ManageEngine
EventLog Analyzer

Todo lo que debería saber sobre el cumplimiento del Reglamento General de Protección de Datos de la UE

Tabla de contenido

Introducción 2

Retos, requisitos y planes de acción

- El RGPD no tiene fronteras 3
- Ampliación del alcance de los datos personales 4
- Nueva definición de los principios de protección de datos 5
- Responsabilidad y rendición de cuentas 7
- Notificación de la filtración de datos 9
- Derechos de los interesados afectados 10

Sanciones por incumplimiento 11

Acerca de EventLog Analyzer 12

El papel de EventLog Analyzer para que las organizaciones cumplan con el RGPD 13

Introducción

El aumento en número, escala y costo de las filtraciones de datos personales han hecho que los gobiernos de todo el mundo promulguen estrictas leyes de obligado cumplimiento para proteger los datos personales de los ciudadanos. Europa no es una excepción. Desde 2012, la Comisión Europea ha estado elaborando nuevos reglamentos de protección de datos que pueden mejorar los métodos de tratamiento de datos, mejorar la seguridad de los datos y también armonizar la protección de datos sensibles en todas las naciones europeas.

El gran número de cambios presentes en el nuevo Reglamento General de Protección de Datos, RGPD, (en inglés: General Data Protection Regulation, GDPR) respecto a las normas actuales está despertando mucha atención. El marco RGPD de la UE es complejo de implementar e incluye nuevas políticas de rendición de cuentas, procedimientos de notificación de filtraciones y normas estrictas para los flujos internacionales de datos. Con solo unos pocos meses por delante para cumplir con este nuevo reglamento, es hora de que las organizaciones vuelvan a revisar sus estrategias de seguridad.

Esta guía destaca los principales cambios, retos y planes de acción que las organizaciones deben tomar para asegurar el cumplimiento del RGPD.

Cambios, requisitos y planes de acción

El RGPD no tiene fronteras

El RGPD es una ley global de protección de datos que no solo es aplicable a las empresas que operan en UE. Cualquier organización que se dirija a los consumidores de la UE, que procese datos personales de los ciudadanos de la UE o que analice el comportamiento de personas de la UE debe cumplir con los requisitos del RGPD.

Requisitos:

- Es hora de revisar los marcos de seguridad y las políticas de las empresas. Las organizaciones que no operan dentro de la UE pero que gestionan datos de la UE también deberán adoptar las medidas necesarias para cumplir con el nuevo RGPD.
- Las organizaciones que operan en la UE y cumplen con la legislación vigente de la UE en materia de protección de datos también deberán revisar su marco de seguridad para garantizar que cumplen los estrictos requisitos del nuevo RGPD.

Planes de acción

- Si su organización proporciona bienes o servicios o analiza el comportamiento de los ciudadanos que residen en la UE, estará obligada a cumplir con los requisitos del RGPD antes del 25 de mayo de 2018.
- Revise sus políticas de seguridad y asegúrese de tomar las medidas adecuadas que se indican a continuación respecto al tratamiento de datos personales.
- Elabore las notas de privacidad y demás documentos necesarios que se pueden utilizar para obtener el consentimiento explícito y claro de las personas cuyos datos personales se procesarán. Si ya tiene dichos documentos, considere si hay que revisarlos para asegurarse de que satisfacen el nuevo reglamento.
- Supervise las medidas técnicas y organizativas adoptadas para garantizar la privacidad y seguridad de los datos personales recopilados.
- Si es necesario, nombre funcionarios que puedan supervisar los procesos y tengan responsabilidad sobre la seguridad de los datos personales y sensibles.

Ampliación del alcance de los datos personales

El nuevo reglamento amplía la definición de datos personales y datos personales sensibles.

Según el RGPD, los datos personales son "cualquier información relativa a una persona física identificada e identificable". También incluye "identificadores en línea" tales como direcciones IP e identificadores de cookies.

Aparte de definir los datos personales, el RGPD clasifica algunos de los datos personales como datos personales sensibles. Según el RGPD, los datos personales sensibles son "cualquier dato relativo al origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, salud o vida sexual y datos genéticos y biométricos".

Los nuevos requisitos también imponen que las organizaciones deben tener el consentimiento válido de los "interesados afectados" antes de procesar sus datos personales.

Retos:

- Esta amplia definición de datos personales y la inclusión del "identificador en línea" obliga a las organizaciones que realizan análisis de datos, análisis de comportamiento, publicidad y redes sociales a cumplir con el RGPD.

