TDL | Trust in Digital Life

RGPD para PYMEs

Guía para pequeñas y medianas empresas sobre cómo abordar el cumplimiento de la protección de datos

Publicación del Grupo de Trabajo TDL
Diciembre 2018
Versión 1.0

Contenido

Introducción	3
Lo que necesitas saber	4
Lo que debes hacer	5
Privacidad desde el diseño.	6
Lista de verificación	7
Conclusión	8
Una instantánea RGPD	9

Introducción

El 25 de mayo de 2018, entró en vigor el Reglamento general de protección de datos (RGPD), que es una revisión importante de la legislación existente sobre protección de datos que se inició en un momento en que muy pocas personas estaban utilizando Internet. El RGPD finalmente consagra en la ley los derechos inalienables de los individuos a tener cualquier información relacionada con ellos para estar adecuadamente protegidos y administrados, con multas y multas severas para las compañías que no cumplan.

Si su compañía se encuentra entre los muchos miles en la UE y más allá que no están al tanto del RGPD o de las consecuencias de no cumplir, debe seguir leyendo. Nuestra intención no es profundizar en los 99 artículos del reglamento, sino proporcionar una idea de los principios rectores que los respaldan y cómo una posible pesadilla de cumplimiento puede convertirse en un beneficio y una ventaja comercial.

Existen nuevas medidas legislativas, como el RGPD, que están a punto de tener un gran impacto en las empresas que poseen datos sobre los ciudadanos de la UE. El masivo las multas por incumplimiento o incumplimiento de hasta 20 millones de euros o el 4% de la facturación global no son, como se pensó en un principio, burocracia para fines de burocracia, ni costes comerciales sin objetivo comercial. Por el contrario, el objetivo de la nueva legislación es aumentar la confianza de los clientes en los servicios digitales y, por lo tanto, acelerar la adopción de tecnología con todos sus ahorros de eficiencia asociados y ventajas económicas. También armoniza las leyes de gestión de datos para empresas en toda Europa, reduciendo simultáneamente los costos legales a medio plazo y facilitando mayores oportunidades de participación de clientes paneuropeos.

Antes de la introducción del RGPD a finales de mayo de 2018, los ciudadanos de toda la Unión Europea fueron atacados con correos electrónicos y otras comunicaciones de minoristas, instituciones financieras, compañías de viajes en línea, proveedores de servicios, agencias gubernamentales locales y muchos, muchos más. Todos buscaban asegurar que los clientes pasados y presentes, consintieran el almacenamiento continuo de su información personal en las bases de datos corporativas y los sistemas CRM y su uso futuro para fines claramente identificados. Detrás de esta actividad se encuentra un enorme volumen de trabajo administrativo para revisar, analizar, validar y limpiar sistemáticamente todos los datos personales acumulados para garantizar que lo que se tenía en el registro estaba allí de manera legal.

Como consecuencia, la mayoría de los ciudadanos se dieron cuenta, al menos, de la existencia de la nueva regulación, incluso si no conocían completamente los detalles. Lo mismo se puede decir de la mayoría de las empresas y organizaciones, grandes y pequeñas, con la diferencia de que si bien las empresas más grandes tienen muchos más sistemas de soporte de datos, generalmente tienen recursos mucho mayores para comprender, interpretar y abordar lo que se debe hacer que los pequeños. a medianas empresas.

A pesar de la aparente fatiga general de RGPD que se ha establecido desde mayo pasado, el reglamento no ha desaparecido y está siendo monitoreado bajo la atenta vigilancia de las autoridades nacionales de protección de datos en cada uno de los Estados miembros de la UE, así como el organismo supervisor general con sede en Bruselas. Si bien puede haber un grado de indulgencia para las PYMEs, en reconocimiento de los desafíos que enfrentan para lograr el cumplimiento, cualquier período de luna de miel inevitablemente tendrá que terminar.

Lo que necesitas saber

Dei 99 articoli e 173 considerando (o definizioni legali) nel RGPD, la maggior parte è aperta a una potenziale interpretazione. A meno che tu non abbia il tempo e sia disposto a studiarli in profondità, è irragionevole aspettarsi che le PYME abbiano le risorse per cogliere tutto ciò che è loro richiesto. Quindi, che cosa arriva al cuore del regolamento, i concetti che sono fondamentali per qualsiasi attività commerciale per conoscere e rispettare?

