DocuWare

White Paper
RGPD

DocuWare GmbH
Therese-Giehse-Platz 2
82110 Germering
www.docuware.com (http://www.docuware.com)

Contenido

1 El cumplimiento del reglamento RGPD de la Unión Europea es una obligación

RGPD o Reglamento general de protección de datos es un nuevo conjunto de normas y normativas europeas relacionados con la privacidad y gobernanza de datos. Este reglamento no es solo aplicable a empresas europeas sino también a empresas que hacen negocios en Europa o con clientes europeos. El reglamento requiere el consentimiento activo de los clientes y les proporciona nuevas capacidades de portabilidad para controlar la transmisión de su propia información. Establece sanciones importantes para el no cumplimiento del reglamento. Todo esto entra en vigor a partir de mayo de 2018

Existe la tentación a asumir que nada en la RGPD es realmente diferente. Después de todo, Europa cuenta con sus regulaciones de gobernanza y protección de datos desde 1995. Pero el reglamento RGPD es un conjunto de principios al que se ha otorgado la máxima prioridad y requiere la atención de todas las organizaciones.

Los seis principios del reglamento RGPD

En esencia, el RGPD es básicamente acerca de la protección de datos personales o información de identificación personal (PII). Se pueden considerar datos personales cualquier información que permita que alguien, directa o indirectamente, identifique a otra persona física. Esto incluye información como pueden ser nombres, direcciones de correo electrónico, publicaciones en medios sociales, información física, fisiológica o genética, información médica, ubicaciones, datos bancarios, cookies e identidad cultural.

Esta protección se establece en seis principios:

1 Procesados de forma jurídica, justa y transparente.

2 Recopilados por motivos legítimos, explícitos y específicos.

3 Adecuados, relevantes y limitados a lo necesario.

4 Precisos y, cuando proceda, actualizados.

5 Retenidos solo durante el tiempo necesario.

6 Procesados de forma adecuada de manera que se mantenga la seguridad.

las empresas no solo debe cumplir con los seis principios generales del RGPD, además deben demostrar su cumplimiento normativo a través de documentación y/o procedimientos operativos estándar (POE) relacionados con la protección de datos.

Los datos importantes a tener en cuenta

1 **RGPD es un reglamento de la UE que deroga todo los demás:** Al contrario que las anteriores directivas de la UE sobre protección de datos, el nuevo reglamento RGPD es una normativa europea. Esto significa que entrará en vigor inmediatamente a partir del 25 de mayo de 2018, después de un periodo de transición de dos años. Al contrario que una directiva, este no requiere la aprobación de ninguna legislación habilitadora por parte de los estados miembros. Al igual que cualquier normativa de la UE, el RGPD es un derecho comunitario. Este deroga las leyes nacionales y todas las directivas de la Unión Europea anteriores.

2 **Sanciones altas:** Las multas por no cumplir con el reglamento son bastante elevadas. Las multas impuestas pueden alcanzar hasta los 20 millones de euros o 4% de los ingresos anuales globales del ejercicio anterior, el que sea más alto (Artículo 83: Condiciones generales para la imposición de multas administrativas)

3 **Consentimiento explícito del consumidor:** El consentimiento válido debe ser específico para los datos recopilados y los motivos para los que se utilizan los datos (Artículo 7; definido en el artículo 4). Además, los responsables del tratamiento deben ser capaces de demostrar el "consentimiento" (opt-in) y el consentimiento se puede retirar.

4 **Cumplimiento fuera de la Unión Europea:** Las antiguas cláusulas de excepción para empresas no europeas ya no funcionan. Anteriormente, empresas no europeas utilizaban provisiones de puerto seguro (safe harbor) para cumplir con las regulaciones originales de protección de datos. En julio de 2000, la Comisión Europea (CE) decidió que las empresas americanas que cumplían con los principios y que registraban dicho cumplimiento de la normativa europea podían transmitir datos desde la Unión Europea a Estados Unidos. Pero los Principios internacionales safe harbor fueron anulados el 24 de octubre de 2015 por el Tribunal de Justicia Europeo después de que un consumidor denunció que sus datos de facebook no estaban lo suficientemente protegidos.

