GUÍA

DE LA **LOPD** AL **RGPD** EN 6 PASOS

¿SABES QUÉ PASOS TIENES QUE DAR?

TE DESVELAMOS LAS CLAVES.

MILENIUM
THE SOLUTIONS FACTORY

DE LA **LOPD** AL **RGPD** EN 6 PASOS

Uno de los grandes retos que tendrán que afrontar las empresas en 2018 es la adaptación al Reglamento General de Protección de Datos o RGPD (también conocido como GDPR por sus siglas en inglés).

Seguramente ya hayas oído hablar de las principales novedades y de los cambios más significativos que trae esta nueva normativa. Incluso es posible que te hayan encomendado la tarea de llevar a cabo esta adaptación dentro de tu organización. Pero… ¿sabes qué pasos tienes que dar?

Si quieres saber cómo afrontar un proyecto de adaptación al RGPD sigue leyendo…
Aquí te desvelamos las claves.

PASO 1

CONOCE LAS NUEVAS OBLIGACIONES

El primer paso a la hora de comenzar el proceso de adaptación debes conocer muy bien cuáles son las nuevas obligaciones a las que se enfrenta tu empresa. Para ayudarte, aquí te resumimos las novedades principales:

NUEVO RÉGIMEN SANCIONADOR

Las sanciones por infracciones de las obligaciones del RGPD pueden ascender hasta 10 millones de euros o el 2% de la facturación mundial anual (el que sea mayor) o hasta 20 millones de euros o el 4% de la facturación mundial anual (el que sea mayor). Como puedes ver, el Reglamento europeo sólo define los límites máximos de la sanción. El importe de la multa en cada caso será la que resulte de aplicar los criterios de ponderación previstos en la nueva LOPD.

DELEGADO DE PROTECCIÓN DE DATOS

(En inglés, Data Protection Officer – DPO). Es una figura novedosa que será obligatoria para determinadas empresas (en la nueva LOPD puedes encontrar un listado indicativo). Sus funciones son, entre otras, las de informar y asesorar a la empresa en el cumplimiento de sus obligaciones de protección de datos, supervisar el cumplimiento de lo dispuesto en la normativa y en los protocolos internos, concienciar y formar a los empleados, realizar las auditorías y ser el enlace con la Agencia Española de Protección de Datos (AEPD). Puede ser alguien interno de la organización o un experto externo, pero es imprescindible que cuente con formación y experiencia en el asesoramiento en protección de datos.

REFORZAMIENTO DEL DEBER DE INFORMACIÓN

Con el nuevo Reglamento se amplían las cuestiones de las que la empresa debe informar a los interesados antes de llevar a cabo un tratamiento de sus datos como, por ejemplo, la identidad y datos de contacto del DPO, el plazo de conservación de los datos, si se van a hacer transferencias internacionales, los nuevos derechos de los afectados…

CAMBIOS EN LA FORMA DE OBTENCIÓN DEL CONSENTIMIENTO

El RGPD establece que, cuando el tratamiento de datos personales se base en el consentimiento del interesado, éste deberá ser claro, informado e inequívoco. Esto implica que la autorización de la persona debe provenir de una manifestación o clara acción afirmativa, quedando excluida -en consecuencia- la posibilidad de obtener consentimientos de manera tácita (lo que sí estaba permitido, en determinados casos, por la anterior LOPD).

PASO 1

EVALUACIÓN DE IMPACTO EN LA PRIVACIDAD DE LOS DATOS

(En inglés, Privacy Impact Assesment – PIA). En aquellos casos en los que, tras la evaluación de riesgos, se detecte que un determinado producto, servicio o proyecto conlleva un riesgo alto para la privacidad, debe realizarse una Evaluación de Impacto con carácter previo a realizar cualquier tratamiento. Lo anterior, que no es más que una determinada metodología para evaluar los riesgos asociados a un tratamiento (de todo tipo, no sólo los de cumplimiento normativo) es además obligatoria para determinados tratamientos listados en el RGPD.

