Destructoras
Rexel

Porqué una política de seguridad del papel es integral
para el cumplimiento de la GDPR.

Acerca de este documento

Este documento le proporcionará **un resumen de lo que busca conseguir el GDPR**, los problemas que puede representar para las organizaciones.

El propósito de este documento es brindarle una introducción a la Norma de Protección de Datos Generales (GDPR) y qué impacto tendrá en diferentes negocios, de forma que pueda desarrollar un marco para una política de seguridad del papel para su propios negocios, antes de que las normas entren en vigor en mayo de 2018.

Por tanto, ¿qué es la GDPR? Requiere que las organizaciones apliquen buenas prácticas de seguridad para datos electrónicos y basados en papel y, en caso de violación de datos, notificar a las personas afectadas o potencialmente afectadas.
El alcance de la GDPR se extiende globalmente a todas las organizaciones que controlan o procesan datos identificables personalmente acerca de personas en la UE, sin consideración de la ubicación geográfica de esas organizaciones. Los requisitos de la GDPR se aplican a datos personales tanto electrónicos como basados en papel y significa que todas las organizaciones deben abordar los requisitos de la GDPR si manejan datos identificables personalmente originados en la UE.

Mientras que la seguridad de los datos electrónicos está adecuadamente bien presente para muchas organizaciones, muchas no abordan adecuadamente la seguridad de los datos en papel.
De hecho, dos tercios de las oficinas admiten que no destruyen información confidencial[1]. Esto pone a las organizaciones en riesgo de incumplir la GDPR, y a los sujetos de los datos ante el riesgo de fraude y robo de identidad. Teniendo esto en cuenta, Rexel, una marca líder de máquinas destructoras, anima a las organizaciones a revisar sus políticas y prácticas de seguridad en relación con datos tanto electrónicos como en papel.

LA NORMA DE PROTECCIÓN DE DATOS GENERALES

Un resumen

La GDPR busca proteger los derechos de privacidad de personas en Europa, tanto si son ciudadanos de la UE como si no lo son. Estos derechos de privacidad incluyen, pero sin limitación:

Transparencia
El derecho de recibir información clara sobre como las organizaciones procesan la información personal.

Consentimiento
El derecho de controlar cómo las organizaciones utilizan la información personal.

Seguridad
El derecho de tener información acerca de cómo las organizaciones protegen adecuadamente la información personal.

Limitación de recogida y propósito
El derecho de esperar que las organizaciones minimicen su recogida y usos de la información.

Notificación de violación
El derecho de ser informado en el caso de una violación de datos.

La GDPR forma parte del plan de la Comisión Europea para modernizar y armonizar las normas de protección de datos.

Aunque el objetivo principal de la GDPR es reforzar los derechos de privacidad online, también aborda la privacidad de datos en papel.

Se centra en combatir los retos siempre crecientes de la protección y privacidad de datos, la exposición a violaciones de seguridad, pirateo y otros procesos ilegales.

LA NORMA DE PROTECCIÓN DE DATOS GENERALES

¿Qué ha cambiado?

Los siguientes puntos **identifican las áreas específicas en la GDPR que son nuevos** derechos para personas o los derechos existentes según la Ley de Protección de Datos(DPA) que se han reforzado como parte de la GDPR:

Portabilidad de datos y el derecho al olvido

- Los individuos tienen ahora el derecho de transportar sus datos personales de una organización a la siguiente.
- Los datos personales deben proporcionarse en un formato estructurado y legible por máquina.
- Una persona puede solicitar el borrado o la eliminación de datos personales.

Notificación de violación de datos

- Cualquier violación debe ser notificada a la autoridad supervisora.
- También debe notificarse de la violación a los individuos afectados.

Inventario

- Las autoridades locales ya no tienen que estar informadas de que se están procesando datos personales.
- Las organizaciones deben mantener un registro de actividades de procesamiento bajo su responsabilidad.

Evaluaciones del impacto de la protección de datos y seguridad

- Las DPIAs son un medio para identificar riesgos elevados para los derechos de privacidad de los individuos.
- Los requisitos y recomendaciones de seguridad deben basarse en una evaluación del riesgo.

Gestión y responsabilidad de datos

- Las organizaciones deben también poder demostrar cumplimiento con la GDPR.

