A pyme comercio

La protección de datos para tu pyme explicada de un vistazo

Fondo Europeo de Desarrollo Regional

"Una manera de hacer Europa"

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

red.es

UNIÓN EUROPEA

A pyme comercio

Contenidos

Fondo Europeo de Desarrollo Regional
"Una manera de hacer Europa"
GOBIERNO DE ESPAÑA · VICEPRESIDENCIA PRIMERA DEL GOBIERNO · MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL · red.es · UNIÓN EUROPEA

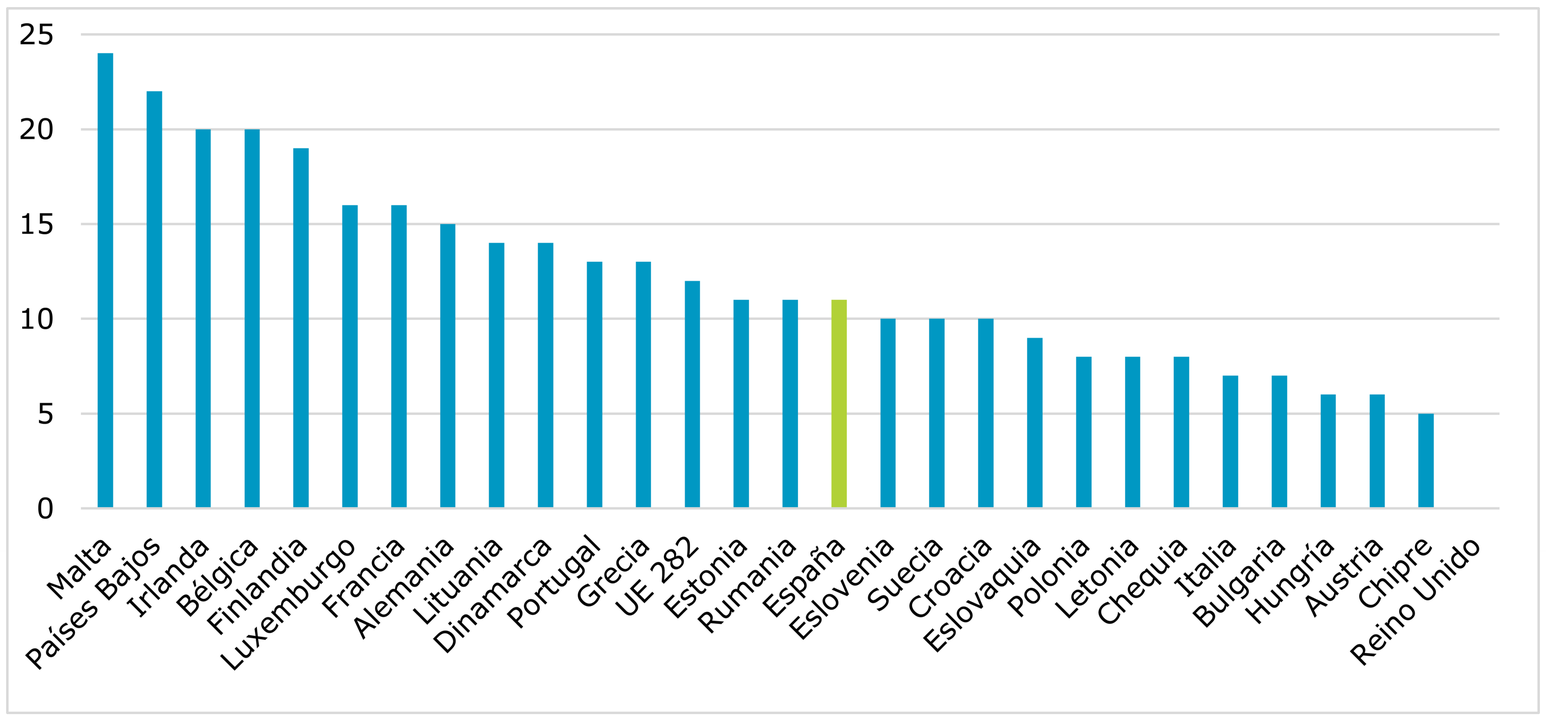
Introducción

Disponer de información es tener poder, ya que en la mayor parte de los casos, las empresas necesitan estos datos para un funcionamiento normal de sus negocios. Actualmente el uso de las nuevas tecnologías, nutridas de datos es tan común, que la práctica totalidad de las empresas se ha hecho a su uso diario y se ve como algo normal. En este escenario la protección de la privacidad se presenta como un reto clave en el día a día de las empresas.