OBLIGACIÓN DE NOTIFICACIÓN DE VIOLACIONES DE LA SEGURIDAD DE LOS DATOS PERSONALES.

Por último, en el supuesto de que se produzca una violación en la seguridad de los datos tratados por la organización, ésta deberá notificarlo en el plazo máximo de 72 horas a la AEPD y también a los afectados, cuando dicha violación suponga un riesgo alto para su privacidad.

Ahora ya conoces cuáles son las nuevas obligaciones que tu empresa tiene que cumplir, pero ¿y ahora qué? El proceso de adaptación a la nueva normativa europea puede ser una tarea ardua pero las buenas noticias son que, si tu empresa parte de un buen nivel de cumplimiento con la actual LOPD, el proceso será relativamente sencillo con un poco de orientación sobre qué pasos tienes que dar.

PASO 2

CREA UN **CRONOGRAMA** Y ORGANIZA EL EQUIPO

Como en cualquier proyecto, la etapa de planificación es una de las más importantes, pues de ella puede depender el éxito o el fracaso de nuestro objetivo. Por tanto, antes de empezar te aconsejamos que planifiques con detenimiento los principales recursos que necesitas para adaptar tu organización al RGPD.

CRONOGRAMA

No debemos olvidar que este proyecto de adaptación tiene una fecha límite: el 25 de mayo de 2018. Como ya sabes, el Reglamento europeo se aprobó en mayo de 2016 pero se concedió un plazo de gracia de dos años para que las empresas pudiéramos ir realizando las modificaciones necesarias. Sin embargo, si eres de los que aún no ha empezado, tranquilo, no eres el único.

Según un estudio publicado por NetApp, se calcula que el 70% de las organizaciones europeas no llegarán a tiempo de adaptarse al nuevo Reglamento. Es un porcentaje demasiado alto, especialmente teniendo en cuenta el importe de las nuevas sanciones que podrán aplicarse a todas aquellas empresas que no hayan hecho los deberes antes del 25 de mayo de 2018.

Ten en cuenta que un proyecto de estas características no se realiza en un día ni en una semana. Evidentemente el tiempo que pueda suponer dependerá del tamaño que tenga tu organización, pero para una empresa de tamaño medio la duración aproximada es de dos o tres meses. Por tanto, si tu empresa aún no ha empezado el proceso de adaptación, ha llegado el momento de comenzar.

PASO 2

EQUIPO

Otro de los recursos que tienes que planificar, además del temporal, es el humano, el equipo de profesionales que te van a ayudar en esta tarea.

Y es que el proceso de adaptación no es un proyecto que, con carácter general, pueda llevar a cabo una única persona. Para realizar el proyecto es necesario, al menos, una persona que tenga un conocimiento legal especializado de esta normativa y una persona con un perfil técnico que pueda ocuparse de la parte de las medidas de seguridad. Por consiguiente, tanto el departamento de Informática como el de Asesoría Jurídica van a ser claves en este proyecto.

En el supuesto de que, por las características de la organización, debas contar con un Delegado de Protección de Datos será éste quien lidere el proyecto. Recuerda que esta figura puede ser alguien interno de la organización, pero también externo que aúne los dos perfiles indicados (legal y técnico).

Pero de igual modo, como veremos a continuación, vas a necesitar la participación e involucración de otros departamentos de la empresa que traten datos de carácter personal, como recursos humanos, administración, atención al cliente, etc.

Ahora que ya has planificado el tiempo que tendrás que dedicarle a este proyecto y el equipo que te va a acompañar, es hora de dar el siguiente paso.

PASO 3

ELABORA TU **ANÁLISIS DE RIESGOS**

El segundo aspecto clave a la hora de adaptarse al nuevo Reglamento es el análisis minucioso de las particularidades de tu organización, pues no todas las obligaciones del RGPD se aplican a todas las empresas, ni en la misma medida.