Notifica di violazione dei dati

Se sei abbastanza sfortunato da aver subito una violazione dei dati, ora sei obbligato a informare le autorità e tutti coloro che ritieni siano stati interessati.

Buone notizie!

Non ci sono molte esenzioni per le PYME, quindi è importante evidenziare una soluzione che riduca gli oneri: le PYME sono esentate dal fare un record di elaborazione (inventario).

Los principios básicos del RGPD son:

- **Capacite a sus clientes** informándoles, con claridad, sobre qué información ha obtenido y para qué fin la va a utilizar;
- **Muestre su compromiso** al proporcionar una forma fácil de usar para que los clientes den su consentimiento y un mecanismo tan sencillo como rechazar el uso de sus datos, a menos que su empresa tenga un claro propósito legítimo.
- **Ofrecer las herramientas** para controlar y administrar esos datos personales a medida que cambie su situación;
- **Haga saber a sus clientes** que pueden desafiar legalmente a su empresa si su empresa cambia su propósito o uso de los datos personales (sin el consentimiento revisado), o los pierde debido a una atención inadecuada.

Los clientes tienen derecho a:

- Objetar que sus datos sean utilizados para cualquier comercialización.
- Revelación completa de cómo se procesarán sus datos
- Objetar que sus datos se procesen automáticamente para fines de creación de perfiles
- Acceso completo a los datos
- Requerir que sus datos sean rectificados si son inexactos
- Exigir que borres sus datos
- Obtenga una copia de sus datos en una forma que puedan llevar a su competidor (conocida como "portabilidad de datos")

Lo que debes hacer

Realizar una auditoría de datos

Identifique todos los datos personales de los que es responsable y averigüe dónde residen. Puede que te sorprenda lo mucho que tienes.

Identificar el procesamiento de datos

Aclare cómo procesa los datos personales y si ese procesamiento está en línea con sus intereses comerciales legítimos.

- ***Obtener consentimiento:** si necesita esos datos para fines comerciales beneficiosos, deberá validar que tiene un consentimiento explícito para el acceso y el procesamiento de esos datos.*
- ***Eliminar y retirar:** si no, considere eliminar los datos y eliminar esos procesos.*

Verificar el cumplimiento del proveedor

Si utiliza a terceros para ayudar a procesar los datos, y es casi seguro que lo hace, audite a esos proveedores y pídales que confirmen el cumplimiento de RGPD. Puede que incluso tenga que revisar sus contratos de servicio con ellos para indemnizarlo adecuadamente. A su vez, indudablemente requerirán la confirmación de su consentimiento auditable para el acceso a los datos y el procesamiento.

En resumen, la solución simple es hacer de la privacidad y la seguridad de los datos personales de sus clientes su negocio. Tome la mentalidad de "el cliente es el rey" en su procesamiento digital y en línea y no se equivocará. Muchas personas se están volviendo cada vez más cautelosas de cometer información personal a Internet. Las empresas pueden tomar algunos pasos simples para minimizar esos riesgos al adaptar sus prácticas de trabajo para presentar una ventaja de privacidad a los clientes.

Mantenlo simple, delgado y mezquino

Un principio clave dentro de RGPD es la minimización de datos, lo que significa que no solo garantiza que no posee datos personales que no necesita estrictamente, sino que también no los retiene durante más tiempo del necesario. Una infracción tiene consecuencias para su cliente y, si no tuvo que conservar los datos que fueron violados, espere que las multas aumenten. Las empresas innovadoras encontrarán formas de prestar servicio con menos datos y, potencialmente, diferenciarán su oferta a prospectos sobre esta base, especialmente para los datos legalmente sensibles o los datos considerados sensibles por los prospectos en su industria.

No almuerzos gratis

Es sorprendente la cantidad de empresas que descuidan el software de terceros (especialmente gratuito) que utilizan para crear sitios web y generalmente buscan los proveedores de servicios de Internet más baratos o los sistemas de gestión de relaciones con los clientes (CRM). Aunque los sistemas de administración de contenido (CMS) más populares son confiables, muchos de los complementos asociados pueden no serlo. El software "gratuito" rara vez llega sin un problema: puede estar bastante seguro de que el precio se extrae en los datos de sus clientes, así que verifique, ¡porque ahora es responsable! Los servicios baratos también pueden usar las mismas técnicas, precios de negociación para su negocio o los datos de sus clientes.

