mencionada directiva del año 1995 (Data Protection Directive), pero hay algunas nuevas exigencias que supondrán un reto incluso para empresas que hasta ahora siempre habían sido «cumplidoras». Un breve resumen:

- Derecho al olvido: El cliente tendrá «derecho a obtener la supresión de los datos personales que le conciernan» (artículo 17).
- Licitud y derecho a autorización: Cada cliente debe ser informado «exhaustivamente y en términos sencillos» sobre la finalidad de los datos que proporciona. Debe autorizar su uso voluntariamente, es decir, la autorización no debe estar vinculada a otras condiciones (p. ej. la aceptación de que los datos se usen para fines publicitarios para poder hacer un pedido). Esto se establece en los considerandos nº 42 y 43 del GDPR.
- Notificación inmediata a la autoridad de control: «En caso de violación de la seguridad, el responsable del tratamiento la notificará a la autoridad de control sin dilación indebida, a más tardar 72 horas después de que haya tenido constancia de ella» (artículo 33).

- Derecho a la portabilidad de los datos: Los clientes tendrán derecho a recibir los datos conservados sobre ellos «en un formato estructurado, de uso común y lectura mecánica» (artículo 20).

Está claro que la aplicación de esos derechos y su reflejo en multitud de procesos empresariales no es asunto trivial. Por ejemplo, muchas especificaciones dan por supuesto que las empresas saben en qué medida y en qué lugares han conservado estos datos personales que son objeto de la Ley. Y puede que sea así en una pequeña empresa con sólo un banco central de datos de clientes, pero cuando hablamos de fuentes de datos como, por ejemplo, las grabaciones de video vigilancia en espacios públicos o el tratamiento de datos en plataformas en la nube (que ofrece el software de Salesforce, por ejemplo), se constata que muchas empresas conservan y tratan más datos personales de los que quizás sean conscientes y que éstos también se conservan y tratan fuera del propio ámbito de influencia directo. También hay un potencial de conflictos en un cliente que quiere borrar sus datos personales cuando estos deben conservarse atendiendo a otras leyes (p. ej. datos contables).

4. ¿Qué ocurre si se infringe el GDPR?

No solamente son nuevas las medidas descritas en el GDPR: también se definieron nuevas multas para las empresas que no las apliquen o lo hagan inadecuadamente. Una autoridad competente en la protección de datos podrá imponer las siguientes multas en función de la gravedad del caso:

- Hasta 20 millones de euros o el 4% de las ventas anuales de la empresa a nivel mundial (aplicándose el importe mayor)
- Hasta 10 millones de euros o el 2% de las ventas anuales de la empresa a nivel mundial (aplicándose el importe mayor)

La primera categoría de multas se aplicará, por ejemplo, si una empresa infringe las disposiciones del artículo 17 (derecho al olvido). La última categoría está pensada para infracciones relativamente leves, por ejemplo, la violación de la obligación de notificar conforme al artículo 33, pero el importe máximo de 10 millones de euros o el 2% de las ventas implican cifras realmente elevadas. Las multas están definidas en el artículo 83 del GDPR que, además, garantiza que, en todo caso, la imposición de multas sea «efectiva, proporcionada y disuasoria».

5. Ha empezado la cuenta atrás: ¿Cuáles son los puntos esenciales?

A pesar de las elevadas multas de las que pueden ser objeto las empresas no cumplidoras y de lo rápido que pasa el período transitorio, muchas organizaciones aún no han tomado medidas. Según la consultora Gartner, a finales de 2018, cuando el Reglamento ya lleve

mucho tiempo en vigor, más de la mitad de las empresas afectadas por el GDPR aún no habrán aplicado todas las especificaciones[2]. Con tantos efectos posibles es importante conocer los puntos de aplicación más importantes.

5.1. Nombrar a un delegado de protección de datos

El primer paso es el nombramiento o la designación de un delegado de protección de datos. Conforme al artículo 37, esto se aplicará a autoridades, organismos públicos y empresas que procesen datos personales. También las PYME podrán considerar nombrar a un delegado externo de protección de datos. El delegado de protección de datos será la persona de contacto oficial ante el público en general y la autoridad regional de protección de datos competente. Pero incluso las empresas no obligadas a nombrar a un delegado de protección de datos pueden aprovecharse de ello, por ejemplo, para establecer un punto de contacto para cuestiones internas y externas relacionadas con la protección de datos.