En este sentido, los dos pilares fundamentales sobre los que se basa el Reglamento europeo son: **el principio de responsabilidad activa y el enfoque basado en el riesgo. ¿Qué significa esto?**

Como sabes, hasta ahora las empresas tenían que tener implantadas una serie de medidas de seguridad legales, técnicas y organizativas (descritas en el reglamento de desarrollo de la LOPD) en función del tipo de datos que trataran -de nivel básico, medio o alto– procediendo a la imposición de sanciones en caso de incumplimiento.

Con el nuevo Reglamento ya no existe un catálogo cerrado de medidas de seguridad que las empresas tengan que implantar, sino que las empresas deben:

- Analizar detenidamente qué tipo de datos tratan (categorías, origen, naturaleza…) y de qué modo (finalidades, cesiones, transferencias internacionales…) y, en función de lo anterior
- Evaluar los riesgos que se desprenden de cada tratamiento
- Aplicar las medidas que la empresa considere adecuadas e idóneas para garantizar la seguridad de esos datos.

Por tanto, como puedes ver el nuevo Reglamento da a un giro de 180º, pasando de un enfoque represivo a un enfoque proactivo (accountability, privacy by design, privacy by default). Por ello, a la hora de hacer la adaptación, es esencial que conozcas en detalle el tratamiento que se hace de los distintos flujos de datos personales en tu organización. ¿Cómo? Mediante un análisis de riesgos.

El análisis de riesgos será la principal herramienta para adaptar tu organización y de sus resultados dependerán el resto de medidas a implementar. Por ello es muy importante que dediques todo el tiempo que sea necesario a este análisis y que en él impliques a todas las áreas y departamentos de la organización con responsabilidades en el tratamiento de datos.

Igualmente, al realizar este análisis detectarás si además tienes que llevar a cabo o no una Evaluación de Impacto en la Protección de Datos para determinados tratamientos que impliquen un riesgo alto para la privacidad de las personas.

PASO 4

REDACTA EL **REGISTRO DE ACTIVIDADES** DE TRATAMIENTO

Con el RGPD la declaración de ficheros ante la Agencia Española de Protección de Datos pasa a ser sustituida por un registro obligatorio de todas las actividades del tratamiento efectuadas por la organización.

Dicho registro debe contener, a grandes rasgos, la siguiente información:

- Nombre y datos de contacto del responsable del tratamiento.
- Datos de contacto del Delegado de Protección de Datos, en su caso.
- Finalidades del tratamiento.
- Categorías de interesados.
- Categorías de datos personales.
- Categorías de destinatarios a quienes se comunican los datos.
- Transferencias internacionales, en su caso.
- Plazos previstos de supresión, cuando sea posible.
- Descripción general de medidas técnicas y organizativas de seguridad, cuando sea posible.

Sin embargo, la obligación de llevar este registro de actividades del tratamiento no resulta aplicable a las empresas con menos de 250 empleados, salvo que el tratamiento pueda conllevar un riesgo para los derechos de los interesados, no sea ocasional o incluya categorías especiales de datos o datos relativos a condenas e infracciones penales.

PASO 5

REVISA LAS CLÁUSULAS DE FORMULARIOS Y CONTRATOS

Como hemos visto, una de las novedades es el reforzamiento del deber de información a los afectados. Por ello, es necesario que revises todas las cláusulas informativas de protección de datos que aparezcan en contratos, impresos, formularios, páginas web, etc. e introduzcas en ellas la información adicional ahora requerida.

- Identidad y datos de contacto del responsable del tratamiento.
- Datos de contacto del Delegado de Protección de Datos, en su caso.
- Finalidades y base jurídica del tratamiento.
- Los destinatarios de los datos y transferencias internacionales, en su caso.
- El plazo de conservación.
- Los derechos del interesado de acceso, rectificación, supresión y portabilidad de los datos, así como a la limitación u oposición al tratamiento.
- El derecho a presentar una reclamación ante la autoridad de control.
- Si la comunicación de datos es un requisitos legal o contractual, o necesario para suscribir un contrato y si existe obligación de facilitar los datos y las consecuencias de no hacerlo.
- La existencia de decisiones automatizadas

Recuerda que, para ello, puedes utilizar el sistema de información por capas, igual que en el caso de las cookies.

