GUÍA

SOBRE EL RGPD

PARA

Autónomos y Pymes

CG consulting
ASESOR EMPRESAS Y AUTÓNOMOS

ÍNDICE

INTRODUCCIÓN

El próximo 25 de mayo el Reglamento General de Protección de Datos (RGPD) será de obligado cumplimiento en todos los estados de la Unión Europea. Esta normativa entró en vigor el pasado 25 de mayo de 2016 y dio un plazo de adaptación de dos años que ya culmina.

El RGPD tiene por finalidad garantizar la protección de los datos personales facilitados a empresas y Organismos Públicos.

La nueva normativa europea, de obligado cumplimiento para autónomos y pymes, nace para unificar el criterio de los 28 Estados miembro y ofrece las pautas para que cada uno de ellos adapte su propia legislación a la directriz europea.

El RGPD no solo incluye los derechos y deberes clásicos en materia de protección de datos, que ya venían recogidos en la ahora derogada Directiva 95/46/CE, sino que los especifica e introduce otros nuevos.

Este documento, es una guía para orientarte a ti como profesional y empresario sobre el RGPD, para que conozcas sus pormenores y consigas adaptar tu negocio a las nuevas obligaciones.

En este documento, que ponemos a tu disposición, encontrarás una aproximación al actual marco normativo español, donde está vigente la Ley Orgánica de Protección de Datos (LOPD), y hablamos sobre el proyecto de Ley en vías de tramitación que la modificará próximamente. Y, por supuesto, profun-dizaremos en el propio RGPD, lo que debes saber y cómo debes de adaptarte a él.

Esta hoja de ruta aborda los principios básicos de la norma europea y la forma en que tienen que ser aplicados. Se detiene en la figura del Delegado de Protección de Datos (DPD) y explica cómo realizar la Gestión de Riesgos y la Evaluación de Impacto.

Además, analiza las consecuencias económicas del incumplimiento del Reglamento y la cuantía de las sanciones a las que podrías que tener que enfrentarte en caso de infracción.

Esta guía sobre el RGPD termina acercándote a los derechos de acceso, rectificación, cancelación y oposición que tienes como persona física frente a otros autónomos y empresarios.

1. MARCO LEGAL ESPAÑOL ACTUAL

El marco normativo actual que regula en España la protección de datos, junto con el ya vigente Reglamento de Protección de Datos (RGPD), se fundamenta en la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD).

Se trata de una norma que recoge el derecho a la protección de datos personales y el control sobre el uso que personas físicas, jurídicas y organismos públicos realizan de los mismos.

Si te preguntas si, como autónomo o pyme, estás obligado a cumplir la Protección de Datos la respuesta es clara, sí. La LOPD establece que tanto trabajadores por cuenta propia como empresas, del ámbito privado y público, garanticen el derecho a la intimidad de quienes facilitan sus datos. Unos datos que son clasificados de nivel básico, medio o alto, en función de la información que contengan.

"Autónomos y pymes estáis obligados a cumplir tanto la LOPD como el RGPD"

Por tanto, ¿por qué has de seguir cumpliendo con la actual LOPD al tiempo que lo haces también con el RGPD?

▷ Por imperativo legal. La protección y la privacidad de datos de carácter personal es un derecho fundamental, recogido en el artículo 18 de la Constitución, por el que debes velar desde tu posición.

▷ Por evitar sanciones de la Agencia Nacional de Protección de Datos. El incumplimiento de la ley conlleva sanciones administrativas que pueden ser cuantiosas. Multas que van desde los 900 euros, en caso de infracciones leves, hasta los 600.000 si son graves, en el caso de la LOPD, y sin establecer mínimo puedes ser sancionado hasta con 20 millones de euros o el 4% del volumen anual global de tu negocio, en el caso del RGPD.

▷ Por una cuestión de confianza: La solicitud de datos es el pan nuestro de cada día para el desarrollo de tu actividad económica. Garantizar al cliente el correcto tratamiento de sus datos es básico para que las relaciones lleguen a buen puerto.