5 **Es posible considerar datos personales a casi cualquier cosa:** La gestión de información y documentación no estructurada es clave para el cumplimiento. De acuerdo con la Comisión Europea, "toda información relativa a una persona física identificada o identificable, ya sea relacionada con su vida privada, profesional o pública, se considera datos personales". Según la Comisión, "se pueden consideran datos a un nombre, una dirección postal, una fotografía, una dirección de correo electrónico, detalles de una cuenta bancaria, publicaciones sitios web de redes sociales, información médica o una dirección IP". Las empresas deben tener la capacidad de identificar **cualquier lugar o documento** que contenga información de identificación personal y de proporcionar un índice de esos datos PII al consumidor si este lo solicita: un requisito imposible sin un sistema de gestión de contenidos.

6 **Los documentos impresos también se incluyen:** El reglamento RGPD es aplicable al procesamiento de datos personales en su totalidad o en parte a través de medios automatizados. Incluso más importante: También se aplica al procesamiento de datos personales que no se realizan a través de medios automatizados y que forman parte de un sistema de archivado, o que se pretende que formen parte de un sistema de ficheros. (Artículo 2: Ámbito material)

7 **Cadenas de responsabilidad extendidas:** Si la información personal de identificación se archiva o gestiona a través de proveedores de servicios en la nube o de un proveedor de servicios de procesamiento de documentos externo en su nombre, usted es responsable por las prácticas de gobernanza de los datos de sus proveedores.

Conozca quién es: responsable del tratamiento de datos, encargado del tratamiento o ambos.

Existen cinco términos o roles que debería conocer, junto con el reglamento RGPD: interesado o afectado, responsable del tratamiento, encargado del tratamiento, delegado de protección de datos y agencia de protección de datos.

- Un **interesado o afectado** es una persona física Él o ella pueden ser un cliente o un empleado de una empresa, un usuario de una plataforma de redes sociales u otro. El papel del "interesado" se puede comparar con el concepto legal (o término) del propietario, en este caso de los datos. Esto significa cualquier ciudadano "Los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal deben, cualquiera que sea su nacionalidad o residencia, respetar sus libertades y derechos fundamentales, en particular el derecho a la protección de los datos de carácter personal". El interesado cuenta con varios derechos a la obtención de información sobre la información de identificación personal almacenada y procesada; para corregir o incluso eliminar dichos datos, o transferirlos a otra empresa. El papel del "interesado" se puede comparar con el concepto legal (o término) del propietario, en este caso de los datos.
- Un **responsable del tratamiento** "es la persona física o jurídica, autoridad pública, agencia o cualquier otro organismo que, solo o conjuntamente con otros, determina la finalidad y los medios del tratamiento de datos personales; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros". El papel del "responsable de tratamiento" se puede comparar con el concepto legal (o término) del poseedor.
- Un **encargado del tratamiento** es "la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales en nombre del responsable del tratamiento".

Su empresa puede ser un responsable del tratamiento, un encargado del tratamiento o ambos Sus consumidores, clientes, posibles clientes y proveedores también pueden ser todos responsables y encargados. Y sus consumidores, clientes, posibles clientes, empleados y proveedores externos son todos interesados/afectados, además de los grupos análogos de sus socios.