Planes de acción

- Defina el alcance de los datos con los que trabaja su organización.
- Si los datos se ajustan a la definición de "datos personales" del RGPD, prepare una nota o documento de privacidad que solicite el consentimiento explícito y claro de las personas para poder procesar sus datos.
- Si ya está solicitando el consentimiento para procesar los datos, considere si hay que revisar este procedimiento para asegurarse de que satisface el nuevo reglamento.

Nueva definición de los principios de protección de datos

El principio de protección de datos que constituye la espina dorsal de los requisitos del RGPD sigue siendo el mismo que se establece en la anterior Ley de Protección de Datos, con algunos elementos adicionales.

Los seis principios de protección de datos establecen que los datos personales y los datos personales sensibles deben ser:

- Procesados de manera justa, lícita y transparente.
- Recopilados con fines específicos, explícitos y legítimos y no se deben procesar de ninguna manera que sea incompatible con los fines indicados anteriormente. No se considerará incompatible con los fines iniciales el archivo posterior de los datos para fines públicos o científicos, históricos o estadísticos.
- Adecuados, relevantes y limitados a los datos necesarios en relación a la finalidad para la cual se procesan.
- Exactos y actualizados. Se deben tomar medidas para borrar o rectificar datos personales que sean inexactos.
- Conservados en un formato que permita identificar a los interesados afectados durante un período de tiempo que no supere el tiempo necesario para los fines por los que se procesan. Se pueden archivar por un período más largo sólo si el archivo sirve para intereses públicos o fines científicos, históricos o estadísticos. Además, las organizaciones tienen que tomar las medidas técnicas necesarias para salvaguardar los derechos y la libertad de los individuos.
- Procesados con las medidas técnicas y de organización adecuadas para garantizar la seguridad apropiada, incluyendo protección contra procesos ilegales, pérdida accidental, destrucción o daños.

El nuevo RGPD establece estrictos requisitos de rendición de cuentas que obligan a los responsables de los datos a) garantizar que los principios de protección de datos están en vigor y b) demostrar que la organización cumple con el RGPD.

Requisitos:

- Además de cumplir con los principios de protección de datos como tales, las compañías deberán definir su papel en el tratamiento de los datos (a saber, controladores o procesadores) en conformidad con el nuevo reglamento.
- Las organizaciones deberán revisar el flujo de auditoría de datos para cumplir con los nuevos requisitos de rendición de cuentas del RGPD.

- Las empresas deberán adoptar un nuevo enfoque basado en el riesgo si están procesando datos personales de alto riesgo. Los controladores de datos deben llevar a cabo evaluaciones de impacto de la protección de datos (DPIA) para determinar el riesgo asociado con los datos personales, incluso antes de su tratamiento. Las evaluaciones DPIA también permiten la identificación y mitigación de las filtraciones de datos en una etapa temprana, a fin de reducir el costo de los posibles daños.
- Cuando se inicia un proyecto que trata con datos personales, las organizaciones deberán adoptar un enfoque de privacidad integrada en el diseño para reducir el riesgo de filtraciones de datos.

Planes de acción

- Documentar toda la información relacionada con el tratamiento de datos, incluyendo:
  - Qué tipo de datos personales se están recopilando.
  - Cómo se recopilan, utilizan, transmiten y almacenan.
  - Cómo se protegen contra la revelación en cada paso.
- Aparte de documentar la información incluyendo dónde se almacenan los datos y quién es el propietario de los datos, las compañías deben supervisar constantemente actividades tales como:
  - Quién tiene acceso a los datos personales.
  - Con quién se comparten los datos.
- Supervisar continuamente el archivo o la carpeta donde se almacenan los datos, para identificar e informar instantáneamente sobre cualquier intento de acceso no autorizado o ilegal.
- Mantener un registro de cuánto tiempo deben almacenarse los datos. Y mientras se almacenan, garantizar que los datos están cifrados y a prueba de manipulaciones.

Responsabilidad y rendición de cuentas

Toda organización que procesa datos personales o sensibles actúa como controlador o como procesador. Para garantizar la rendición de cuentas, el RGPD establece el equilibrio adecuado entre las funciones de los controladores y los procesadores, haciéndolos igualmente responsables del cumplimiento.

Controladores de datos

- Según el RGPD, "los controladores son cualquier entidad que, de forma independiente o conjuntamente con otras, determina cómo y por qué se procesan los datos personales".
- Los controladores son responsables de:
  - Revisar todas las actividades de tratamiento de datos.
  - Mantener la documentación relevante de todas las actividades de tratamiento de datos.
  - Realizar las evaluaciones de riesgo de protección de datos para procesos de alto riesgo.
  - Implementar la protección de datos por diseño y por defecto.
  - Designar los procesadores de datos y definir las instrucciones sobre cómo procesar los datos.
  - Notificar a las autoridades en caso de filtración de datos.