▷ En previsión a pérdidas de información. Debes considerar el coste para tu negocio que supondría la fuga de datos personales y confidenciales ya que pueden incurrir en responsabilidades civiles y, con la RGPD en mano, incluso penales.

Las obligaciones legales que conlleva el cumplimiento de la Ley Orgánica de Protección de Datos (LOPD) son en aras de garantizar la privacidad de los datos. Para ello, el responsable del tratamiento de datos tiene como cometidos:

▷ Identificación de los ficheros que contengan datos de carácter personal (empleados, clientes, proveedores, etc...).

▷ Registro de los ficheros de datos en la Agencia de Protección de Datos.

"El incumplimiento del marco legal puede llevarte a ser sancionado administrativa, civil y penalmente"

▷ Identificación del nivel de seguridad que se les aplica.

▷ Incluir avisos legales de información y consentimiento.

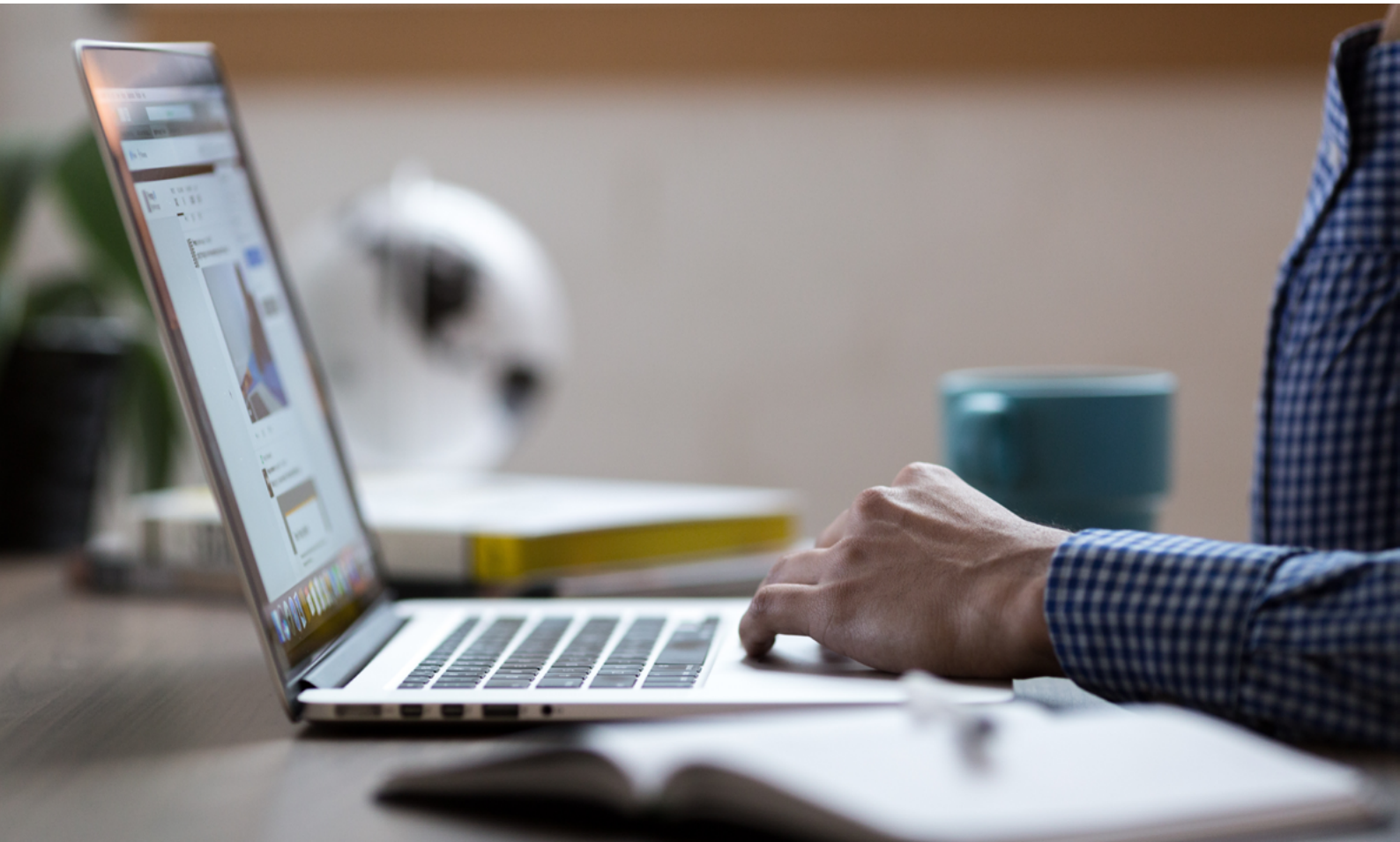
▷ Elaboración del Documento de Seguridad.