La falta de cumplimiento de la GDPR puede resultar en **multas de hasta 20 millones de euros, o el 4 % de los ingresos globales de la empresa**, cualquiera que sea la mayor. Además, un sujeto de los datos tiene el derecho de demandar a una organización ante los tribunales.

LA NORMA DE PROTECCIÓN DE DATOS GENERALES

¿Cómo se aplica?

La introducción de la GDPR en mayo de 2018 tendrá impacto en los siguientes puestos:

Controladores de datos – dicen cuándo y porqué se procesan los datos personales.
Procesadores de datos – personas actuando en nombre del controlador.

Es responsabilidad de estas dos figuras asegurarse de que sus clientes cumplen totalmente todos los aspectos de la GDPR, para evitar incurrir en alguna multa.

Un Procesador de datos o un Controlador de datos puede necesitar **nombrar a un Responsable de la Protección de Datos** y mantener registros de todas las actividades de procesamiento que realizan en nombre de los clientes.

La GDPR cubre datos personales y datos personales sensibles en formatos electrónico y físicos

Es importante considerar para qué tipos de datos se aplicará la GDPR, antes de crear una política de cumplimiento para su organización.

Los datos en el ámbito de la GDPR incluyen cualquier información acerca de una persona identificable. Algunos ejemplos de datos personales cubiertos por GDPR incluyen el nombre completo, la dirección de e-mail y el número de teléfono.

La GDPR también aplica protecciones adicionales a una **subcategoría de datos personales, llamada datos personales sensibles**.

La GDPR se relaciona con datos personales manejados por organizaciones tanto en **formatos electrónicos como físicos**, tales como documentos en papel.

Un marco empresarial para el cumplimiento de la GDPR

Las organizaciones tienen tres áreas principales que deben revisarse para conseguir el cumplimiento con la GDPR. Afrontando estos tres componentes, la empresa será capaz de construir marcos claros de una política de seguridad de datos para cada aspecto, lo cual ayudará a respaldar el cumplimiento en todas las áreas de la GDPR.

Estos componentes son:

Personas

La propiedad y responsabilidad del personal respecto a cualquier dato procesado por ellos en la organización son críticos. Una organización debe establecer reglas claras para cada uno de los empleados buscando la adecuada gestión de todos los datos electrónicos o en papel que hay en el negocio. Estas normas ponen en marcha los requisitos de la GDPR en relación con el manejo de todos los datos. Por ejemplo, puede ser que desee introducir reglas claras acerca del uso de documentos en papel que contienen información sensible y el proceso para la correcta destrucción del documento una vez utilizado, basado en el nivel de sensibilidad de los datos contenidos en el mismo.

Procesos

Esto se refiere a procesos dentro de la organización. Por ejemplo, para gestionar el uso de datos tal como procesamiento o almacenaje de datos sobre clientes. Es crucial que las empresas estén revisando todos sus procesos actuales relativos a datos. Una vez identificados los puntos débiles y las lagunas existentes en sus procedimientos actuales, debe desarrollarse un plan marco por parte de la empresa que hará que estas áreas se refuercen o sustituyan, cuando sea necesario, para cumplir la GDPR.

Tecnología

También las capacidades y requisitos de TI actuales deben revisarse y ajustarse en consecuencia antes de mayo de 2018. Corresponde a las empresas individuales asegurarse de que cualquier sistema existente que no apoye totalmente las normas sea mejorado o sustituido para evitar incurrir en alguna multa potencial, después de que la GDPR entre en vigor.

¿Porqué la seguridad en papel es importante?

Habiendo tratado lo que requiere la GDPR que hagan las empresas, ahora es pertinente abordar el tema de la seguridad en papel en las organizaciones y por qué es una preocupación clave para las empresas, a medida que se preparan para cumplir los requisitos de la GDPR.

De hecho, un informe PwC de 2014, realizado en conjunción con la empresa de gestión de registros Iron Mountain[2] –que evaluó cómo perciben y gestionan las compañías europeas del mercado medio sus riesgos de información – descubrió que dos tercios de sus encuestados manifestó que la gestión de los riesgos asociados con los registros en papel era una preocupación de primer nivel.