No queremos imaginar el supuesto de la pérdida o filtración de la información o los datos de nuestro negocio o que esta información sea extraída de manera ilícita de nuestros servidores, pero son riesgos que las empresas pueden correr y supondrían grandes pérdidas y, en caso de resultar datos personales, supondría una infracción de la regulación. Adicionalmente, considerando la conciencia adquirida sobre la importancia de los datos, para la empresa también daría lugar a una gran pérdida de reputación. Por esto es tan importante la protección de los mismos.

Esto pone de manifiesto la gran importancia que tienen los datos a día de hoy en las empresas. En este sentido, el volumen de datos que gestionaron las empresas ha aumentado en los últimos años más de un 500%, [REF-1] por lo que nos podemos hacer a la idea de la creciente importancia que tienen.

Por otro lado, aunque este volumen de datos resulte abrumador, según datos del Dossier de indicadores sobre el uso de Big Data por empresas en España y Europa, desarrollado por ONTSI, éste es todavía muy incipiente. En este sentido, únicamente el 11% de las empresas españolas utilizaron el Big Data, sin embargo la tendencia es creciente en los últimos años, aumentando en 2 puntos porcentuales de 2016 a 2018. [REF-2].



Adicionalmente, según el Estudio de madurez data driven de las empresas, elaborado por INCIPY, únicamente el 36,1% de las empresas españolas señalan que tienen una cultura del dato desplegada en su empresa. Sin embargo, el 78% de las empresas aseguran haber acelerado el uso de los datos por el impacto de la pandemia de COVID-19 [REF-3].

Otro aspecto destacable sobre el uso de los datos en las empresas españolas es la fuente de obtención de los mismos, según el dossier elaborado por el ONTSI, el 5% de las empresas utilizan, como fuente de información, la geolocalización de los dispositivos móviles y, en el mismo porcentaje, obtienen los datos provenientes de las redes sociales. Adicionalmente, un 4% de las empresas recogen y analizan los datos obtenidos en dispositivos o sensores inteligentes propios de la empresa [REF-2].

Considerando el gran volumen de datos que gestionan las empresas, otro aspecto importante sería destacar el valor de dichos datos. En este sentido, según el informe del sector infomediario para el año 2021, elaborado por ASEDIE (Asociación Multisectorial de la Información), el mercado de datos en España, en el año 2019, tiene un valor de más de 2.500 millones de € [REF-4]. Sin embargo, el valor de los datos va mucho más allá, considerando su relevancia a la hora de conocer a los clientes, mejorar la publicidad, establecer canales de comunicación con ellos, fidelizarlos, etc.

Puede parecer complicado recopilar y manejar datos personales, sin embargo estos se encuentran y se generan en muchas de las actividades cotidianas que realizan las pymes: actividad de la página web (qué usuarios entran o se registran), redes sociales (interacciones con clientes o potenciales clientes), feedback de los productos o servicios que comercializa la pyme (quién deja comentarios o reseñas) o quién adquiere estos productos o servicios, entre otras muchas formas.

En definitiva, los datos son fundamentales a la hora de mejorar la competitividad de las pymes, ya que, con su correcto análisis y explotación generan oportunidades de optimización de los procesos de negocio, apoya la toma de decisiones, ayudan a la optimización de los costes y dan soporte en el control de los gastos empresariales.

¿Qué es la protección de datos?

Desde que en mayo de 2018 fuese directamente aplicable en España el Reglamento General de Protección de Datos o RGPD, la protección de datos se ha convertido en un tema recurrente en el mundo empresarial, ya que todas las empresas han tenido que adoptar medidas para proteger los datos personales y así “esquivar” las cuantiosas multas que impone la nueva normativa mientras mejoran la imagen de su marca.

En la práctica, el tejido empresarial ha ido adaptándose de forma desigual. Aunque no manejamos datos de este 2021, los últimos estudios concluían que en torno al 48% de las empresas españolas no han terminado de implantar las medidas necesarias para cumplir con el RGPD, a pesar de que el 69 % de la población de la UE de más de 16 años ha oído hablar del RGPD según la encuesta de la Agencia de los Derechos Fundamentales de la Unión Europea “Your rights matter: data protection and privacy” [REF-5].

La protección de datos es un derecho fundamental (de hecho, está reconocido como tal, a la misma altura que el derecho a la salud, a la dignidad, etc.) de todas las personas físicas. Esto impone a las empresas (“Responsables del tratamiento”) la necesidad de cumplir una serie de obligaciones y principios de cara a proteger los datos de carácter personal de sus clientes/proveedores/empleados (“interesados”). En definitiva, es una garantía de que este derecho se respeta y los datos se utilizan tan solo para lo necesario.

Una correcta gestión de la privacidad va a reportar numerosos beneficios a medio y largo plazo a los comercios, tales como mejora de la reputación, mejor gestión de los activos, mayor competitividad, menos exposición a brechas e incidentes y sobre todo, garantía de cumplimiento normativo de cara a no ser multados y/o demandados con los costes que ello apareja.