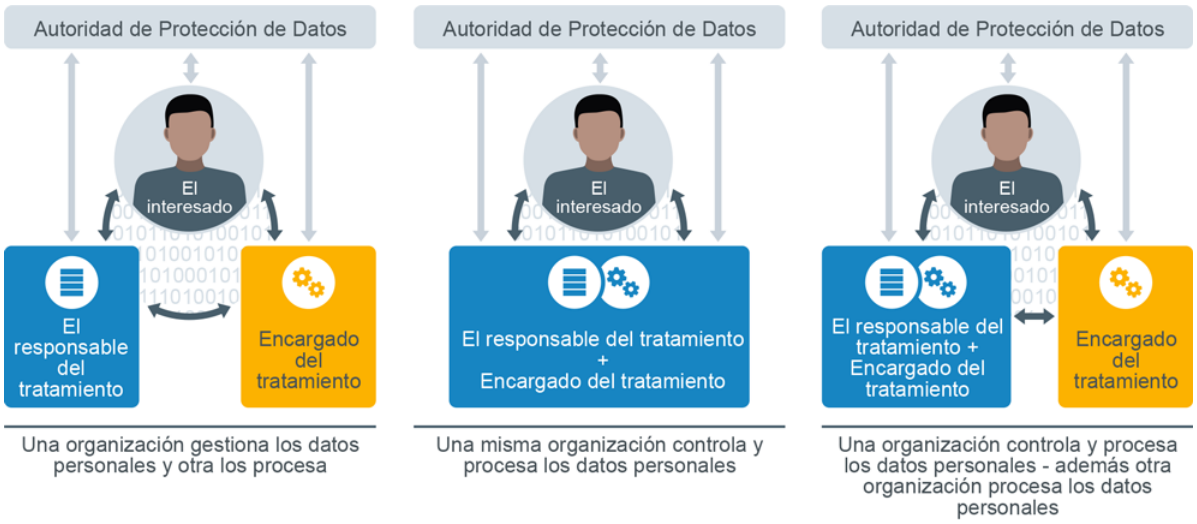
Artículo 4: Definiciones

Ambos encargados y responsables deben generar seguridad en sus productos y procesos desde el primer día. Si aún no se ha hecho, todos los encargados y responsables deben designar un **delegado de protección de datos** (DPO, del inglés data protection officer) que también es responsable si:

- usted procesa PII de más de 5000 interesados por año
- es una organización o agencia estatal
- usted procesa principalmente categorías especiales de datos
- usted realiza observaciones regulares a gran escala

Artículo 37: Designación del delegado de protección de datos

Cada estado miembro de la Unión Europea ha de proporcionar una o más **autoridades de protección de datos** (DPA, del inglés data protection authorities) responsables de la supervisión del sector privado.



¿Quién puede realizar reclamaciones y dónde?

Con el reglamento RGPD, no solo un individuo puede registrar reclamaciones. Él o ella también pueden autorizar a una organización no gubernamental, sin ánimo de lucro, p. ej., una asociación de defensa de los derechos de los consumidores, para que realicen las reclamaciones en su nombre.

Artículo 80: Representación de los interesados/afectados

Una denuncia legal llevada a cabo en las cortes de los estados miembros de la Unión Europea donde el responsable o encargado tiene un establecimiento (principio de ventanilla única, OSS). De forma alternativa, también es posible que sean las cortes del estado miembro donde el solicitante o interesado tiene su residencia habitual.

Artículo 79: Derecho a una solución judicial efectiva contra un responsable o encargado

2 Cómo DocuWare le puede ayudar a cumplir con el reglamento RGPD

Se pueden considerar datos personales un correo electrónico, un archivo, un papel, una nota o un documento que contenga PII. Esto significa que deben archivarse, gestionarse, protegerse y controlarse de acuerdo al reglamento RGPD.

Mientras que el reglamento RGPD es bastante claro en cuento al nivel de protección necesario para los datos personales, este no indica los procesos o las tecnologías que las empresas han de usar para garantizar dicha protección. De hecho, es poco probable que un único sistema pueda cumplir con todas las facetas del reglamento. El cumplimiento requerirá una labor conjunta de tecnologías y políticas.

Una de esas tecnologías importantes es un sistema de gestión documental que no solo digitaliza los registros en papel sino que también aprovecha los metadatos para aplicar la seguridad y la gobernanza necesaria para la protección de los datos de los clientes.