Procesadores de datos

- Según el RGPD, un procesador de datos es "cualquier persona (que no sea empleado del controlador de datos) que procesa los datos en nombre del controlador de datos".

  Los procesadores de datos hacen lo siguiente:

  - Procesar los datos siguiendo únicamente las instrucciones documentadas del controlador.
  - Emplear medidas de seguridad y organizativas para evitar filtraciones de datos.
  - Eliminar todos los datos personales al final del procesamiento siguiendo las instrucciones del controlador.
  - Mantener un registro escrito de las actividades de procesamiento realizadas por orden de los controladores.
  - Designar a un Responsable de Protección de Datos (DPO) cuando sea necesario.
  - Notificar a los controladores inmediatamente sobre cualquier filtración de datos.
  - Proporcionar a los controladores toda la información que sea necesaria para demostrar el cumplimiento y permitir que el controlador realice auditorías.

Requisitos:

- Las empresas deben revisar cuidadosamente sus contratos de tratamiento de datos existentes para cumplir con los requisitos cambiantes de rendición de cuentas. Todo nuevo contrato debe cumplir con los nuevos requisitos del RGPD.
- Tanto los procesadores como los controladores deben revisar sus políticas de seguridad, auditoría y filtración de datos para cumplir con los nuevos requisitos del RGPD.
- Las organizaciones tienen que conservar los registros de las medidas adoptadas para impedir las filtraciones de datos.

Planes de acción

- Mantenga un registro claro del flujo de datos dentro de la organización: cómo se recopilan, acceden, comparten y quién es el propietario.
- Diseñe políticas de seguridad que puedan evitar filtraciones de datos. Esto incluye:
  - Supervisión de la red de la organización para detectar cualquier anomalía.
  - Seguimiento de los comportamientos de los usuarios, especialmente los usuarios privilegiados que tienen acceso para procesar los datos personales.
  - Auditar el archivo y la carpeta en la que se guardan los datos personales. Obtener información instantánea siempre que haya intentos de acceso inapropiados o no autorizados a los datos personales.
  - Instaurar medidas organizativas y técnicas adecuadas para proteger la red de la empresa contra ataques y amenazas.

Notificación de la filtración de datos

El RGPD define una filtración de datos personales como "una filtración de la seguridad que conduce a la destrucción, pérdida, alteración, divulgación no autorizada o acceso a datos personales".

Esto explica que una filtración de datos es más que la pérdida de datos. El reglamento también obliga a las organizaciones a denunciar las filtraciones de datos "sin demora indebida y, cuando sea factible", en un plazo de 72 horas.

Requisitos:

- Las empresas deben tener un procedimiento interno de notificación de filtraciones.
- Las organizaciones deben realizar revisiones y auditorías periódicas de la cadena de suministro para asegurarse de que cumplen con los nuevos requisitos de seguridad.
- Las empresas deben implementar un sistema técnico y de seguridad adecuado que facilite la detección instantánea de la filtración de datos. El sistema también debe proporcionar información en profundidad para acelerar la respuesta o contener la filtración en una etapa temprana.

Planes de acción

- Identificar los indicadores de peligros (COI) que causan brechas de seguridad en la red y preparar políticas de seguridad para defenderlos.
- Implementar sistemas de seguridad como cortafuegos e IDS/IPS que puedan ayudar a impedir ataques de seguridad.
- Considerar la posibilidad de implementar soluciones de seguridad que puedan detectar, alertar e informar sobre brechas de seguridad de forma instantánea. Además, las soluciones deben ser capaces de alertar en tiempo real cada vez que se produzca un percance o un intento de filtración.
- Promulgar políticas de seguridad que ayuden a garantizar la integridad de los datos mediante la identificación de:
    - Accesos o intentos de acceso no autorizados.
    - Borrado no autorizado.
    - Compartimiento no autorizado.
    - Copias o intentos de copiar datos personales no autorizados
- Supervisar el comportamiento de los usuarios privilegiados (es decir, los usuarios que tienen acceso a datos personales) para identificar actividades irregulares en caso de suplantación de identidad, e informar inmediatamente.