▷ Información a los propietarios de los datos, sobre la existencia de los ficheros.

"La aplicación del RGPD obliga a la adaptación de la normativa española a su articulado. En la actualidad ya hay un Proyecto de Ley a la espera de ser aprobado"

Como ya apuntábamos, la aplicación del RGPD obliga a la adaptación de la Ley Orgánica de Protección de Datos en vías de tramitación. El pasado 10 de noviembre el Gobierno aprobaba el proyecto de Ley de Protección de Datos que derogará la actual ley de 1999.

Sin embargo, todo apunta a que la nueva norma nacional no llegará a tiempo para el próximo 25 de mayo. Por tanto, hasta la aprobación definitiva y puesta en marcha del proyecto de ley, la LOPD actual regulará la protección de datos en aquello que no se oponga al reglamento.



Preguntas y respuestas sobre el RGPD

"¿Cuál es el objetivo del RGPD?"

Unificar la normativa de los Estados miembro de la Unión Europea

"¿Cuándo entra en vigor la aplicación definitiva del RGPD?"

¡El **25 de mayo** de 2018!

"¿Habrá sanciones si no se cumple con el RGPD?"

Sí, y pueden ser **de hasta 20 millones de euros** o hasta el **4% de tu volumen de negocio**

"¿Cuáles son los principios básicos del RGPD?"

Ampliar y reforzar los derechos en protección de datos personales

"¿Qué debo tener en cuenta para implementar el RGPD?"

Debes tener en cuenta la figura del **Delegado de Protección de Datos** (DPD) y el **Programa de Evaluación de Impacto**

3. ACERCAMIENTO AL RGPD

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, RGPD, establece un nuevo articulado sobre el tratamiento de los datos personales. Y aunque a veces ni caigamos en la cuenta, en innumerables ocasiones, recabamos información personal que está protegida por ley. Lo hacemos, por ejemplo, cada vez que hacemos una ficha de contacto al visitar nuestra web o cuando pedimos información telefónica a nuestro cliente.

Esta normativa será de aplicación en todo el territorio de la UE, el Reino Unido (tras su salida del UE en 2019) y todas las empresas fuera de la UE que ofrezcan bienes o servicios a personas de la UE o que controlen su comportamiento dentro de las UE.

Están obligadas a adecuarse a su articulado todas las empresas, sociedades, autónomos, comunidades, asociaciones y administraciones públicas de los Estados miembro, obviamente, también las españolas.

Están obligadas a adecuarse a su articulado todas las empresas, sociedades, autónomos, comunidades, asociaciones y administraciones públicas de los Estados miembro, obviamente, también las españolas.

El RGPD recoge los principios básicos en los que se basa su articulado:

▷ Relativos a la protección de datos.

La información en la recogida de datos personales tiene que ser clara para que sea fácilmente comprendida por el interesado. Además, los datos tienen que ser recogidos de manera limitada a lo necesario ya que tienen que tener un fin previamente establecido que además tiene que ser legítimo.