Procesos de negocios

La mayoría de los anteriores son realmente procesos de negocios, no, como la mayoría de las empresas piensa, una responsabilidad de TI que tiene un papel que desempeñar en la validación de proveedores, sino que, en el contexto de RGPD, su función principal es evitar las violaciones. El equipo de TI también será responsable de detectar e informar de las infracciones (¿Tiene herramientas para eso? Muchos no lo hacen). Dichos informes se envían al controlador de datos designado por la empresa, que luego tiene que decidir si se debe informar a la autoridad nacional de supervisión para la protección de datos. Una recopilación de infracciones menores a lo largo del tiempo puede indicar una falla sistémica que debe abordarse. La autoridad de supervisión espera un registro de todas las infracciones internas menores y, si indican un problema sistémico, esperarán que se solucione, especialmente si conduce a una infracción más grave más adelante.

Privacidad desde el diseño.

Sitios web orientados al público

Muchos sitios web tienen instalado Google Analytics sin pensar mucho en los datos que se recopilan sobre los visitantes. Si nunca ha tomado una sola decisión basada en análisis web, debería considerar eliminarlo. Y mientras lo hace, revise las políticas de privacidad y cookies de su sitio web; considerar si el software de análisis y seguimiento (incluyendo los botones de redes sociales) que empleas valen El problema de hacerlos compatibles con RGPD.

Con respecto a la privacidad del usuario, el RGPD ha intentado poner en práctica los siete principios de privacidad por diseño que no solo se aplican al desarrollo de software, sino también a los procesos y procedimientos de la empresa. En otras palabras, cada PYME debe tener un proceso para tratar los datos personales.

La revisión de los procesos de su empresa en relación con estos principios puede ayudar a comprender qué tan cerca o lejos está de tener la cultura de liderazgo adecuada para mitigar el riesgo y maximizar las oportunidades de negocios. Si cumple con estos principios según la carta, puede encontrar poca necesidad de consentimiento y sus servicios tendrán pocas o ninguna configuración de privacidad. Toda la privacidad es contextual: usted entiende qué datos necesita procesar, pero ¿su cliente? Al encontrar formas de dejar en claro a sus clientes qué datos recopila y qué hace con ellos, mitigará sus desafíos de administración de la privacidad.

Los siete principios de privacidad desde el diseño son:

- Proactivo no reactivo: preventivo no reparador
  Adopte un enfoque proactivo de la protección de datos y anticipe los problemas y riesgos de privacidad antes de que ocurran, en lugar de esperar hasta que sea demasiado tarde.

- La privacidad como la configuración por defecto
  Diseñar sistemas, servicios y procesos para proteger automáticamente los datos personales. Incorpore la privacidad en todas las prácticas comerciales de su empresa y los clientes aprenderán a confiar en que sus datos están protegidos adecuadamente.

- Privacidad incrustada en el diseño
  Incorpore la protección de datos en el diseño de sus sistemas, servicios y procesos, haciendo que la privacidad sea parte de la funcionalidad principal.

- Funcionalidad completa - suma positiva, no suma cero
  Asegure un ganar-ganar asegurando que cada sistema respalde la privacidad y la seguridad y que no haya concesiones innecesarias.

- Seguridad de extremo a extremo: protección completa del ciclo de vida
  Instale medidas de seguridad sólidas que garanticen la gestión segura del ciclo de vida de los datos desde su recopilación inicial hasta su eliminación segura.

- Visibilidad y transparencia - mantenerlo abierto
  Cualquiera que sea la práctica comercial o la tecnología que utilice, debe funcionar de acuerdo con las premisas y los objetivos verificables de forma independiente.

- Respeto por la privacidad del usuario: manténgalo centrado en el usuario
  Mantenga el interés de los individuos en los diseños de sistemas ofreciendo fuertes valores predeterminados de privacidad, controles fáciles de usar y avisos apropiados.

Lista de verificación

La razón empresarial se reduce a tratar los datos como un activo empresarial cuantificable. La inversión requerida para proteger estos activos puede compararse con el enfoque de una compañía de seguros para proporcionar una indemnización para cubrir el hogar y los contenidos.

Las PYMEs se pueden adaptar de manera ágil al nuevo RGPD en formas que las corporaciones van a encontrar desafiantes.

