GDPR: 5 lecciones aprendidas

la experiencia de Veeam en materia de cumplimiento compartida.

El 25 de mayo de 2018
EL REGLAMENTO GDPR ENTRARÁ EN VIGOR
ESTÉ PREPARADO PARA GARANTIZAR EL CUMPLIMIENTO

El Reglamento General de Protección de Datos (GDPR por sus siglas en inglés)) exige a las empresas que protejan la información de carácter personal y la privacidad de los ciudadanos de la UE para las transacciones que se produzcan dentro de los estados miembros de la Unión Europea. Tendrá que poder garantizar la seguridad de todos los datos personales que recopile y/o procese, o enfrentarse a posibles sanciones.

Descubra las cinco lecciones aprendidas por Veeam® en su camino para cumplir con el reglamento GDPR y agilice sus propios esfuerzos para el cumplir con GDPR. ¡Todavía no es tarde!

El cumplimiento de GDPR no puede lograrse usando una única solución.

GDPR abarca todos los niveles de la empresa, incluyendo la concienciación de los empleados, procesos de negocio y gobernanza, supervisión e informe, y sistemas de información.

Sanciones por incumplimiento del 4% del volumen de negocio total anual o 20 millones de euros.

Afecta a las empresas que procesan datos de carácter personal de ciudadanos de la UE.

Puede requerirse un Delegado de protección de datos (DPO por sus siglas en inglés).

Notificar a las autoridades e individuales de una violación dentro de estrictos plazos estipulados

Debe destacarse el consentimiento, ser claro e incluir las razones por las que se recopila la información

Las personas pueden decidir revocar el acceso a sus datos

Las personas tienen el derecho a obtener, modificar, mover y eliminar sus datos

Incluir protección de datos en la etapa de diseño para nuevos sistemas

¿Qué es lo que realmente exige el GDPR a las organizaciones? Las cinco lecciones fundamentales aprendidas por Veeam

1. **Conocimiento de sus datos** — Identifique la información de carácter personal o PII (por sus siglas en inglés) que su organización recopila, posee y quién accede a ella;.
2. **Gestión de los datos** — Establezca las reglas y procesos para acceder y usar dicha información de carácter personal (PII).
3. **Protección de los datos** — Implemente y garantice que existan controles de seguridad en marcha para proteger la información y responder ante una posible violación de la seguridad de los datos..
4. **Documentación y cumplimiento** — Documente sus procesos, ejecute las solicitudes de datos e informe sobre cualquier problema o violación de los datos dentro de las pautas establecidas.
5. **Revise y mejore constantemente** sus procesos y procedimientos de protección y privacidad de datos

© 2018 Veeam Software. Información Confidencial. Todos los derechos reservados. Todas las marcas registradas son propiedad de sus respectivos titulares.

Veeam Availability Suite proporciona información detallada sobre la protección de datos, auditoría y generación de informes con características de clase enterprise para ayudarle a cumplir con GDPR.