Deben mantenerse actualizados y almacenados de un modo en el que quede garantizada su seguridad.

▷ Relativos al tratamiento de los datos.

"El RGPD se basa en los principios relativos a la protección de datos, el tratamiento de los mismos y su envío internacional"

El tratamiento de los datos tiene que ser lícito. Y solo estamos ante un tratamiento lícito si cumple con determinadas condiciones como que se dé el consentimiento expreso por parte del interesado para su uso, que los datos sean utilizados para la firma de un contrato en el que el interesado interviene o cuando sean imprescindibles para para proteger intereses legítimos.

▷ Relativos al envío internacional de datos personales.

Debes saber que está prohibido enviar datos personales fuera de Espacio Económico Europeo a un país que no ofrezca la suficiente protección a los mismos. En caso de no existir una garantía, esa transferencia puede estar limitada con determinadas cláusulas contractuales.

Si tienes claro que tienes que adecuar tu gestión de los datos a la nueva normativa y tienes claro en qué término, atento al listado de claves básica del RGPD que debes tener en cuenta:

1º Se amplía el derecho de las personas a conocer la finalidad y el tratamiento de sus datos personales cuando le sean solicitados.

2º Para pedir datos personales hay que hacerlo mediante una declaración clara y expresa. ¿Te acuerdas de la casilla en una plantilla fija de tu web donde venía

"Se amplía el derecho de las personas a conocer la finalidad y el tratamiento de sus datos personales"

la información sobre la protección de datos? Podrás seguir poniéndola, pero ¡cuidado! porque en ningún caso podrá estar premarcada.

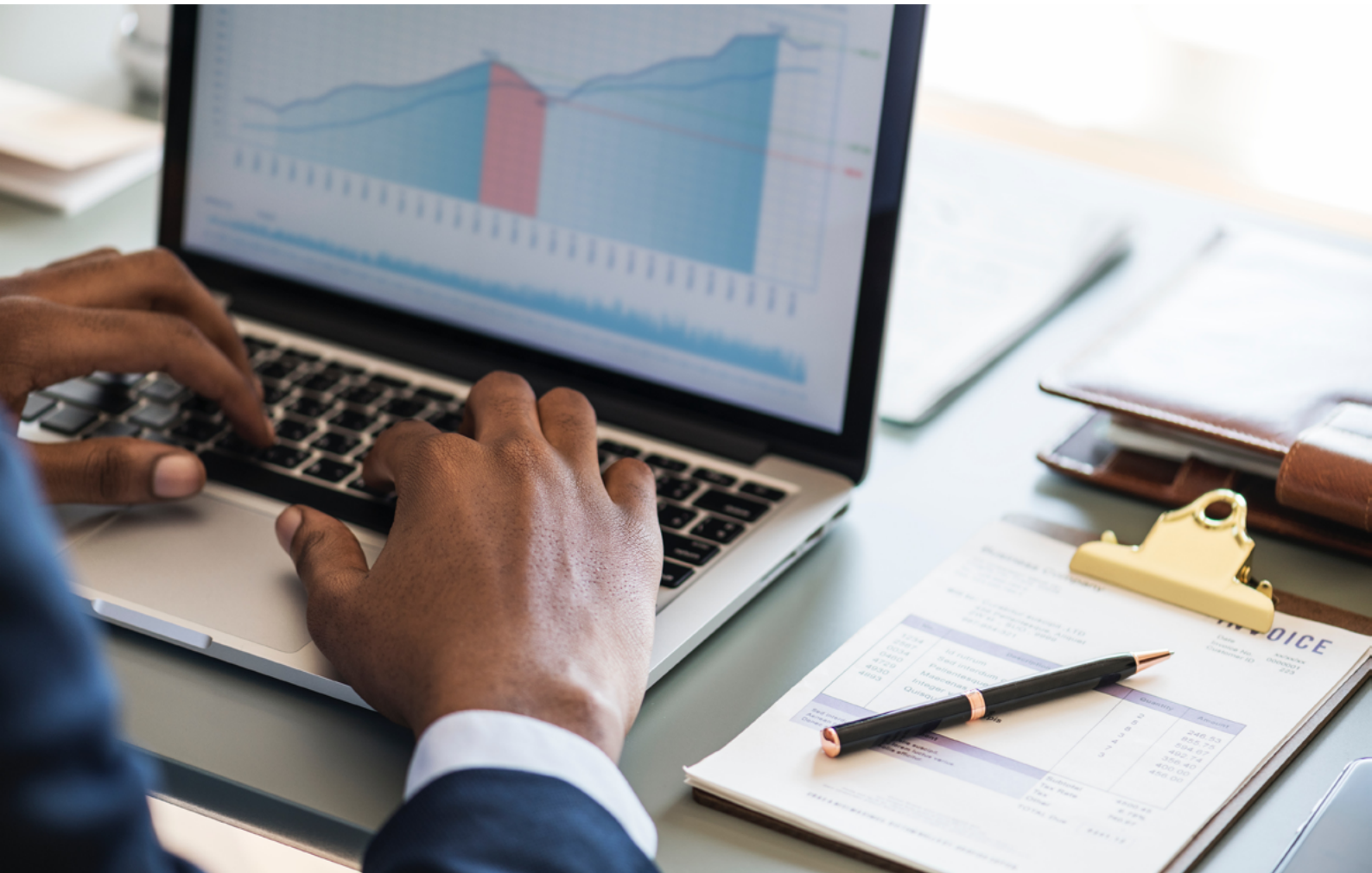
3º Solo pueden usarse los datos para los fines estipulados desde el inicio, cualquier otro uso, en principio, es considerado ilícito.