Esta breve lista de verificación le ayudará a cumplir con el GDPR. Ser capaz de responder "sí" a todas las preguntas no garantiza el cumplimiento, pero debería significar que va en la dirección correcta.

Información de los clientes

- ✓ ¿Realmente necesita esta información sobre un individuo? ¿Sabes para qué lo vas a usar?
- ✓ ¿Las personas cuya información usted posee saben que la tienen, y es probable que comprendan para qué se utilizará?
- ✓ ¿Está satisfecho de que la información se mantiene de forma segura, ya sea en papel o en una computadora? ¿Y qué hay de tu sitio web? ¿Es seguro?
- ✓ ¿Está seguro de que la información personal que posee es precisa y está actualizada?
- ✓ ¿Borra o destruye información personal tan pronto como ya no la necesite?
- ✓ ¿El acceso a la información personal se limita solo a aquellos con una necesidad estricta de saber?

Datos del personal

- ✓ Si desea poner detalles del personal en su sitio web, ¿ha consultado con ellos sobre esto?
- ✓ Si desea monitorear al personal, por ejemplo, verificando su uso del correo electrónico, ¿les ha contado esto y ha explicado por qué?
- ✓ ¿Ha capacitado a mi personal en sus deberes y responsabilidades bajo el RGPD, y se asegura regularmente de que los estén poniendo en práctica?
- ✓ Si se le solicita que transmita información personal, ¿está usted y su personal en claro cuando el RGPD le permite hacerlo?

Asuntos de política

- ✓ Si usa CCTV, ¿está cubierto por el GDPR? Si es así, ¿está mostrando avisos que le dicen a la gente por qué tiene CCTV? ¿Están las cámaras en el lugar correcto o se entrometen en la privacidad de alguien?
- ✓ ¿Sabría qué hacer si uno de sus empleados o clientes individuales solicita una copia de la información que tiene sobre ellos?
- ✓ ¿Tiene una política para lidiar con problemas de protección de datos?
- ✓ ¿Necesita notificar a la oficina del comisionado de información nacional? Si ya lo ha hecho, ¿su notificación está actualizada o necesita ser eliminada o modificada?

Conclusión

Muchas personas se están volviendo cada vez más cautelosas de cometer cualquier información personal a Internet, aunque demasiados están ajenos a los riesgos. Algunos pasos simples que pueden tomar las empresas para minimizar esos riesgos; Edúquese rápido y adapte sus prácticas de trabajo para presentar una ventaja de privacidad a los clientes.

¡Saber más!

Para obtener más orientación práctica para las empresas sobre cómo implementar los requisitos de RGPD:

- *El Supervisor Europeo de Protección de Datos (SEPD) de la autoridad de protección de datos independiente de la UE: https://edps.europa.eu/data-protection/data-protection/reference-library_en*
- *El Consejo Europeo de Protección de Datos (CEPD): https://edpb.europa.eu/our-work-tools/our-documents_en*
- *La Oficina del Comisionado de Información del Reino Unido: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/*

El RGPD ya está teniendo un gran impacto en las empresas, grandes y pequeñas, que tienen datos sobre los ciudadanos de la UE. Las multas masivas por incumplimiento o incumplimiento de hasta 20 MEUR o el 4% de la facturación global no son, como se pensó en un principio, burocracia para fines de burocracia, ni costos de negocios sin objetivo comercial.

Tomando responsabilidad

No se puede esperar que las pequeñas empresas sigan el ritmo del volumen de las regulaciones emergentes, pero deben hacerlo o arriesgar su medio de vida. Cada empresario puede comprender la importancia de tener un conjunto de principios rectores y esto es solo un nuevo conjunto para comprender e inculcar en la cultura de la empresa. Entonces, para que quede claro: la gestión del nuevo desafío es un tema de liderazgo ejecutivo, no uno que debe entregarse a marketing, ventas o TI.

The privacy paradox

A medida que los clientes se dan cuenta de sus nuevos derechos, incluso si es solo un pequeño número que comienza a consultar sus sistemas y procesos, y genera inquietudes con las autoridades de supervisión, el costo para su empresa podría aumentar rápidamente. Adoptar las nuevas leyes y buscar formas de facilitar a los clientes demuestra que desea que tengan estos nuevos derechos, que sean de fácil acceso y que se entiendan fácilmente. Si los habilita con el control y la transparencia sobre los datos personales que posee y lo que hace con ellos, las recompensas se obtienen en términos de lealtad y confianza del cliente, por lo que ofrecen más datos para más servicios.