Las circunstancias de cada tratamiento van a determinar los requisitos que debemos cumplir en función del riesgo que implica cada tratamiento de datos. Evidentemente, a mayor riesgo, mayores cautelas deben adoptarse, y mayor será la sanción en caso de incumplimiento. En este sentido, un tratamiento de datos de contacto de proveedores tiene un riesgo mucho menor que el riesgo resultante de tratar datos de salud de menores de edad, por ejemplo.

Fondo Europeo de Desarrollo Regional
“Una manera de hacer Europa”
GOBIERNO DE ESPAÑA · VICEPRESIDENCIA PRIMERA DEL GOBIERNO · MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL · red.es · UNIÓN EUROPEA

Los datos personales

Los datos personales son cualquier tipo de información que identifique o haga identificable (permita identificar con ayuda de otros datos) a una persona física. [REF-6].

Los datos personales que son de gran importancia para las personas y las empresas que reutilizan los mismos. El problema de esto es que su publicación abierta o uso para finalidades distintas de la planteada en un primer momento, puede crear amenazas hacia la privacidad de las mismas personas, lo que conllevaría sanciones y un detrimento reputacional de la empresa.

Todos los datos personales están protegidos por el RGPD. Lo que significa que, una vulneración de los mismos está sancionada y perseguida por la normativa aplicable. Son embargo, los datos anonimizados (desvinculados de las personas a la que les pertenecen) no están sujetos a dicha normativa, pero sería el único caso.

Con la finalidad de conocer qué son considerados datos personales y no personales, a continuación, se exponen diversos ejemplos que podrían ser obtenidos, por ejemplo, en el momento que un cliente realice una compra online en nuestra web:

› Cumplimiento técnico de la protección de datos

La Agencia Española de Protección de Datos (AEPD) es la autoridad pública independiente, creada en 1992, cuyo objetivo es el de garantizar la privacidad y la protección de datos de los ciudadanos, así como el cumplimiento de las normas: el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPD-GDD).

En este sentido, consciente del reto que puede suponer para las pymes una correcta adaptación sin contar con un experto, la AEPD ha puesto a disposición de los ciudadanos herramientas gratuitas que se explican a continuación para que las empresas y comercios puedan tomar decisiones adecuadas sobre cuál se adapta mejor a sus necesidades y puedan poner a prueba su nivel de cumplimiento.

Facilita RGPD

El RGPD es de aplicación desde mayo de 2018 y, la AEPD, con la finalidad de que las empresas y profesionales puedan tratar datos con un menor para los derechos y libertades de la ciudadanía, ha puesto a su disposición la herramienta Facilita RGPD [REF-7].

Su funcionamiento es muy básico. Mediante tres pantallas con preguntas determinadas, facilita el conocimiento de la situación actual de la empresa que la utiliza en relación con el tratamiento de los datos que lleva a cabo en su día a día. Avisa también a la empresa o comercio en cuestión si se adapta a esta herramienta o si, por el tipo de tratamiento y sus circunstancias, debe someterse a un análisis de riesgos.

Facilita RGPD, una vez terminado el análisis de la empresa, proveerá a la misma de documentación que debe ser incorporada en sus formularios de recogida de datos personales, cláusulas contractuales, el registro de actividades de tratamiento y también ofrecerá un anexo con medidas de seguridad orientativas para la empresa.

Sin embargo, la obtención de esta documentación no implica el cumplimiento automático del RGPD, debiendo la empresa adaptar la documentación resultante del análisis a la situación de los tratamientos de datos que esté llevando a cabo.