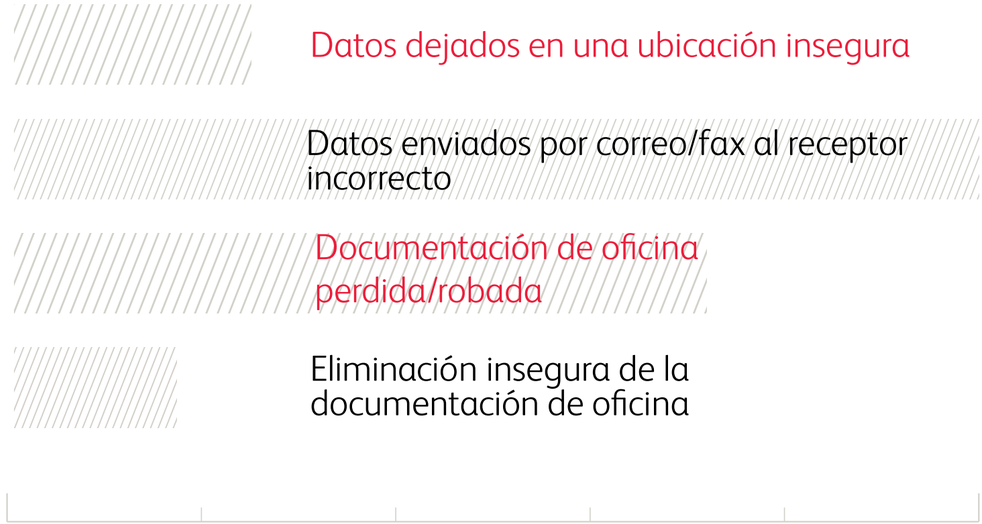
Mientras que las amenazas digitales suponen un punto clave en la agenda de una organización, sería un error asumir que los ***riesgos de seguridad del formato papel*** *han desaparecido.*

El papeleo de oficina aún explica muchas violaciones de seguridad habituales

Más de 598 incidentes de seguridad de datos registrados entre julio y septiembre de 2016 por el regulador de protección de datos del RU, la Oficina del Comisionado de Información (ICO):

14 % se debieron a la pérdida o robo de papeleo de oficina, **un 19 % adicional** se enviaron por correo o por fax al receptor incorrecto **y 4 %** se debieron a datos dejados en una ubicación insegura. **Otro 3 %** se debieron a la eliminación insegura del papel. Por lo tanto, a pesar de un incremento exponencial en las tecnologías digitales, **40 % de los incidentes** fueron atribuibles al papel[3].

El 40 % de los incidentes de seguridad de datos se atribuyeron al papel



La cooperación del usuario es crítica para el cumplimiento de la GDPR

Sí podemos concluir que la seguridad en el papel sigue siendo vital para la seguridad de la información, entonces la pregunta es:
¿qué pueden hacer las organizaciones al respecto?

Rexel se especializa en proporcionar destructoras de papel a organizaciones, con la capacidad de colaborar directamente con organizaciones tales como Kensington, el líder mundial en seguridad física para hardware de TI cuando se comparten conocimientos del cliente, lo cual nos ha permitido obtener conocimientos valiosos de las necesidades, deseos y retos a los que se enfrentan las organizaciones que buscan protegerse y cumplir con la GDPR.

Estos conocimientos nos han llevado a creer que hay dos barreras para la destrucción eficaz de documentos en organizaciones:

Falta de concienciación

Las empresas están ignorando la importancia del papel en un lugar de trabajo cada vez más digital y, por lo tanto, no se están tomando el tiempo de abordar los temas de seguridad asociados con documentos en papel. Incluso cuando existe una política, si la regulación no se comunica eficazmente a todos los niveles de la empresa, provoca a menudo una falta de concienciación.

Fácil de usar

La disponibilidad de máquinas destructoras adecuadas es crucial para el éxito de una política de destrucción eficaz. Demasiado a menudo las empresas o las oficinas confían en destructoras manuales ineficaces que no son adecuadas para cumplir con sus capacidades, dejando a los empleados sin capacidad para destruir documentos eficaz y productivamente.

Una vez las barreras para implantar una política de destrucción eficaz han sido identificadas en la organización, el siguiente paso es determinar una solución adecuada para combatir estas barreras.