Asimismo, ten en cuenta que todo tratamiento de datos de carácter personal debe estar basado, con carácter general, en (i) el consentimiento del afectado, (ii) la ejecución de un contrato, (iii) el cumplimiento de una obligación legal o (iv) un interés legítimo. Por tanto, revisa que los tratamientos efectuados por tu empresa se amparan en alguno de estos supuestos.

Además, recuerda que ya no se permiten los tratamientos basados en el consentimiento tácito. Por ello, todos aquellos datos que la organización haya obtenido por esta vía deben eliminarse, o bien, volver a recabar la autorización del interesado, pero esta vez de forma inequívoca.

Finalmente, deberás también analizar los contratos suscritos con aquellos proveedores que tengan acceso a datos de carácter personal responsabilidad de la empresa (también conocidos como encargados del tratamiento) para garantizar su adecuación a la nueva regulación.

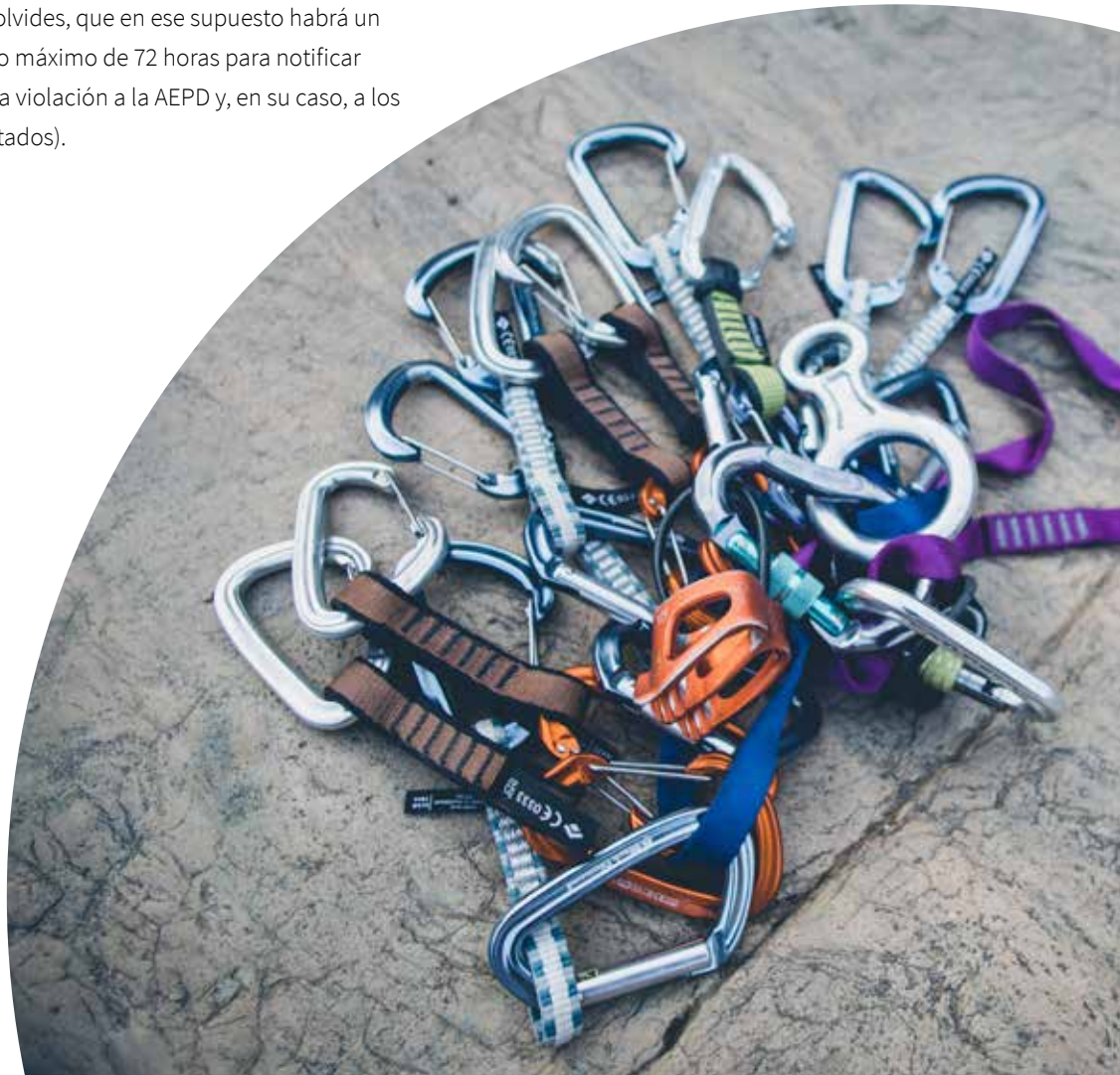
PASO 6

REDACTA PROCEDIMIENTOS PARA GARANTIZAR LA SEGURIDAD

Si tras el análisis de riesgos o la Evaluación de Impacto has detectado que existen determinados riesgos para la privacidad que no están suficientemente cubiertos, implanta las medidas de seguridad técnicas y organizativas que sean suficientes y efectivas para cubrir esos gaps.

Del mismo modo, elabora un procedimiento de reacción en caso de que se produzca una violación de la seguridad de los datos (no olvides, que en ese supuesto habrá un plazo máximo de 72 horas para notificar dicha violación a la AEPD y, en su caso, a los afectados).

Finalmente, recuerda que tu empresa debe contar con mecanismos para dar cumplimiento a los derechos de acceso, rectificación, supresión (derecho al olvido), limitación y portabilidad de los afectados. Por ello, redacta protocolos de actuación que se ajusten a las nuevos plazos y derechos previstos en el RGPD.



