ManageEngine
DataSecurity Plus

Cumplimiento del GDPR

Satisfaga los requisitos de protección de datos del GDPR d la UE con DataSecurity Plus

Cumpla con el GDPR utilizando DataSecurity Plus

DataSecurity Plus le ayuda a reforzar la postura de seguridad de su organización, a prevenir las pérdidas de datos y a evitar las sanciones relacionadas con el cumplimiento. Cumpla los estrictos requisitos del GDPR utilizando los diversos informes generados por DataSecurity Plus.

Echemos un vistazo a algunos de los artículos más comunes del GDPR, y aprendamos cómo DataSecurity Plus puede ayudarle a cumplir con estos requisitos fácilmente:

Lo que dice el artículo del GDPR:	Lo que usted debe hacer:	Cómo ayuda DataSecurity Plus:
Artículo 5(1)(c) Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario.	Eliminar los datos redundantes, obsoletos y triviales, es decir, los archivos innecesarios de sus almacenes de datos.	Encuentra y elimina los datos basura, incluidos los archivos obsoletos, duplicados y huérfanos, y ayuda a garantizar que sólo se almacenen los datos necesarios y relevantes.
Artículo 5(1)(c) Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario.	Introducir las medidas técnicas y organizativas adecuadas para garantizar la integridad, seguridad y confidencialidad de los datos personales y sensibles.	**Para ayudar a mantener la integridad de los datos:** 1. Audita las acciones de archivos y carpetas, como crear, cambiar nombre, eliminar, copiar, etc., en tiempo real. 2. Activa alertas instantáneas por correo electrónico a los administradores sobre el monitoreo de acciones de archivos sospechosos, como cambios excesivos de permisos, cambios de nombre, etc. 3. Supervisa los intentos fallidos de acceso a sus datos críticos. 4. Mantiene una pista de auditoría infalible de todos los accesos a los archivos para ayudar a las investigaciones forenses. **Para ayudar a mantener la seguridad de los datos:** 1. Detecta y contiene las posibles infecciones de ransomware al instante para evitar la devastadora pérdida de datos. 2. Detecta y evita la pérdida de archivos críticos para la empresa a través de dispositivos USB o como archivos adjuntos de correo electrónico.
Artículo 15(1) El titular de los datos tiene derecho a solicitar qué información sobre él se está tratando.	Localizar y compartir toda la información sobre el titular de los datos almacenada por su organización.	Encuentra la información de identificación personal (PII) de un usuario específico utilizando RegEx o haciendo coincidir una palabra clave única, por ejemplo, el ID del cliente, el nombre, etc. a través del servidor de archivos de Windows y los entornos de failover cluster.

Artículo 15(3) El responsable del tratamiento facilitará una copia de los datos en tratamiento.	Compartir una copia electrónica de todos los datos relevantes para el titular de los datos almacenados por la organización.	Identifica el lugar donde se almacenan los datos personales/sensibles para facilitar los procesos posteriores.
Artículo 16 El titular de los datos puede solicitar al responsable del tratamiento que rectifique la información inexacta que le concierne.	El titular de los datos puede solicitar al responsable del tratamiento que rectifique la información inexacta que le concierne.	Utiliza la detección de datos para encontrar instancias de datos personales/sensibles del titular utilizando un conjunto de palabras clave únicas, por ejemplo, número de identificación nacional, detalles de la tarjeta de crédito, número de licencia, etc.
Artículo 17(1) De conformidad con las directrices mencionadas en la ley, el titular tiene derecho a solicitar al responsable del tratamiento que borre toda la información que le concierne.	De conformidad con las directrices mencionadas en la ley, el titular tiene derecho a solicitar al responsable del tratamiento que borre toda la información que le concierne.	De conformidad con las directrices mencionadas en la ley, el titular tiene derecho a solicitar al responsable del tratamiento que borre toda la información que le concierne.
Artículo 24(2) Deben implementarse políticas de protección de datos adecuadas para proteger los derechos de los titulares interesados.	Aplicar las medidas técnicas y organizativas necesarias para garantizar un alto nivel de privacidad de los datos.	1. Utiliza políticas predefinidas para ayudar a prevenir transferencias de datos injustificadas a dispositivos USB, monitorear la integridad de los archivos y mucho más. 2. Utiliza mecanismos automatizados de respuesta a las amenazas para apagar los sistemas infectados, desconectar las sesiones de los usuarios maliciosos, etc.
Artículo 25 (2) Practicar la minimización de datos y garantizar que los datos personales no sean accesibles para un número indefinido de personas.	Localizar y revertir los privilegios y permisos excesivos otorgados a los usuarios.	1. Encuentra usuarios con acceso de control total a sus recursos compartidos de Windows. 2. Localiza todos los archivos y carpetas que se han compartido con todo el mundo.