Gracias a su estrategia centrada en el control, DocuWare directamente proporciona soporte a sus proyectos de cumplimiento del reglamento RGPD. Por ejemplo, los archivadores en DocuWare se pueden configurar fácilmente para impedir las descargar, reenvíos o impresión de documentos. Esto no requiere programación, cifrado o una implementación laboriosa dado que es una función básica ya disponible.

2.1 Buscar y acceder a datos personales

Si una persona le pregunta que datos personales suyos se procesan en su empresa, primero debe **localizar los datos personales**. Sin embargo, ya que el reglamento RGPD también se aplica a los registros **impresos** almacenados por una empresa, esto es más fácil decirlo que hacerlo cuando se trata de la gestión de procesos en papel.

Cómo puede DocuWare ayudarle en el cumplimiento normativo

Con DocuWare, todos sus documentos se digitalizan y archivan en un sistema seguro, de forma que pueda **localizar y acceder a todos los datos personales** en sus documentos de forma sencilla. Estos pueden ser correos electrónicos, contratos, facturas, etc. DocuWare puede automatizar el proceso de archivado, búsqueda, localización exportación y eliminación de la información de identificación personal.

Eso hace que este proceso no sea dependiente de individuos. Al contrario, este aplica políticas de gobernanza de datos corporativos. El enfoque automatizado a la protección de PII ofrece orden, coherencia y eficacia a los procesos de su empresa y le ayuda a cumplir con los requisitos del reglamento RGPD con mayor celeridad y de forma más sencilla. El equipo de DocuWare le ofrece apoyo para la configuración de la estrategia de digitalización para sus registros de papel.

Los metadatos juegan un papel clave en el cumplimiento del reglamento RGPD ya que permiten clasificar, categorizar y describir correctamente la información de identificación personal de acuerdo con los requisitos del reglamento. Un ejemplo básico sería una simple búsqueda por tipo de documento (contratos, facturas, correspondencia) que usted sabe que contiene PII.

DocuWare Intelligent Indexing utiliza aprendizaje automático e inteligencia artificial (IA) para automatizar este proceso de clasificación, apoyando el cumplimiento mientras que alivia a su equipo de complicados y tediosos procesos de introducción de datos.

Una vez que un documento se ha indexado, DocuWare puede automáticamente iniciar otras acciones para garantizar la manipulación y el tratamiento adecuado de la información, tales como:

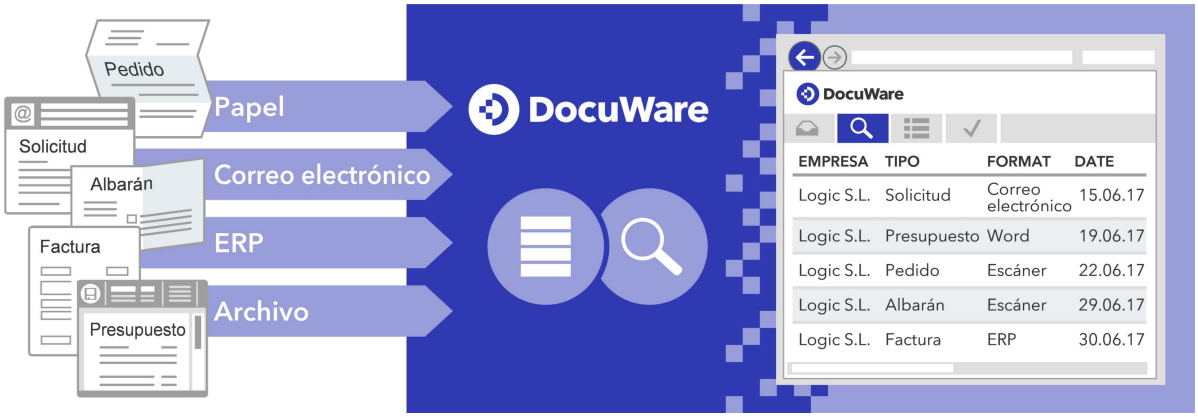
- Cifrado de todos los datos y objetos que contienen PII, tanto durante la transmisión como durante los periodos de inactividad
- Aplicación de controles de acceso y gestión de permisos para garantizar que solo usuarios autorizados puedan acceder a la información de identificación personal. Por ejemplo, los representantes de atención al cliente pueden ver los pedidos de compra de los clientes pero no los miembros de los equipos de marketing
- Aplicación de las reglas relacionadas con la retención y eliminación, para garantizar que los datos no se mantienen más allá de lo necesario.
- La prevención del envío, por correo electrónico o a través de transmisiones, no intencionado o involuntario de información de identificación personal fuera de la organización.
- Seguimiento de cualquier modificación a los documentos de información de identificación personal, para mostrar quién cambió qué y cuándo.
- Provisión de un registro de auditoría para demostrar que solo los empleados autorizados tenían acceso a la información de identificación personal del cliente.