Derechos de los interesados afectados

Cualquier acción que pueda realizar con datos se considera tratamiento de datos. Sin embargo, el RGPD define límites estrictos sobre lo que las organizaciones pueden hacer y no pueden hacer con la información personal que recopilan.

Derecho a ser informado: Comienza desde el punto de recolección de datos. Las organizaciones deben informar a los interesados afectados, mediante una nota de privacidad, que la información personal recopilada se procesará de manera transparente y justa. También es imprescindible que las empresas obtengan un consentimiento claro y válido de los interesados afectados para procesar su información personal mediante un documento de consentimiento expresado en términos sencillos.

Derecho de acceso: Los interesados afectados tienen el derecho de acceder a su información personal en cualquier momento. Con este requisito, el RGPD garantiza que las personas tienen el derecho de verificar y validar que su información se está tratando de manera justa.

Derecho de rectificación: Si alguien considera que sus datos personales son incompletos o inexactos, tiene el derecho de pedir a la empresa que rectifique sus datos personales. Cuando se recibe una solicitud de rectificación, es responsabilidad del controlador proporcionar a los interesados afectados información sobre las medidas adoptadas respecto a la solicitud sin demora indebida.

Derecho a restringir el tratamiento de datos: Cuando el tratamiento de datos tiene limitaciones, el controlador sólo puede almacenar los datos personales y no puede realizar ningún tipo de tratamiento de los datos. Las personas pueden restringir el tratamiento de datos si:

- Los datos son inexactos o incompletos.
- Los datos se procesan de manera ilegal.
- El controlador ya no tiene ninguna razón (de acuerdo con los principios de protección de datos) para procesar los datos personales.

Derecho a la portabilidad de datos: Las personas, en cualquier momento y sin ningún obstáculo, pueden obtener sus datos y transferirlos a otro controlador para su procesamiento. Este derecho permite a las personas mover, copiar o transferir datos personales fácilmente de un entorno a otro de una manera segura.

Derecho al olvido: El RGPD otorga derechos completos a las personas para solicitar la eliminación o borrado de sus datos personales. La solicitud de borrado de datos puede plantearse en estas circunstancias:

- Cuando el almacenamiento de los datos personales ya no sea necesario en relación con el objetivo para el que se han recopilado o procesado inicialmente.
- Cuando una persona retira el consentimiento para el tratamiento de datos.
- Cuando el interesado afectado solicita que se detenga el tratamiento de datos por tratamiento ilícito de datos o si ha habido una filtración de datos.
- Si los datos tienen que borrarse para cumplir con una obligación legal.

Planes de acción

- Elabore un formulario o nota de privacidad adecuada para obtener el consentimiento claro y explícito de las personas cuyos datos personales se van a procesar.
- Documente las técnicas de procesamiento de datos y los flujos de trabajo para poder proporcionarlos a los interesados afectados cuando ejerzan su derecho de acceso.
- Tome medidas técnicas para borrar los datos personales automáticamente una vez cumplido su propósito.
- Durante el almacenamiento de los datos, asegúrese de que se preserva la integridad de los mismos mediante cifrado.
- Documente la información de cifrado para proporcionarla a los interesados, si es necesario.

Sanciones por incumplimiento

La administración puede imponer una multa de hasta ***10 millones de euros, o el 2% del volumen total de ventas anuales de la compañía en el año anterior***, lo que sea mayor, a aquellas organizaciones que no cumplan las normas RGPD o infrinjan los requisitos del RGPD. Los controladores y los procesadores de datos pueden recibir esta enorme sanción cuando se infrinjan las siguientes condiciones:

- Principios básicos de protección de datos
- Condiciones de tratamiento de datos no personales
- Condiciones para el consentimiento
- Condiciones de tratamiento de datos sensibles
- Derechos de los interesados afectados

El inspector de protección de datos que impone la sanción tomará en consideración la naturaleza e intensidad de la infracción, las medidas de mitigación adoptadas, las medidas técnicas y organizativas implementadas, así como otros factores para decidir el importe de la multa.

Cumplimiento de los requisitos de cumplimiento del RGPD con las soluciones de seguridad de TI de ManageEngine

El portfolio de soluciones de seguridad de TI de ManageEngine tiene una amplia gama de herramientas que ayudan a las organizaciones a cumplir con el reglamento general de protección de datos (RGPD). Nuestra suite incluye:

- **Log360**, una herramienta SIEM integral que ayuda a las empresas a detectar filtraciones de datos, garantiza la seguridad de los datos personales almacenados y rastrea el acceso a los datos personales, garantizando así los requisitos de rendición de cuentas.
- **File Audit Plus**, una herramienta de auditoría y monitorización de archivos en tiempo real que ayuda a rastrear cualquier cambio crítico en el archivo y la carpeta en la que se almacenan los datos personales.