5.2. Hacerse las preguntas adecuadas… y poder responderlas

Las siguientes preguntas pueden resultar útiles a cualquier empresa, del tamaño que sea, para identificar los puntos centrales:

- ¿Qué datos afectados por el nuevo GDPR se recopilan o se tratan en mi empresa?
- ¿Estás esos datos lo suficientemente protegidos? ¿La tecnología empleada está obsoleta o es un buen reflejo de lo que la tecnología actual ofrece para este menester?
- En caso de violación de la seguridad de los datos, ¿podemos notificarlo a la autoridad de protección de datos en un plazo máximo de 72 horas?
- ¿Las personas físicas a las que afectan los datos almacenados pueden obtener información sobre sobre ellos? ¿Pueden borrarse en caso necesario?
- ¿Los datos almacenados se transmiten a otras empresas para su conservación o tratamiento (p. ej. servicios en la nube)? En su caso, ¿deben adaptarse los contratos sobre servicios de tratamiento de datos al nuevo GDPR y al nuevo contexto? Es importante resaltar que los contratos antiguos no gozan de garantía de continuidad.

5.3. Comprobar flujos de trabajo y herramientas

Se trata de sensibilizar a los empleados acerca del tema y comprobar asimismo flujos de trabajo y herramientas y, en su caso, adaptarlos a la nueva ley. En ese contexto, un paso importante es el establecimiento de normas de cumplimiento que definan cómo se trata la información. Esas normas son una combinación de medidas técnicas y organizativas. Por

[2] Fuente: https://www.gartner.com/newsroom/id/3701117.

ejemplo, nivel tecnológico, un gestor de políticas de seguridad TIC facilitará que se empleen sólo las herramientas necesarias para el tratamiento de datos y que se excluyan del mismo aplicaciones como, por ejemplo, los servicios privados de almacenamiento en la nube o el uso de dispositivos externos, evitando así que los empleados puedan grabar esos datos personales en memorias USB, por ejemplo.

5.4. Proteger su infraestructura TI

Otro elemento importante es la exhaustiva protección de los sistemas TIC de las organizaciones. Hay que comprobar los sistemas existentes y, en caso necesario, planificar e implementar sistemas nuevos. La protección incluye toda la red informática y las comunicaciones. Es esencial la presencia de un firewall que impida conexiones no autorizadas. Además, hay que comprobar a fondo el tráfico web y otros canales de comunicación online mediante algún sistema de protección web y el escaneo de los correos electrónicos. La monitorización proactiva del sistema y sus procesos también contribuye a proteger contra el malware. Para procurar que el sistema operativo y las aplicaciones estén actualizados y se subsanen deficiencias con la debida antelación se puede recurrir a un sistema de administración de parches (Patch Management) que garantice la distribución correcta y en los tiempos adecuados de las actualizaciones que sellan las vulnerabilidades de los programas instalados. Igual de relevantes son las copias de seguridad y los sistemas de recuperación de datos: esenciales para que los datos no se pierdan en caso de ciberataque o por cualquier otra causa.

G DATA le ayuda a cumplir con el nuevo GDPR

Para poder cumplir con las obligaciones y requisitos exigidos en el nuevo GDPR es esencial el despliegue de una solución de seguridad que proteja de forma integral la infraestructura TIC, que pueda ser administrada de forma centralizada y que haga llegar a su administrador las alertas oportunas en caso de un eventual incidente relacionado con la protección de datos.

La nueva Ley obliga a notificar cualquier brecha de seguridad informática, pues se considera que conduce a la destrucción de información, a su pérdida o a su extracción por un tercero no autorizado. La oferta de seguridad por capas de las soluciones empresariales de G DATA, ofrece una protección integral frente a cualquier tipo de ciberataque y adecuada a redes empresariales de cualquier tamaño que combina una excelente protección proactiva, sella brechas y vulnerabilidades de seguridad (ver *G DATA Patch Management*, https://www.gdata.es/empresas/patch-management) y facilita las notificaciones de incidentes.

Además, la implementación y administración de las soluciones empresariales de G DATA también se puede poner en manos de su proveedor TIC de confianza gracias al formato SaaS (Software as a Service) de nuestro «*G DATA Managed Endpoint Security*».

Más información sobre las soluciones empresariales de G DATA en www.gdata.es/empresas. Además, el blog de G DATA, www.gdatasoftware.com/blog, le mantendrá al tanto de las soluciones más recientes y eficaces en las áreas de protección de datos, cumplimiento y seguridad TI.

Por último, tenga en cuenta que este informe pretende invitar a reflexionar sobre los posibles efectos del GDPR y no sustituye a un exhaustivo asesoramiento legal.