La automatización de este enfoque para la protección de la información de identificación personal trae orden, coherencia y eficacia a la tarea, mientras que aplica políticas de gobernanza de datos de nivel corporativo.

2.2 Obtenga la habilidad para exportar, corregir y eliminar los datos personales

Si se le pregunta acerca de la PII, debe poder **exportar** los datos personales para mostrarlos al solicitante. Esto también puede habilitar a esta persona para transferir sus datos en un "formato comúnmente utilizado y legible por máquina" a otro proveedor o prestatario de servicios.

Debe proporcionar una copia de cualquier dato personal en tratamiento sin coste alguno la primera vez que se le solicite. Además, debe hacerlo dentro de un periodo de 30 días.



Si su empresa está en posesión de información personal incorrecta, debe **corregir** estos datos sin demora una vez solicitada. Si alguien desea que sus datos se **eliminen**, también debe proceder con dicha solicitud: de acuerdo al "derecho al olvido". Solo puede rechazar una solicitud de eliminación a causa del cumplimiento con una obligación legal, interés público o demandas legales.

Cómo puede DocuWare ayudarle en el cumplimiento normativo

Cualquier consulta para exportar, corregir o eliminar los datos personales se puede almacenar en DocuWare y puede activar automáticamente un flujo de trabajo adecuado especialmente diseñado para la exportación, corrección o eliminación de la información de identificación personal. Las tareas de flujo de trabajo se pueden distribuir automáticamente al delegado de protección de datos (DPO) quién tomará las decisiones si dicha solicitud está justificada.

Gracias al módulo de Solicitud, la portabilidad de datos es una función lista para usar de DocuWare. Puede **exportar y transmitir** todas las PII de forma sencilla.

Artículo 20: Derecho a la portabilidad de los datos

El visor de DocuWare garantiza que todas las modificaciones realizadas a los documentos en el visor se archivan como capas en el documento. Así pues, es posible exportar una factura que contenga información de identificación personal de un cliente sin el sello de liberación y PII de un de sus empleados.

Las tareas de flujos de trabajo se pueden distribuir a los delegados de protección de datos (DPO). Ellos actualizarán los contenedores de datos en los diferentes sistemas por su cuenta o distribuyendo las tareas a sus compañeros adecuados. Los delegados de protección de datos pueden **acceder a todos los registros** acerca del interesado fácilmente y marcarlos para su eliminación. O un flujo de trabajo de DocuWare automáticamente inicia dichas acciones una vez que el delegado de protección de datos ha confirmado que la solicitud está justificada.

Para **corregir** todos los datos correspondientes, los metadatos archivados en DocuWare se pueden actualizar automáticamente o de forma semiautomática como parte de estos procesos. Esto garantiza coherencia entre sistemas y fortalece aún más su cumplimiento del reglamento RGPD.

Si es necesario, DocuWare puede **eliminar tanto los documentos como los metadatos**. DocuWare puede incluso abrir aplicaciones de terceros, simplificando dichas tareas. DocuWare puede informar a los interesados automáticamente acerca de las fechas de eliminación de datos y establecer un horario para su disposición.