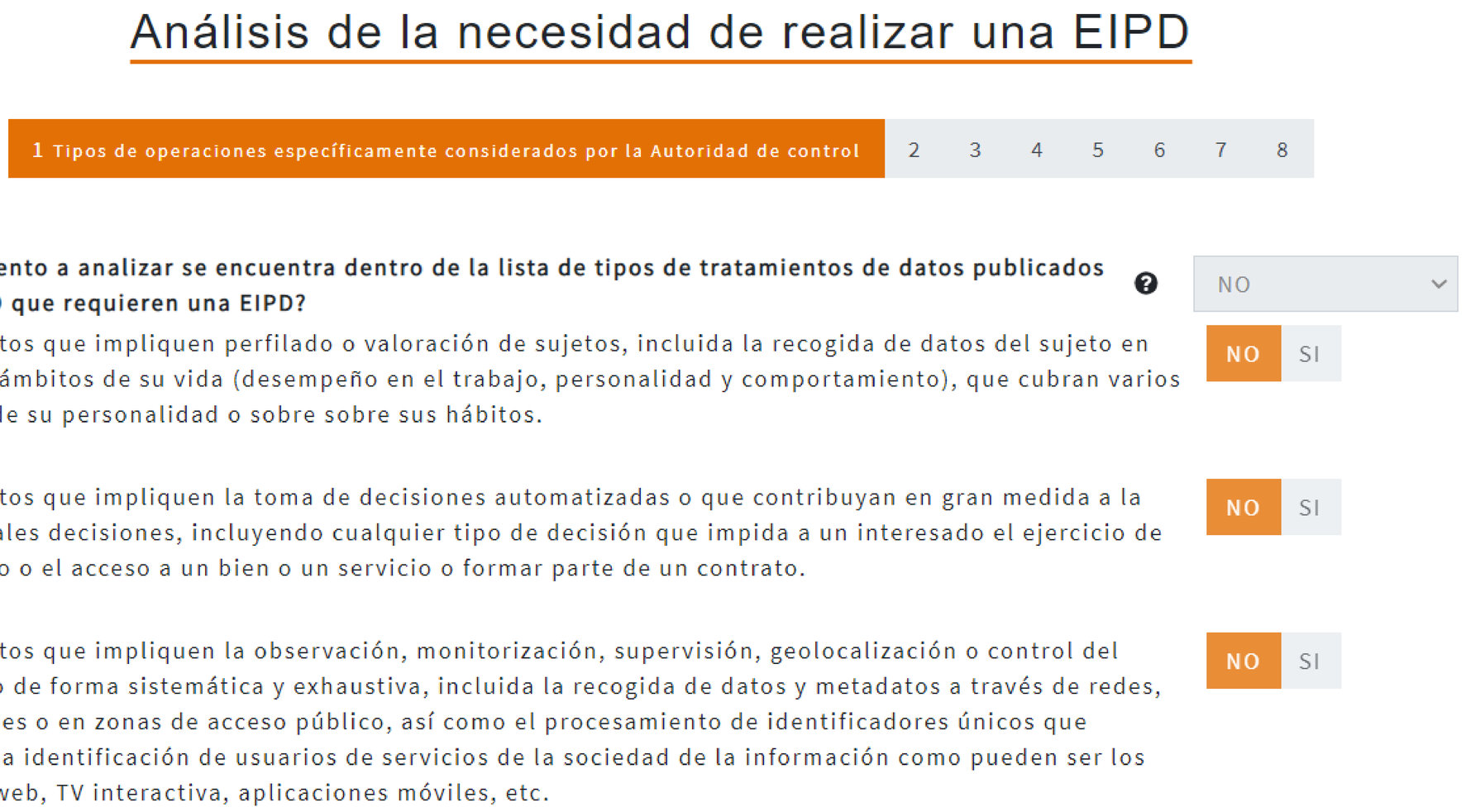
Gestiona EIPD

Cuando un tratamiento de datos sea potencialmente de alto riesgo, el RGPD exige a las empresas o comercios la realización de la Evaluación de Impacto relativa a la protección de datos (EIPD) con el fin de gestionar los riesgos que podrían afectar a derechos y libertades de los ciudadanos.

Gestiona EIPD [REF-8] es una herramienta de carácter gratuito que da soporte en la realización de la evaluación de impacto y guía al usuario a través de los elementos a considerar en los análisis de riesgos.
La herramienta ofrece las bases mínimas y los requisitos de cumplimiento normativo que deben ser considerados para la reducción del riesgo en el tratamiento de los datos.

Gestiona EIPD ofrecerá al usuario la documentación sobre la que debe realizar el análisis y la gestión de riesgos para cumplir con el RGPD y la LOPDGDD.

Será especialmente útil para aquellas pymes que deben realizar por primera vez una evaluación de impacto en la protección de datos personales.



Fondo Europeo de Desarrollo Regional
"Una manera de hacer Europa"
GOBIERNO DE ESPAÑA · VICEPRESIDENCIA PRIMERA DEL GOBIERNO · MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL · red.es · UNIÓN EUROPEA

Facilita EMPRENDE

Es una herramienta similar a Facilita RGPD, basada en cuestionarios guiados que permiten considerar el tipo de tratamiento de datos realizado por las empresas. Sin embargo Facilita EMPRENDE [REF-9] está orientada a emprendedores y start-ups cuyo tratamiento de datos esté muy vinculado a las nuevas tecnologías.

Servicio AntiBotnet

De forma adicional y, sin ser una herramienta en sí mismo, la Oficina de Seguridad Internauta (OSI), del INCIBE, pone a disposición de cualquier empresa o comercio la posibilidad de identificar si desde la conexión a internet de la persona que realiza el análisis se ha detectado algún tipo de incidente de seguridad para tus datos, relacionado con botnets (Una botnet es capaz de controlar numerosos ordenadores de usuarios de forma completamente remota para propagar virus, generar spam y cometer otros tipos de delitos y fraudes en la Red) u otras amenazas, aportando al usuario información y distintos enlaces que podrán dar soporte en la limpieza de los dispositivos, en caso de resultar infectados [REF-10].