A business opportunity

Para las empresas dinámicas con visión de futuro, adoptar la nueva legislación es una oportunidad de negocio. Si esto no es lo suficientemente atractivo, también vale la pena señalar que las personas tendrán un poder mucho mayor por parte del GDPR con derechos sobre "sus" datos personales. Si su empresa abusa o hace un mal uso de su confianza en la forma en que procesa sus datos, entonces ellos tienen nuevos derechos para demandar o incluso buscar demandas colectivas.

En resumen, la nueva legislación es un reequilibrio de los derechos y poderes entre el individuo y el proveedor en la era digital. Las compañías que no responden rápidamente se verán dejadas atrás por competidores que logran multas o juicios lo suficientemente grandes como para destruir negocios.

Una instantánea RGPD

Conciencia
Asegúrese de que su personal esté al tanto de los cambios en el manejo de datos afectados por el GDPR

Información que usted tiene
Documente qué datos personales tiene de dónde provino y con quién los comparte: una auditoría de datos.

Comunicado
Revise sus avisos de privacidad actuales y realice los cambios necesarios para alinearse con el RGPD

Derechos del cliente
Verifique sus procesos y procedimientos para asegurarse de que cubran todos los derechos que tienen los clientes, incluida la forma en que eliminaría los datos personales o los proporcionaría en un formato de uso común.

Consentimiento
Revise su solicitud, registre y administre el consentimiento para cumplir con los estándares RGPD

Solicitudes de acceso de clientes
Actualice sus procedimientos para manejar las solicitudes dentro de los plazos de GDPR.

Leyes nacionales de aplicación.
Más de la mitad de los Estados miembros de la UE han promulgado leyes que implementan GDPR y, a veces, estas leyes contienen requisitos adicionales.

Base legal para su tramitación. información personal
Identifique y documente la base legal para el procesamiento de su información personal y actualice su aviso de privacidad en consecuencia

Niños
Considere si necesita implementar sistemas para verificar las edades de los individuos y obtener el consentimiento de los padres o tutores para el procesamiento de datos.

Violaciones de datos
Asegúrese de contar con los procedimientos correctos para detectar, informar e investigar una violación de datos personales.

Protección de datos por diseño.
Verifique sus procesos y procedimientos para asegurarse de que cubran los derechos de sus clientes, incluida la forma en que eliminaría los datos personales o los proporcionaría en un formato de uso común.

Oficial de protección de datos
Designe a alguien para que asuma la responsabilidad del cumplimiento de la protección de datos y su papel en la estructura de gobierno de su empresa.

Internacional
Si opera en más de un Estado miembro de la UE, determine su autoridad de supervisión principal de protección de datos. Si su negocio en línea utiliza proveedores de servicios no basados en la UE, debe asegurarse de que también cumplen con RGPD

trustindigitallife.eu

Trust In Digital Life Association
avenue Maurice Dekeyser 11 1090 Jette, Bruselas

office@trustindigitallife.eu
+44 141 588 0892

TDL | Trust in Digital Life

La visión de TDL es que la confianza debe convertirse en una propiedad intrínseca de cualquier transacción en línea que involucre información personal, incorpore avances legales, comerciales y técnicos, respalde políticas de seguridad cibernética e integre consideraciones sociales para que los ciudadanos y usuarios finales reconozcan servicios, transacciones y datos confiables y prepárate para pagar por ellos. Las TIC confiables aumentarán la confianza en la sociedad moderna, traerán nuevas y atractivas formas de vivir y trabajar, y fortalecerán aún más los valores democráticos y sociales de Europa.

La misión de la asociación es proporcionar a sus miembros una plataforma de desarrollo empresarial europea para estimular el desarrollo y la aceptación por parte de los usuarios de TIC innovadoras pero prácticas y confiables. Guiado por su agenda de investigación estratégica, TDL actúa como una incubadora para una cartera de proyectos de sprint destinados a validar conceptos tecnológicos nuevos e innovadores, promueve la colaboración entre sectores y agrega los resultados en las recomendaciones de la industria para los responsables políticos y la Comisión Europea.

trustindigitallife.eu

Trust In Digital Life Association
avenue Maurice Dekeyser 11, 1090 Jette, Bruselas

office@trustindigitallife.eu
T +44 141 588 0892

TDL | Trust in Digital Life