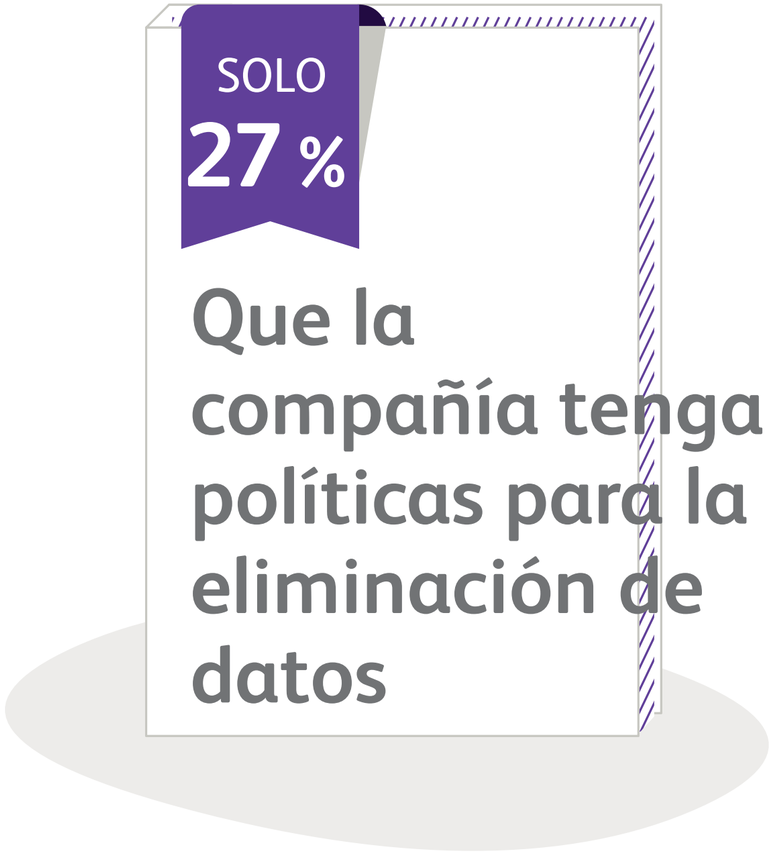
Cooperación del usuario uno para cumplimiento de la GDPR

Falta de concienciación

Los empleados generalmente realizan actividades que están claramente destacadas como una prioridad por sus directores.

Teniendo esto en cuenta, una política de destrucción de documentos clara y firme puede resolver muchas ineficacias

El estudio PwC/Iron Mountain de compañías europeas del mercado mediano de 2014[2] indica que solo un 40 % posee unas directrices claras para el empleado sobre la eliminación interna y el almacenamiento de los documentos físicos, y solo un 27 % dispone de políticas de la empresa relativas a la seguridad, almacenamiento y eliminación de información confidencial de forma segura.



Cooperación del usuario dos para cumplimiento de la GDPR

Fácil de usar

Una segunda causa habitual de incumplimiento de destrucción de documentos por parte del empleado es la dificultad y el tiempo que tarda la tarea.

Aunque los trabajadores pueden tener acceso a destructoras, no todos los trabajadores pueden destruir documentos necesarios si la actividad tarda un tiempo significativo o es difícil de gestionar.

Previsiblemente, ninguna organización desea invertir en destructoras que sus empleados probablemente no utilizarán debido a baja productividad o barreras a la facilidad de uso, por lo tanto, estos temas deben resolverse para asegurar el máximo uso.

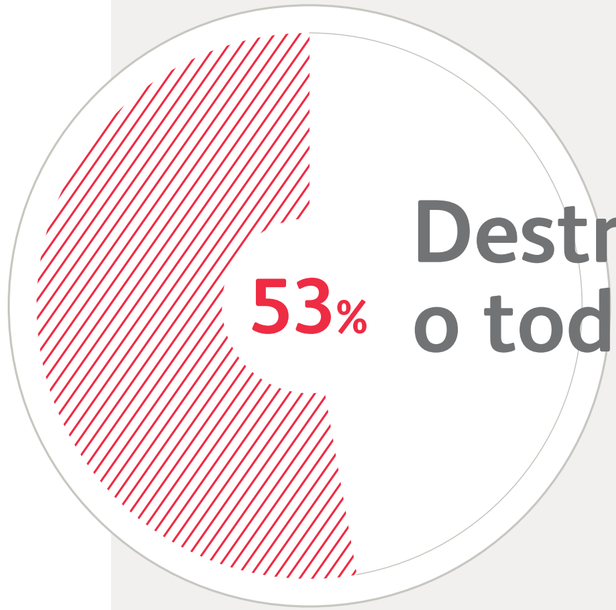
Aumentar la productividad del empleado con la tecnología de alimentación automática