4º El interesado tiene derecho a mover, copiar o transferir de manera personal sus datos a otra empresa, incluso cuando quiera llevárselos a la competencia.

5º Si existen violaciones en la seguridad de la protección de datos los responsables de estos tienen que avisar a las autoridades competentes en menos de 72 horas.

6º Aparece la figura del Delegado de Protección de Datos (DPD) obligatoria para empresas que llevana a cabo una observación habitual y sistemática o si tratan a gran escala categorías especiales de datos.

7º Se amplían las sanciones, con respecto a la LOPD, por el incumplimiento y las infracciones al articulado. Pueden llegar a oscilar entre a los 10 y los 20 millones de euros o entre el 2 y 4% del volumen de negocio en caso de ser una empresa, en casos extremos.



4. CÓMO ADAPTARSE AL RGPD SI ERES AUTÓNOMO O PYME

Si durante los últimos dos años no has procedido ahora puedes hacerlo.

Y es que con el articulado del RGPD en la mano se te exige una responsabilidad proactiva, también llamada "Accountability" que, básicamente, significa que estás en disposición de adaptarte de manera garantizable a las reglas, derechos y garantías que ordena la normativa europea para garantizar los derechos y libertades de las personas.

Piensa que el RGPD actúa cuando la infracción sucede porque entiende que se está ocasionando daños a los interesados, por ello es muy importante que, previamente, analices el riesgo que existe en el tratamiento de los datos que manejas.

Toma buena nota de los pasos que debes de dar. Esta es una hoja de ruta que debes adaptar a tus necesidades:

1º Designación de un Delegado de Protección de Datos (DPD) en caso de ser obligatorio, o si la empresa decide asumirlo de forma voluntaria. Si no es obligatorio para ti, identifica a la persona responsable de Coordinar la Adaptación.