UNOS **CONSEJOS** FINALES

Esperamos que esta pequeña guía te haya servido de utilidad para abordar el proyecto de adaptación al Reglamento General de Protección de Datos. Sabemos que es mucho trabajo, pero con una adecuada planificación y un buen asesoramiento tu empresa llegará al 25 de mayo de 2018 con los deberes hechos.

No obstante, permítenos unas recomendaciones finales:

CUENTA CON UN BUEN DELEGADO DE PROTECCIÓN DE DATOS

Aunque por las circunstancias de tu organización no tengas la obligación legal de contar con esta figura, el contratar de manera voluntaria a un DPO (ya sea interno o externo) te permitirá tener la tranquilidad de cumplir en todo momento con la normativa, evitando las elevadas sanciones y, además, será visto por las autoridades sancionadoras como una muestra de esa responsabilidad proactiva de la que hemos hablado.

INFÓRMATE Y FÓRMATE

Actualmente tienes a tu disposición un montón de información sobre el nuevo Reglamento europeo, en forma de ponencias, cursos, charlas, noticias y documentos. Te recomendamos que consultes la página web de la Agencia Española de Protección de Datos, en la que encontrarás multitud de guías y recursos para ayudarte durante el proceso de adaptación.

PIDE AYUDA

Si a pesar de lo anterior, todavía tienes dudas sobre algunos puntos habla con otras empresas de tu sector para ver cómo están realizando la adaptación y, si es necesario, pide ayuda a un experto en protección de datos. En ese caso, asegúrate de que efectivamente tiene conocimientos especializados y puede acreditar experiencia en otros trabajos similares.

GUÍA

DE LA **LOPD** AL **RGPD** EN 6 PASOS

MILENIUM
THE SOLUTIONS FACTORY