Cumplimiento organizativo y legal

Tan importante es el cumplimiento de las normas sobre protección de datos, como ser capaz de demostrarlo mediante la actualización de los documentos pertinentes. El RGPD se basa en el principio de responsabilidad proactiva, que implica que el responsable debe cumplir con sus obligaciones por sí mismo, y ser capaz de acreditarlo.

La documentación clave que debe ser generada por la empresa y actualizada cada vez que sea necesario es la siguiente:

- Política de privacidad. Documento legal en el que la empresa detalla su manera de retener, manejar o procesar los datos recabados sobre los usuarios y sus clientes.
- Registro de Actividades de Tratamiento (RAT) precumplimentado. Sustituye la anterior inscripción de ficheros, estableciendo que cada responsable y encargado del tratamiento de los datos tendrá un registro de cada actividad de tratamiento que se haya efectuado bajo su responsabilidad.
- Modelo de hoja de registro de incidentes. Este modelo se anexará al RAT, y en él, se podrán registrar las incidencias en el caso de que las hubiere.
- Cláusulas contractuales a incluir en los contratos que sean suscritos con los encargados de tratamientos de datos y proveedores.
- Para el caso de las empresas con una página web disponible en la que se estén utilizando cookies, una política de cookies y un banner advirtiendo de su utilización.

Estos documentos son generados por las herramientas que se indican en el apartado anterior.

Sin embargo, como se ha mencionado con anterioridad, el hecho de descargar y completar los formularios disponibles en las herramientas no implica el cumplimiento automático con RGPD. Además de ello, hay muchas obligaciones que podrían afectarte en ciertos casos, tales como la obligatoriedad de nombrar un DPO, implementar medidas de seguridad, conservar consentimientos, o ser capaz de dar respuesta al ejercicio de derechos de los interesados.

> RGDP para pymes

Desde que en mayo de 2018 fuese directamente aplicable en España el Reglamento General de Protección de Datos o RGPD, la protección de datos se ha convertido en un tema recurrente en el mundo empresarial. Por esto, es necesario que todas las empresas, sin importar su tamaño, analicen su situación en este sentido.

En este sentido, el Incibe pone a disposición de las pymes, toda la información necesaria para el cumplimiento del RGPD [REF-11].

¿Debo cumplir con RGPD?

Las empresas que se exponen a continuación son las que deberán cumplir con el RGPD.

Las autoridades competentes podrán investigar y sancionar a aquellas pymes que no cumplan con la normativa. En el caso de ser investigada, una empresa deberá aportar toda la información que le sea solicitada, se someta a auditorías o ceda el acceso a sus datos.

Las sanciones en caso de incumplir con la normativa irán desde una advertencia, pasando por apercibimientos y limitaciones de la actividad delimitados en el tiempo, hasta prohibir el tratamiento de datos y la imposición de multas.

¿Cómo he de cumplir con la normativa?

Para que pueda decirse que una empresa cumple con el RGPD, se deben garantizar los derechos y libertades de los ciudadanos desde el planteamiento inicial del modelo de tratamiento de sus datos personales. Para ello, deben de considerarse una serie de aspectos:

- Identificación de si son tratamientos de datos de alto riesgo [REF-12]. En caso de no serlo, como se ha mencionado con anterioridad, se podrá utilizar la herramienta Facilita RGPD.
- Realización de una evaluación de los riesgos, con la finalidad de garantizar los niveles más adecuados de seguridad.
- Desarrollar un procedimiento de verificación, evaluación y valoración de la aplicación de las medidas desarrolladas para la protección de los datos.

Organización

En este punto, ya se conoce si el tipo de tratamiento de datos realizado en una empresa o comercio es considerando de alto riesgo o para todo tipo de tratamientos. En este sentido:

Si se ha llegado a la conclusión de que el tratamiento de datos es de alto riesgo, deben realizarse una serie de actividades:

- Desarrollar un registro de las actividades en las que se realiza un tratamiento de datos personales.
- Nombrar, en la organización, a un delegado de protección de datos.
- Llevar a cabo un análisis de impacto del tratamiento de los datos personales.

Por otro lado, tanto para tratamientos de alto riesgo como de bajo riesgo, deben realizarse una serie de tareas:

- Establecer procedimientos adecuados, así como los distintos canales para informar a los usuarios sobre el tratamiento de los datos, recabar su consentimiento y permitir, en todo caso, el ejercicio de sus derechos. Adicionalmente, se notificará la existencia de algún tipo de brecha de seguridad que pueda afectar la privacidad de los datos.
- En caso de tener un encargado del tratamiento de los datos, se deben revisar los contratos.
- Establecer políticas para asegurar que el tratamiento de datos es seguro.
- Realizar formaciones y concienciar a los empleados en el tratamiento de los datos.