DocuWare mantiene un **historial** completo de las consultas de rectificación de los datos. Cuando la solicitud de una persona no está justificada, DocuWare puede ayudar al delegado de protección de datos a enviar una respuesta automática al solicitante con una explicación del por qué **no está justificada** y por qué la empresa procesará sus datos durante más tiempo. Los datos solicitados se mantendrán durante el periodo de tiempo requerido y automáticamente se eliminarán al final de dicho periodo de tiempo.

2.3 Asegúrese de que la información personal está protegida y no se continúa procesando

A petición, su empresa debe poder **excluir datos personales de actividades de procesamiento futuras**: de forma permanente o provisional. Las condiciones incluyen precisión de los datos cuestionados, procesamientos no legales y el deseo del interesado de ser excluido de las actividades de procesamiento pero sin que sus datos personales se eliminen por varios motivos legales e históricos.

Artículo 18: Derecho a la limitación del tratamiento

Cómo puede DocuWare ayudarle en el cumplimiento normativo

DocuWare aplica las reglas relacionadas con la retención y eliminación para garantizar que los datos no se mantienen más allá de lo necesario. El establecimiento de programas de retención o mantenimiento le permiten prevenir de forma sencilla el envío por correo electrónico o la transmisión no intencionados o involuntarios de información de identificación personal fuera de la organización. Esto no requiere codificación o programación. Es parte de la configuración básica disponible para los administradores o los DPO.

Además, cualquier modificación a los documentos de información de identificación personal se rastrea para mostrar quién cambió qué y cuándo. Con la gestión de derechos segura y flexible, solo los empleados autorizados pueden acceder a la PII del cliente; para demostrar que no había un acceso no autorizado, el sistema proporciona un registro de auditoría.

Por tanto, DocuWare apenas toma decisiones sobre cómo gestionar la información de identificación personal en manos de empleados individuales y, por lo contrario, aplica políticas de gobernanza de datos de nivel corporativo.

3 Definición de una estrategia de empresa para el cumplimiento de las normativas

El uso de un sistema de gestión documental como DocuWare es un paso importante hacia el cumplimiento del Reglamento General de Protección de Datos (RGPD). Sin embargo, su empresa también utiliza otro software que procesa información personal tales como sistemas de marketing, CRM, ERP y otros.

Para gestionar la información personal en todos los sistemas, defina una estrategia coherente. En su sistema CRM, por ejemplo, también debería poder encontrar, acceder, exportar, proteger y eliminar información personal; además de mantener un registro de estas actividades de procesamiento.

Mantenga sus registros actualizados

Ya sea con su sistema de gestión documental, CRM o ERP, si su papel es de responsable del tratamiento, su DPO es garantizar el cumplimiento normativo y por lo tanto debe mantener un registro de la siguiente información:

- Su nombre y datos de contacto y, si procede, la información de cualquier responsable adjunto, representante y delegados de protección de datos;
- Los objetivos de los procesos;
- una descripción de las categorías de interesados y de las categorías de información personal;
- las categorías de los destinatarios, incluidos destinatarios en terceros países u organizaciones internacionales;
- detalles de las transmisiones de información personal a terceros países (si procede);
- periodos de retención para las diferentes categorías de información personal (cuando sea posible); y
- una descripción general de las medidas de seguridad empleadas (si es posible).

Si hace uso de un procesador de datos, debe asegurarse por contrato que ELLOS mantendrán un registro de todas las categorías de actividades de procesamiento en nombre del responsable

---

Artículo 30: Registros de actividades de procesamiento

Y no olvide: Realice una evaluación del riesgo y una evaluación de impacto relativa a la protección de datos de conformidad con el artículo 35. Una guía de Bitkom le ayudará a empezar.

Información adicional

RGPD con índice y búsqueda

Libro electrónico "Information Privacy and Security" de la asociación industrial AIIM

RGPD: Una lista de tareas pendientes por el abogado Rolf Becker, Colonia,

Alemania Descarga de RGPD en todos los idiomas de la UE