"Se te exige una responsabilidad proactiva o "Accountability" que significa que estás en disposición de adaptarte al RGPD"

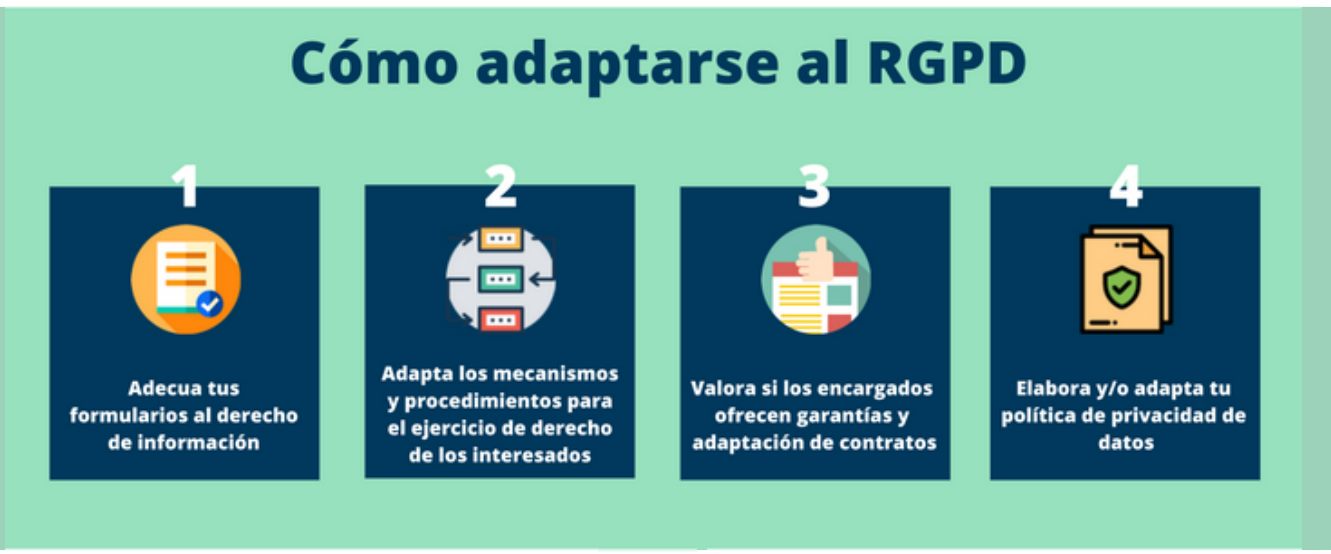
2º Elabora un registro de actividades de Tratamiento teniendo en cuenta la finalidad que darás a los datos recopilados y la base jurídica en el que se fundamenta, ya que en ningún caso podrán recabarse para fines ilícitos.

3º Realiza un Análisis de Riesgos a los que pueden verse sometidos los datos con los que trabajas.

4º Revisa las medidas de seguridad que tienes actualmente implementadas para comprobar si son útiles según los resultados que obtengas del paso anterior.

5º Establece mecanismos y procedimientos de notificación de quiebras de seguridad ya que es valorada la actitud proactiva del infractor en caso de producirse una fuga de la información.

6º A partir de los resultados de análisis de riesgos, realiza también una evaluación de impacto en la protección de datos para saber.



4.1 EL DELEGADO DE PROTECCIÓN DE DATOS

Una de las dudas más comunes que surgen ante la obligación de la aplicación del RGPD es si existe también la obligación de tener un Delegado de Protección de Datos (DPD) en el conjunto de empresas y negocios.

Los artículos 37 y 39 del Reglamento europeo regulan la figura del DPD y la obligatoriedad de designación se establece en tres supuestos:

▷ Si el tratamiento de los datos corre a cargo de una autoridad u organismo público.

▷ Si las actividades y operaciones principales del responsable de datos exigen seguimiento regular y sistemático a gran escala.

▷ Si las actividades y operaciones principales del responsable requieren tratamientos a gran escala de datos personales que tienen que ver con delitos y condenas.

Es decir, estarán obligados a tener un delegado de protección de datos aquellos negocios y empresas que tengan como objetivo el tratamiento de datos por la propia naturaleza de su actividad y/o para permitir el desarrollo de la misma.