Tecnología

Con el fin de garantizar la confidencialidad, disponibilidad e integridad de los datos personales, así como su tratamiento, permitiendo en todo caso que las autoridades competentes puedan verificarlo, se debe revisar que se dispone de los canales tecnológicos, que nos permitan informar sobre el tratamiento de datos, obtener el consentimiento del usuario garantizando en todo caso sus derechos, así como notificar, tanto a las autoridades como a los usuarios, en el hipotético caso de existir algún tipo de violación que pueda suponer un determinado riesgo para los datos que están siendo tratados.

Problemas y errores comunes en la protección de datos

Existen múltiples aspectos que deben ser considerados para el correcto cumplimiento normativo de protección de datos. La AEPD pone a disposición del usuario de una lista, llamada “Listado de cumplimiento normativo” en la que se puede comprobar. Listado de cumplimiento normativo.

Si se navega por el mencionado listado, puede comprobarse que hay múltiples aspectos a considerar, por lo que es común la existencia de numerosos problemas que pueden darse a la hora del tratamiento de datos por parte de las empresas.

A modo de resumen se exponen, a continuación, algunos de los más comunes [REF-13]. Muchos de estos errores pueden llevar asociada una multa o sanción por parte de las autoridades, por lo que debe prestarse atención a los requisitos de la legislación y conocerla.

- Uno de los principales problemas se da por el desconocimiento por parte de numerosas empresas o comercios acerca de las obligaciones legales sobre la protección de datos personales, recogidas en la legislación nacional, lo que hace que puedan existir incumplimientos de determinados aspectos (algunos ejemplos son mostrados a continuación). Adicionalmente, las empresas tampoco forman a sus empleados recurrentemente en este aspecto.

- Otro aspecto relevante en cuanto a la protección de datos es dejar en algún lugar sin ningún tipo de seguridad (encima de la mesa, impresora, etc.). documentos con información confidencial (por ejemplo un contrato). La información sensible debe estar en todo momento fuera de la vista.

- El uso de formularios de contacto únicos es otro de los errores frecuentes que las empresas suelen cometer para obtener datos personales, utilizando un mismo formulario para todo.

A *pyme comercio*

- Otro problema recurrente se da en el momento de la contratación de un empleado que disponga de una base de datos de contactos, ya que frecuentemente se solicita la incorporación de estos contactos a la base de datos de la nueva empresa. Esto no estaría legalmente permitido, ya que los contactos de la persona contratada no han dado su consentimiento explícito para formar parte de la nueva base de datos.
- En muchas ocasiones, las campañas de e-mail marketing o envío de publicidad por correo tampoco están permitidas y suele ser un error frecuente. Determinadas empresas o comercios disponen en sus bases de datos de correos de contacto de personas, sin embargo no tienen el consentimiento explícito de algunas de estas personas para enviarles este tipo de información por correo.
- Otro error que se desconoce normalmente es la necesidad de contar con los datos de la empresa en su página web para que cualquier usuario pueda consultarlos. Adicionalmente en la web, también es necesario contar con el aviso de uso de cookies, así como con la política de privacidad, en la que se informa al usuario sobre el tratamiento de sus datos.
- Muchas pymes desconocen también la necesidad de establecer un contrato con aquellos encargados del tratamiento de sus datos (normalmente suele ser una gestoría).

Sanciones aplicables

El Artículo 83 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD) regula las sanciones aplicables por los Estados Miembro en caso de incumplimiento del mismo reglamento, que pueden ascender a un máximo de 20 millones de euros o el importe equivalente al 2 – 4% del volumen anual de negocios a nivel global [REF-14].

En este sentido y, según un estudio elaborado por Finbold, España encabeza el número de multas impuestas por incumplimiento del RGPD, con un total de 34 multas y un monto que suma más de 15 millones de euros de multas impuestas por las autoridades (en el primer trimestre de 2021) [REF-15].

Country	Total fines in EUR in Q1 2021 (Jan 1 - Mar 31)	Number of fines by country
Spain	€15,700,300	34
Germany	€10,700,200	3
Italy	€5,656,000	20
Netherlands	€ 440,00	1
Norway	€ 382,75	12
France	€ 245,00	3
Czech Republic	€ 118,50	1
Belgium	€ 86,00	4
Poland	€ 81,30	5
Cyprus	€ 81,00	4
Latvia	€ 65,00	1
Lithuania	€ 30,00	3
Romania	€ 13,50	4
Denmark	€ 13,45	1
Greece	€ 2,00	1

A *pyme comercio*

Adicionalmente, un informe realizado por la firma KPMG, analiza los principales motivos por los que se sanciona en Europa, por el incumplimiento o desconocimiento de la normativa [REF-16].