Conclusión:

Las destructoras de alimentación automática son una respuesta directa a la necesidad de que las organizaciones animen a los empleados a cumplir con la seguridad en papel.

Nuestra investigación[4] muestra que el 53 % de los empelados adoptan un comportamiento de destrucción de lote, en el cual el empleado crea una pila de múltiples documentos antes de que sienta que vale la pena ir hasta la destructora.

Al permitir a los empleados destruir pilas de papel, una investigación independiente descubrió que los empleados podían **gastar un 98 % menos de tiempo destruyendo**[5] y estar más inclinados a destruir más frecuentemente.



6 puntos clave de GDPR a considerar

1. Considerar nombrar a un Responsable de la Protección de Datos

Este responsable debe asumir plenamente las responsabilidades de la organización relativas a la GDPR y tener una comprensión completa de los datos que en su organización cuentan como 'personales', dónde se conservan, quién tiene acceso a ellos, cómo detectar violaciones cuando se producen y a quién notificarlas. **El Responsable de la Protección de Datos no tiene por qué ser un empleado, se puede externalizar esta función.**

2. Evaluar sus sistemas

Revise todos los contratos, el soporte tecnológico, los procedimientos y herramientas que tengan relación con el procesamiento, la manipulación, el almacenamiento y el borrado de datos para permitirle identificar cualquier debilidad o laguna que requiera que se hagan cambios.

3. Desarrollar una estrategia

Construir una nueva estrategia que asegurará un cumplimiento total con la GDPR. Esta estrategia puede abarcar nuevas inversiones en tecnología, revisar procedimientos y responsabilidad del personal para el procesamiento de datos y crear nuevos puestos en la organización.

4. Implantar una nueva política de la organización

El siguiente paso hacia el cumplimiento de la GDPR es poner en marcha su plan en todos los niveles de la organización. Invertir e introducir nuevas tecnologías y sistemas necesarios en el lugar de trabajo y publicar una guía informativa de manipulación y procesamiento de datos.

5. Compromiso del empleado

Lanzar su nueva política de cumplimiento de datos a todo el personal, proporcionar formación, información y guías a los empleados de forma que estén formados y sean conscientes de los cambios que tienen lugar y su responsabilidad en asegurarse de que la empresa cumple los requisitos de la GDPR.

6. Revisar y mejorar

Después de lanzar su plan de cumplimiento de la GDPR, ahora es el momento de revisar y mejorar antes de que las normas entren en vigor. Al identificar cualquier mejora necesaria mucho antes de la fecha límite de la GDPR, cuando llegue mayo de 2018, su organización se habrá adaptado con éxito y eficacia a los cambios y será completamente conforme.

FUENTES

1 envirowaste.co.uk/blog/articles/third-companies-shred-private-documents

2 Más allá de las buenas intenciones: La necesidad de pasar de las intenciones a los hechos para gestionar el riesgo de la información en el mercado de nivel medio, informe PwC conjuntamente con Iron Mountain, junio de 2014.

3 ico.org.uk/action-weve-taken/data-security-incident-trends

4 Evaluación de las destructoras de alimentación automática. Elaborada para ACCO Brands por Deep Blue Insight

5 Prueba independiente de Intertek Testing & Certification Ltd, junio de 2012
Ahorro máximo al utilizar la Auto+ 500X en comparación con una destructora de alimentación tradicional con un nivel de precio similar.
La investigación demuestra que se tarda una media de 14 minutos y 25 segundos para introducir manualmente 500 hojas de papel en una destructora de alimentación manual tradicional - pero solo 14 segundos para cargar el mismo número de hojas en una destructora Auto+ 500X.