Artículo 30(1) Se mantendrá un registro de todas las actividades de tratamiento junto con detalles sobre los datos sensibles tratados y las medidas técnicas utilizadas para salvaguardar los datos.	Averiguar qué datos son sensibles, quién puede acceder a ellos y establezca una auditoría para tener un registro infalible de lo que ocurre con sus datos. Mantener detalles precisos sobre las medidas adoptadas para garantizar la seguridad de los datos.	1. Localiza instancias de datos personales/sensibles almacenados en servidores de archivos de Windows y failover clusters utilizando una política de descubrimiento de datos GDPR dedicada. 2. Busca los números de identificación nacional, los datos de la tarjeta de crédito, el número de licencia y mucho más. 3. Descubre quién tiene qué permiso sobre los archivos que contienen datos personales sensibles. 4. Audita la actividad de los usuarios en los archivos con detalles sobre quién accedió a qué, cuándo y desde dónde.
Artículo 32(2) Se aplicarán medidas técnicas y organizativas para hacer frente al riesgo de destrucción accidental o ilícita, pérdida, alteración, divulgación no autorizada o acceso a los datos personales transmitidos o almacenados.	Aplicar medidas preventivas y de detección para proteger los datos que se procesan de un incidente de seguridad.	**Para hacer frente al riesgo de posibles pérdidas de datos:** 1. Monitorea en su organización el uso de dispositivos de almacenamiento extraíbles, como los USB. 2. Bloquea el movimiento de archivos que contengan datos personales en dispositivos USB, o a través del correo electrónico como archivos adjuntos. 3. Proporciona advertencias contextuales mediante avisos del sistema sobre el riesgo de trasladar datos críticos para el negocio a dispositivos de almacenamiento extraíbles o por correo electrónico como archivos adjuntos. 4. Reduce los tiempos de respuesta a los incidentes con alertas instantáneas y un mecanismo de respuesta a las amenazas automatizado.
		Para hacer frente al riesgo de accesos no autorizados o de divulgación: 1. Alerta e informa sobre accesos injustificados, o picos repentinos de accesos y modificaciones de archivos, incluyendo cambios de permisos, eliminaciones, etc. 2. Detecta archivos con vulnerabilidades de seguridad como: * Archivos de usuarios antiguos. * Archivos críticos que permiten el acceso de control total a los usuarios. * Archivos sobreexpuestos, o archivos accesibles para todo el mundo. 3. Supervisa los picos repentinos de intentos fallidos de acceso a sus archivos/carpetas. 4. Revisa periódicamente los derechos de acceso y los permisos de los archivos.

		Para hacer frente al riesgo de destrucción accidental o ilegal: 1. Mantiene un registro completo de todas las eliminaciones de archivos y carpetas, junto con detalles sobre quién eliminó qué, cuándo y dónde. 2. Descubre y pone en cuarentena posibles infecciones de ransomware.
Artículo 33(3) En caso de violación de los datos personales, la notificación debe incluir las medidas adoptadas para abordar y mitigar los posibles efectos adversos de la violación de los datos personales.	Analizar e investigar las posibles causas y consecuencias de una violación de datos.	Ayuda a analizar la causa raíz y el alcance de la violación de datos mediante amplios registros de todas las actividades relacionadas con archivos y carpetas en servidores de archivos de Windows, failover clusters y entornos de grupos de trabajo. Proporciona detalles sobre quién accedió a qué, cuándo y dónde.
Artículo 35(7)(d) Una evaluación de impacto de la protección de datos debe incluir las medidas previstas para hacer frente a los riesgos, incluidas las salvaguardias y las medidas de seguridad para garantizar la protección de los datos personales.	Identificar y evaluar los riesgos para sus datos personales sensibles. Evaluar el riesgo y aplicar medidas para mitigarlo.	1. Calcula la puntuación de riesgo de los archivos que contienen datos personales/sensibles mediante el análisis de sus permisos, el volumen y el tipo de reglas infringidas, los detalles de la auditoría, etc. 2. Identifica los archivos que son vulnerables debido a problemas de higiene de permisos.

DataSecurity Plus

ManageEngine DataSecurity Plus es una plataforma unificada de visibilidad y seguridad de datos. Au cambios en los archivos en tiempo real, activa respuestas instantáneas a eventos críticos, detiene las intrusiones de ransomware y ayuda a las organizaciones a cumplir con numerosas regulaciones de T el almacenamiento de archivos y los permisos de seguridad, elimina los archivos basura y detecta las vulnerabilidades de seguridad. Los usuarios pueden evaluar los riesgos asociados al almacenamient sensibles localizando y clasificando los archivos que contienen información personal identificable (PII información de tarjetas de pago (PCI) e información de salud protegida electrónicamente (ePHI). Tam evita las pérdidas de datos a través de USB, correo electrónico, impresoras y aplicaciones web; mon integridad de los archivos y audita el uso de las aplicaciones en la nube. En conjunto, estas funciones garantizan la protección integral de los datos en reposo, en uso y en movimiento.

Para explorar estas funciones y ver DataSecurity Plus en acción, .
Para obtener más información sobre DataSecurity Plus, visite .

Download free trial $ Get a quote

Explore las funciones de DataSecurity Plus

Auditoría del servidor de archivos

Audite e informe sobre los accesos y modificaciones de los archivos, con alertas en tiempo real y respuestas automatizad para las actividades críticas de los archivos.

Learn more

Análisis de archivos

Analice la seguridad y el almacenamiento de los archivos, gestione los archivos basura, optimice el uso del espacio en d e identifique las vulnerabilidades de los permisos.

Learn more

Evaluación del riesgo de los datos

Analice la seguridad y el almacenamiento de los archivos, gestione los archivos basura, optimice el uso del espacio en d e identifique las vulnerabilidades de los permisos.

Learn more

Prevención de la pérdida de datos

Detecte e interrumpa las pérdidas de datos a través de los USB correo electrónico, las aplicaciones web y las impresoras; monit la actividad de los archivos en los endpoints; y mucho más.

Learn more

Protección en la nube

Supervise el tráfico web de la empresa y aplique políticas para bloquear el uso de aplicaciones web inapropiadas, de riesgo o maliciosas.

Learn more