En este sentido, estos motivos son:

- Incumplimiento al establecer las medidas de seguridad necesarias para el tratamiento de los datos.
- Inexistencia de una base de legitimación que habilite al tratamiento de los datos personales.
- Incumplimientos de los principios de tratamiento de los datos recogidos en el RGPD.
- Falta de notificación de las brechas de seguridad y las violaciones a los usuarios.
- Desatención a los derechos de protección de datos personales ejercidos por los usuarios.
- Incumplimiento del deber de informar.
- No existencia de un contrato de encargo para el tratamiento de los datos que regule la relación entre el encargado del mismo y el responsable.

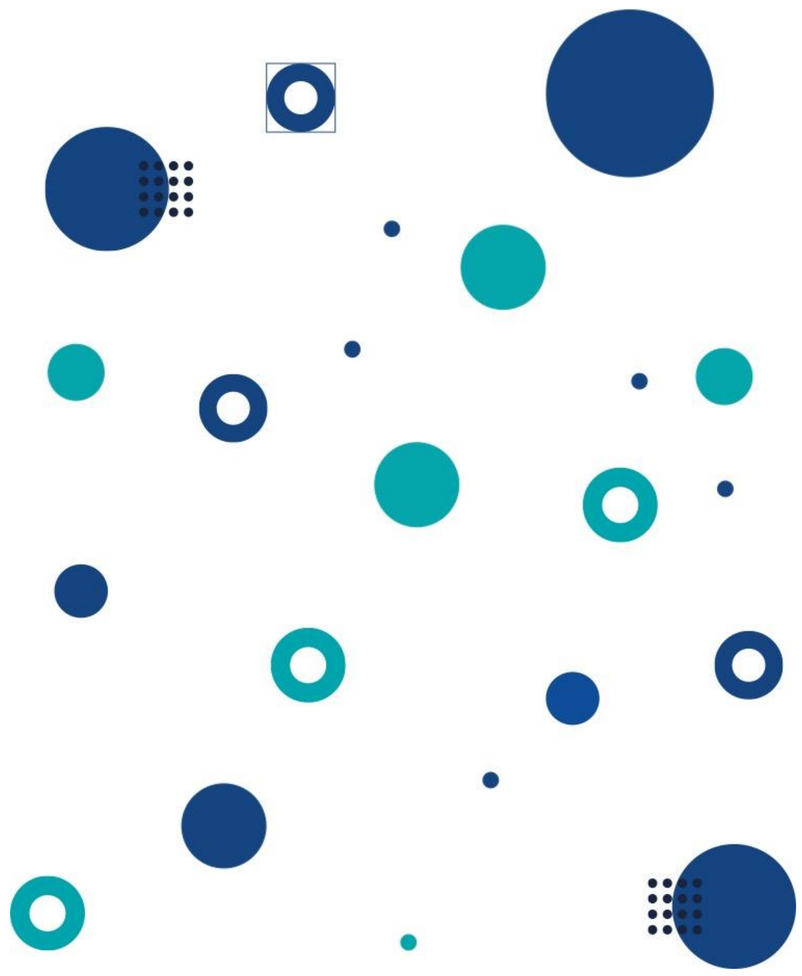
Considerando lo anteriormente descrito se detalla, a continuación, un ejemplo de sanción interpuesta por las autoridades a una pyme nacional por el incumplimiento del RGPD.

La Agencia Española de Protección de Datos multó, en el año 2020 a una pyme madrileña con una cuantía que asciende a 50.000€ por la inexistencia del perfil de DPO (Data Protection Officer) o Delegado de Protección de Datos cuando debía tenerlo.

La figura del DPO es considerada clave por la AEPD como referente en la garantía del cumplimiento de la legislación de protección de datos y la ausencia de esta figura, en el caso de resultar necesario, está considerada como infracción grave en la Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

Otro ejemplo de multa interpuesta por la Agencia Española de Protección de Datos se dio por la reutilización de papeles con datos confidenciales en el reverso por parte de una abogada. En este caso la multa ascendió a un total de 2.000 €

Conclusiones



No es en vano destacar la gran importancia que a día de hoy tienen los datos a nivel empresarial, el gran volumen de datos que gestionan las empresas, generó más de 2.500 millones de euros en 2019.

Considerando que los datos tienen tan alto valor, es necesario velar por su protección y su buen uso. En este sentido, existen múltiples herramientas, puestas a disposición por distintos organismos públicos, cuyo objetivo es dar soporte en el cumplimiento de la protección de los datos personales a las empresas y facilitar la puesta en marcha de políticas de protección de datos en grandes y pequeñas empresas.

