Solution Brief

¿Está su empresa preparada para la Regulación General de Protección de Datos de la UE (GDPR)?

RightsWATCH

De acuerdo con el Reglamento General de Protección de Datos de la UE (GDPR), que entrará en vigor el 25 de mayo de 2018, con tan solo un periodo de adaptación de 2 años, las empresas se vuelven más responsables que nunca en caso de fuga de datos confidenciales.

Si se producen violaciones de seguridad, las organizaciones podrán ser multadas con el 4% de sus ingresos globales o hasta 20 millones de €, la cantidad que sea mayor. Además, la organización retiene su responsabilidad ante cualquier persona que haya sido "dañada" por la violación de sus datos. También está obligada a notificar la fuga dentro de las 72 horas siguientes al conocimiento de la violación. Al mismo tiempo, la insuficiencia de políticas y controles documentados se convierte en una segunda violación, y la Oficina de Protección de Datos impone también responsabilidad personal a los responsables.

Con este panorama, las organizaciones deben empezar a revisar sus políticas de seguridad de datos con el fin de prepararse para el Reglamento General de Protección de Datos.

La pregunta es:

¿Tenemos las herramientas adecuadas y los recursos asignados para adaptarnos al nuevo reglamento en tan solo dos años?

¿Qué es el Reglamento General de Protección de Datos de la UE (GDPR)?

El GDPR sustituirá a la actual Directiva 95/46/CE sobre protección de datos y su objetivo es hacer frente a la evolución tecnológica que ha acelerado las brechas de seguridad. Problemas críticos tales como las operaciones transnacionales, la evolución de las redes sociales y la computación en la nube que no estaban cubiertos de manera coherente y relevante. El nuevo Reglamento GDPR trasciende las leyes de privacidad de datos locales y está diseñado para proporcionar un marco jurídico de alcance más amplio y estricto sobre la privacidad de los datos personales.

Cómo ayuda RightsWATCH a su organización a estar preparados para la GDPR UE

La clasificación de los datos es la base de cualquier iniciativa para disponer de información GRC (Governance, Risk and Compliance) adecuada ya que se limita la responsabilidad corporativa, reduce el riesgo de fuga de datos, al tiempo que aumenta la sensibilización y competencia de los usuarios.

RightsWATCH es un buen aliado por buenas razones: es una solución fácil de usar, digitaliza las políticas de clasificación de las empresas, automatiza el proceso y simplifica la experiencia del usuario.

RightsWATCH ayuda a las organizaciones a cumplir los requisitos GDPR EU de clasificación y etiquetado de datos sensibles al tiempo que aplica los derechos de acceso y uso de la información personal independientemente de donde se encuentre la información.

Adicionalmente, RightsWATCH ofrece registros de auditoría que permiten el análisis forense de los datos, por lo que su organización puede saber "quién", hizo "qué", "cuándo" y "cómo" con los datos.

Los retos de la GDPR UE

A continuación se muestran los retos más importantes a los que se enfrentan las organizaciones y cómo RightsWATCH puede ayudar para conseguir su cumplimiento.

I - Foco en los Datos Personales (PII): El derecho a ser olvidado

La GDPR UE define los datos personales rigurosamente, en referencia a cualquier información que pudiera utilizarse, por sí sola o en combinación con otros datos, para identificar a un individuo.

Los ciudadanos de la UE tendrán que dar explícitamente su consentimiento para el almacenamiento, uso y manejo de sus datos personales, y tendrán derecho a acceder, modificar o solicitar su supresión. Además, podrán oponerse a ciertos tipos de usos, como para fines de marketing, etc.

Cómo puede ayudar RightsWATCH:

- Permitiendo que la información de identificación personal (PII) se clasifique y proteja de forma automática, siempre que se recibe, usa o comparte en forma de un archivo no estructurado (por ejemplo: correo electrónico, documento de Word, PDF, hoja de cálculo Excel o PowerPoint).

- Proporciona un motor inteligente de políticas que identifica los datos personales y toma acciones en tiempo real para clasificar el archivo de acuerdo con la política de la empresa, aplicar marcas de protección, etiquetas para identificar la información y reducir la responsabilidad corporativa.

- Aplicando etiquetas visuales a los correos electrónicos y documentos para educar a los usuarios acerca de la sensibilidad de la información y así garantizar su sensibilización y cumplimiento de las políticas.

II - Notificación obligatoria de la violación de los datos y gestión de la información

Las organizaciones deben realizar un seguimiento activo de cómo y dónde se almacenan los datos y cómo se utilizan. Esto significa la adopción de herramientas de gestión de riesgos, y el diseño y realización de sus operaciones con seguridad y privacidad. Además, cualquier organización directamente involucrada con el tratamiento de los datos, o con más de 250 empleados debe designar un Data Protection Officer.

Por otro lado, la UE requiere que las organizaciones reporten las violaciones de datos a los reguladores y a las personas afectadas dentro de las 72 horas siguientes a la violación junto a las medidas de seguridad en vigor en aquel momento. Las empresas serán evaluadas por la autoridad de supervisión competente para determinar responsabilidades y asegurar el cumplimiento futuro.

Cómo puede ayudar RightsWATCH:

- Facilita un registro para auditoría integral que permite la documentación y el rastro de cualquier acceso autorizado y no autorizado a los datos confidenciales.

- "Alimenta" una herramienta SIEM (Security Information and Event Management) para la generación de conocimiento. Con esta información las empresas son capaces de aprovechar la SIEM para correlacionar eventos, generar cuadros de mando, informes de alarmas y conocer en tiempo real quién está haciendo qué, cuándo y cómo con la información clasificada.

- Etiquetado y marcado de datos sensibles para ayudar a identificar la información que requiere un manejo especial, lo que permite añadir fácilmente descriptores adicionales, textos para cada clasificación o etiquetas de texto para cada clasificación de seguridad.

III - Responsabilidad conjunta

La UE define a los “Controladores” - responsables del tratamiento de los datos - como las organizaciones que adquieren datos de los ciudadanos de la UE y a los “procesadores de los datos” como las organizaciones que pueden gestionar, modificar, almacenar y analizar los datos en nombre o junto con los controladores (como proveedores de la nube y subcontratistas).

De acuerdo con la GDPR UE, ambas partes son conjuntamente responsables de cumplir con las nuevas normas. Esto significa que si una organización externaliza la entrada de datos o el análisis de un tercero, o procesa los datos en nombre de otra organización, será también responsable.

Cómo puede ayudar RightsWATCH:

- Alertar a los usuarios cuando los datos sensibles abandonan la organización con el fin de advertir o evitar la salida de información.

- Controla el acceso a los datos sensibles a través de terceros. RightsWATCH aplica la protección a e-mails, documentos y cualquier otro formato de archivo para que se pueda compartir de forma segura a través de cualquier medio de comunicación.

- Registra los eventos a nivel de cliente y de servidor en una base de datos central para propósitos de auditoría y análisis forense.

www.watchfulsoftware.com
© Copyright Watchful Software, Inc. 2018 All Rights Reserved