Artículos de GDPR de la UE sobre la gestión de datos y el framework de Veeam	Artículo 5 — Principios relativos al tratamiento de datos de carácter personal Artículo 6 — Licitud del tratamiento Artículo 9 — Tratamiento de categorías especiales de datos de carácter personal Artículo 15 — Derecho de acceso del interesado Artículo 17 — Derecho de supresión (el derecho al olvido) Artículo 20 — Derecho a la portabilidad de datos Artículo 25 — Protección de datos desde el diseño y por defecto Artículo 30 — Registros de las actividades de tratamiento Artículo 32 — Seguridad del tratamiento Artículo 35 — Evaluación de impacto relativa a la protección de datos Artículo 39 — Funciones del delegado de protección de datos Artículo 44 — Principio general de las transferencias
Disponibilidad de sus datos	El artículo 32 de GDPR explica que necesidad garantizar la disponibilidad de los datos nuevamente en caso de producirse un desastre, ataque de malware (ransomware) o cualquier otro problema. Con Instant VM Recovery®, puede hacer que sus datos vuelvan a estar disponibles rápidamente y Veeam Backup & ReplicationTM posee más de 50 opciones de recuperación para un único backup. El artículo 20 de GDPR precisa que el interesado tendrá derecho a recibir los datos personales que le incumban. Las funcionalidades avanzadas de recuperación de Veeam le ofrecen la posibilidad de explorar los backups y réplicas y recuperar los datos en formatos comunes para que pueda enviar dicha información al interesado de la forma oportuna.
Etiquetado de datos personales y analítica	Cuando se identifican datos personales, es crítico monitorizar y auditar con un celo constante. Con Veeam ONETM, puede etiquetar las fuentes de datos de su infraestructura si contienen información de carácter personal y ejecutar informes sobre ellas, revisar los dashboards y llevar a cabo auditorías sobre determinadas actividades (p.ej. qué se está restaurando y quién realiza las restauraciones) en su entorno. Estas son partes importantes de los artículos 6, 32 y 35 de GDPR, así como para que el delegado de protección de datos pueda cumplir con sus obligaciones derivadas del artículo 39 de GDPR.
Retención de datos y el derecho a ser olvidado.	Aunque el derecho al olvido (artículo 17 de GDPR) no es absoluto, no puede guardar datos durante más tiempo del que sea legalmente necesario (dependiendo de las leyes del país y los segmentos verticales). Con la retención de datos, puede marcar claramente los backups obsoletos y Veeam Backup & Replication eliminará los puntos de retención de datos cuando haya pasado el periodo de retención que se describe en el artículo 6 de GDPR.
Descubrimiento de datos (Data Discovery)	Una de las primeras tareas que una organización necesita realizar en su viaje hacia el cumplimiento de GDPR es descubrir qué datos posee. La investigación de las fuentes de datos en un entorno de producción no siempre es una tarea sencilla. Veeam Availability SuiteTM con la tecnología Veeam ExplorerTM, el indexado de archivos guest y Virtual Labs le ofrece a su organización la posibilidad de realizar el descubrimiento de los datos que residen en sus copias.
SureBackup, SureReplica y Virtual Labs	SureBackup y SureReplica están diseñados para automatizar y simplificar el proceso de verificación del backup. Esta es la parte más importante de una estrategia de protección y gestión de datos cuando uno se adhiere a la protección de datos privados del interesado en los artículos 5 y 25 de GDPR. Puede verificar automáticamente cada punto de restauración creado de cada una de las VMs o réplicas, y asegurar que estas funcionarán como cabe esperar en el caso de que tenga que rescatar o informar sobre estos inestimables puntos de restauración. Esto proporciona al equipo encargado de los datos las herramientas necesarias para cumplir con los diversos elementos del marco GDPR de una forma perfecta. Virtual Labs, que es la tecnología subyacente, puede usarse para llevar a cabo la evaluación del impacto de la protección de datos antes de realizar actualizaciones, upgrades o tareas de mantenimiento en sus datos de producción, lo que es uno de los elementos clave del artículo 35 de GDPR.
Informes de ubicación	A medida que los datos entran y salen de su organización, es de la máxima importancia ser capaz de protegerlos y cifrarlos. Sin embargo, también es necesario detectar e informar sobre la ubicación geográfica y estado de estos registros de los interesados. Esto se aplica a los datos de su entorno de producción pero también a todas las copias de esos datos. Con Veeam Availability Suite 9.5 Update 3, podrá etiquetar la ubicación de cada punto de datos e informar sobre todos los datos de producción y el backup correspondiente, copias de backup, cintas y réplicas, su ubicación geográfica y si se ha producido una disparidad entre las ubicaciones. Esto resulta vital para mantener la integridad con el artículo 15 y 44 de GDPR.
Cifrado end-to-end	El artículo 44 de GDPR se refiere a la transferencia de daros entre geografías regionales o internacionales fuera y dentro de la Unión Europea. Durante estos procesos es crucial transferir la información del interesado usando canales cifrados seguros. Veeam ofrece cifrado AES 256-bit end-to-end integrado proporcionándole la capacidad de cifrar sus archivos de backup y datos en el origen (durante el backup), en tránsito y almacenados. Este punto es primordial para cumplir con los artículos 32 y 44 de GDPR en toda su organización y organismos o asociaciones afiliadas.
Control de acceso basado en roles	Muchos artículos de GDPR tratan sobre el registro de actividades, informe de dichas actividades y la definición de quién tiene acceso a según qué datos. Veeam Availability Suite incorpora controles RBAC para permitirle restringir el acceso a determinados puntos de datos dentro de su entorno. Con Veeam Backup Enterprise Manager, que forma parte de Veeam Availability Suite, también puede ofrecer funciones en modo autoservicio para sus usuarios, limitar el acceso a determinados datos o dar acceso cuando sea necesario por sus responsabilidades.
Exclusión de datos	Algunos datos deberían tratarse de forma específica (o incluso excluirse — artículo 9 de GDPR) y mantenerse un registro de ese tratamiento (artículo 30 de GDPR). Al usar las exclusiones en Veeam Availability Suite, puede excluir datos basados en VMs, discos e incluso archivos y carpetas con agentes, para mantener el cumplimiento.

© 2018 Veeam Software. Información Confidencial. Todos los derechos reservados. Todas las marcas registradas son propiedad de sus respectivos titulares.