¿Cómo ayudan nuestras soluciones a cumplir con los requisitos de RGPD?

- **La medida técnica y organizativa para defender o mitigar las vulnerabilidades de seguridad:** Las organizaciones pueden implementar Log360 y File Audit Plus para defender o mitigar las vulnerabilidades de seguridad. Estas soluciones tienen la capacidad de monitorizar las actividades de todos los dispositivos y usuarios de la red, e informan de anomalías a los administradores al instante. El profesional de seguridad puede investigar el incidente con los informes exhaustivos y, si se descubre que el incidente es una violación de seguridad (o un intento de filtración), puede tomar medidas inmediatas para evitarlo en las primeras etapas.
- **Auditoría de datos:** La función de monitorización de la integridad de los archivos de Log360 y File Audit Plus monitoriza continuamente los cambios en los datos críticos. También proporciona información exhaustiva sobre quién accedió a los datos, cuándo accedió a ellos y desde dónde. Este informe detallado ayuda a proporcionar información a los interesados afectados sobre los accesos a los datos y también monitoriza los flujos de datos.
- **Seguimientos de auditoría:** La potente capacidad de búsqueda de registros de Log360 ayuda a realizar análisis forenses con facilidad. Uno de los requisitos del RGPD es averiguar la causa raíz de la filtración de datos o del intento de violación impedirla instantáneamente. Nuestra solución puede ayudarle a encontrar la causa raíz de una filtración de datos analizando terabytes de datos de registro en cuestión de minutos. La solución también ofrece la opción de exportar los resultados de la búsqueda como informe forense que se puede enviar al responsable de protección de datos (DPO). Asimismo, la búsqueda se puede convertir en un perfil de alerta para mitigar futuros ataques de seguridad del mismo tipo.

- **Cumplimiento del requisito PIA/DPIA:** Los informes exhaustivos y los perfiles de alertas de Log360 detectan cualquier anomalía de la red e intentos de violación de seguridad instantáneamente. Esto ayuda a contener la filtración de datos en una etapa temprana y también minimiza el daño y el costo en que se podría incurrir si no se actúa a tiempo, cumpliendo así el requisito PIA/DPIA del RGPD.

- **Obligatoriedad de notificación de la filtración:** Log360 envía alertas por correo electrónico o por SMS en tiempo real sobre las filtraciones de datos a los administradores. Esto les ayuda a informar de la filtración a los responsables de mayor jerarquía sin demora indebida. Esta solución viene con más de 600 perfiles de alerta predefinidos basados en distintos IOC. Esto ayuda a detectar instantáneamente los intentos de violación sin mucho esfuerzo. Además, la solución también ofrece una opción para crear perfiles de alertas personalizadas para satisfacer las necesidades de seguridad interna.

Acerca de ManageEngine

ManageEngine proporciona herramientas para la gestión de TI en tiempo real que permite a los equipos de TI cumplir las necesidades de las organizaciones de ofrecer asistencia y servicios en tiempo real. En todo el mundo, más de 60.000 empresas consolidadas y emergentes, entre las que se incluyen más de un 60 por ciento de las empresas incluidas en la lista Fortune 500, confían en los productos de ManageEngine para garantizar un rendimiento óptimo de sus infraestructuras fundamentales de TI, como redes, servidores, aplicaciones, escritorios, etc. ManageEngine es una división de Zoho Corp., que cuenta con oficinas en todo el mundo, incluidos Estados Unidos, Reino Unido, India, Japón y China.

Sobre el autor

Subhalakshmi Ganapathy trabaja actualmente como Analista Senior de Marketing de Productos para Soluciones de Seguridad de TI en ManageEngine. Tiene profundos conocimientos sobre la seguridad de la información y la gestión del cumplimiento. Proporciona orientación estratégica a las empresas sobre Seguridad de la Información y Gestión de Eventos (SIEM), seguridad de la red y privacidad de datos.

Puede ponerse en contacto con Subha en subhalakshmi.g@manageengine.com.

Correo electrónico:
support@eventloganalyzer.com

O bien

Llame al número gratuito:

EEUU: +1 888 720 9500 Reino Unido: 0800 028 6590

Australia: +1 800 631 268 China: +86 400 660 8680

Internacional: +1 925 924 9500

O bien

Visite www.eventloganalyzer.com para obtener información detallada de la solución y sus características.