Sin embargo, esto no es suficiente en todo caso. Es necesario conocer la legislación aplicable en materia de protección de datos, así como los principales problemas que pueden darse por este desconocimiento ya que, en muchas ocasiones, este desconocimiento lleva asociado la comisión de errores que pueden derivar en sanciones o apercibimientos por parte de las autoridades encargadas de velar por el cumplimiento.

Adicionalmente, debemos ser conscientes que nuestro comercio maneja un gran volumen de datos de carácter personal, por lo que debemos conocer la importancia de estos y la necesidad de disponer del conocimiento suficiente para darles una protección adecuada, acorde a la legislación.

En conclusión, conocer la importancia de los datos, asegurar su buen tratamiento acorde a la legislación y cumplir con las obligaciones establecidas para las empresas, son aspectos que deben considerarse para evitar potenciales sanciones.

Fondo Europeo de Desarrollo Regional
"Una manera de hacer Europa"
GOBIERNO DE ESPAÑA · VICEPRESIDENCIA PRIMERA DEL GOBIERNO · MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL · red.es · UNIÓN EUROPEA

Referencias

[REF-1] El volumen de datos en las empresas crece un 569% en dos años. Redacción Computing. https://www.computing.es/analytics/noticias/1113253046201/volumen-de-datos-empresas-crece-569-dos-anos.1.html#:~:text=El%20volumen%20de%20datos%20que,rendimiento%20econ%C3%B3mico%20de%20los%20mismos.

[REF-2] Dossier de Indicadores de sobre uso de Big Data por empresas en España y Europa. ONTSI. Abril 2020. https://www.ontsi.red.es/dossier-de-indicadores-pdf/BigData

[REF-3] Madurez data driven de las empresas. INCIPY. 2021. https://www.incipy.com/estudio-madurez-data-driven/

[REF-4] Sector Infomediario. ASEDIE. 2021. https://static1.squarespace.com/static/600a99c4d2a8133c3599fc67/t/607ff089596f9b27bfc11636/1618997397041/ISI21+VF++web.pdf

[REF-5] "Your rights matter: data protection and privacy". Agencia de los Derechos Fundamentales de la Unión Europea. 2020. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-fundamental-rights-survey-data-protection-privacy_en.pdf

[REF-6] Definición datos personales. Comisión Europea. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es

[REF-7] AEPD. Facilita RGPD. https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd

[REF-8] AEPD. Gestiona EIPD. https://www.aepd.es/es/guias-y-herramientas/herramientas/gestiona-eipd

[REF-9] AEPD. Facilita EMPRENDE. https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-emprende

[REF-10] Oficina de Seguridad del Internauta. Servicio AntiBotnet. https://www.osi.es/es/servicio-antibotnet

[REF-11]. RGPD para pymes. Incibe. https://www.incibe.es/protege-tu-empresa/rgpd-para-pymes

[REF-12] Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (art 35.4). AEPD. https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf

Fondo Europeo de Desarrollo Regional
"Una manera de hacer Europa"
GOBIERNO DE ESPAÑA · VICEPRESIDENCIA PRIMERA DEL GOBIERNO · MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL · red.es · UNIÓN EUROPEA

Referencias

[REF-13] RGPD: las 12 dudas y errores más frecuentes. Blog Cuatrecasas. 2018. https://blog.cuatrecasas.com/propiedad-intelectual/rgpd-dudas-frecuentes/

¿Cuál es el impacto de la protección de datos en las Pymes? Confilegal. 2018. https://confilegal.com/20181013-cual-es-el-impacto-de-la-proteccion-de-datos-en-las-pymes/

Los 10 errores más comunes en RR.HH tras el GDPR. TICPymes. 2018. https://www.ticpymes.es/legislacion/noticias/1106838049204/10-errores-mas-comunes-rrhh-gdpr.1.html

[REF-14 REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). https://www.boe.es/doue/2016/119/L00001-00088.pdf

[REF-15] EU countries hit with over €30 million in GDPR fines in Q1 2021. Finbold. 2021. https://finbold.com/eu-countries-hit-with-over-e30-million-in-gdpr-fines-in-q1-2021/

[REF-16] Aplicando el RGPD: quién, cuánto, cómo, a quién y qué se sanciona. KPMG. 2020. https://www.tendencias.kpmg.es/2020/02/rgpd-aplicacion-sanciones/

Fondo Europeo de Desarrollo Regional

"Una manera de hacer Europa"

GOBIERNO DE ESPAÑA · VICEPRESIDENCIA PRIMERA DEL GOBIERNO · MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL · red.es · UNIÓN EUROPEA