"Los artículos 37 y 39 del RGPD regulan la figura del DPD y la obligación de su designación"

Pongamos un ejemplo para entender cómo se materializan estas indicaciones.

Pensemos en un autónomo que lanza una aplicación móvil para ligar que maneja los perfiles de sus usuarios, un colegio profesional de abogados, una asesoría o una clínica sanitaria privada. Todo ellos manejan datos que inciden directa o indirectamente con datos personales. Por tanto, ¿estarían obligados estos autónomos y pymes a contar con un Delegado de Protección de Datos?

"Para saber si un autónomo o una pyme necesitan un DPD hay que tener en consideración si el tratamiento de datos es a gran escala y si realizan un seguimiento regular y sistemático de los mismos"

Otra de las circunstancias que ha de darse en la actividad principal del empresas y negocios que obliga a disponer de un DPD es que el tratamiento de los datos sea a gran escala. Aquí influye no solo el volumen de datos o el número de perfiles involucrados sino también el alcance geográfico o la duración y permanencia de los datos en el seno de la empresa.

Por desgracia el RGPD no ha establecido unos parámetros objetivos y cuantitativos para estandarizar estos factores influyentes en el significado de datos a gran escala.

Las empresas obligadas a contratar los servicios de un delegado de protección de datos deben realizar un seguimiento regular, es decir continuado y recurrente, y sistemático, o lo que es lo mismo, preestablecido, organizado y metódico, como parte fundamental de una estrategia.

Este seguimiento no se refiere exclusivamente al tratamiento online de los datos sino a todas las empresas que realicen seguimiento y tratamiento de datos con independencia de los mecanismos para ello.

En el artículo 34 de la futura ley española, es decir en el Proyecto de la Ley General de Protección de Datos (PLOPD) del que ya se conoce el texto aunque no esté aprobado, detalla algunas de las entidades que están obligadas a la designación de un delegado de protección de datos:

▷ Colegios profesionales y sus consejos generales.

▷ Centros docentes.

▷ Entidades que exploten redes y presten servicios de comunicaciones electrónicas.

▷ Prestadores de servicios de la sociedad de la información.

▷ Entidades de crédito.

▷ Establecimientos financieros de crédito.

▷ Entidades aseguradoras y reaseguradoras.

▷ Empresas de servicios de inversión.

"El Proyecto de Ley General de Protección de Datos si detalla de forma taxativa los obligados a la figura del DPD"

▷ Distribuidores y comercializadores de energía eléctrica y de gas natural.

▷ Entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude.

▷ Entidades que desarrollen actividades de publicidad y prospección comercial.

▷ Centros sanitarios.

▷ Entidades que tengan como uno de sus objetos la emisión de informes comerciales acerca de personas y empresas.

▷ Operadores que desarrollen la actividad de juego.

▷ Quienes desempeñen las actividades de Seguridad Privada.

"El DPD puede ser interno de tu plantilla o externo, pero en cualquier caso tiene que tener conocimientos jurídicos específicos"

Aquellas empresas que no figuren en este listado pueden designar voluntariamente un delegado de protección de datos.

El delegado de protección de datos, que puede formar parte de tu plantilla o externalizar el servicio, debe tener conocimientos jurídicos que le servirán de base para el tratamiento de los datos y el correcto desarrollo de sus competencias profesionales que más abajo detallaremos.

La Agencia Española de Protección de Datos (AEPD) lanza, en aras de certificar esas competencias profesionales, el esquema de certificación de Delegados de Protección de Datos.

Además, los responsables del tratamiento en las empresas han de comunicar en un plazo de diez días de a la AEPD el nombramiento del delegado de protección de datos.

Las funciones del delegado de protección de datos se especifican en el artículo 39 del Reglamento europeo:

"Las funciones del DPD van desde la información del tratamiento de datos a la supervisión del correcto cumplimiento de la normativa"

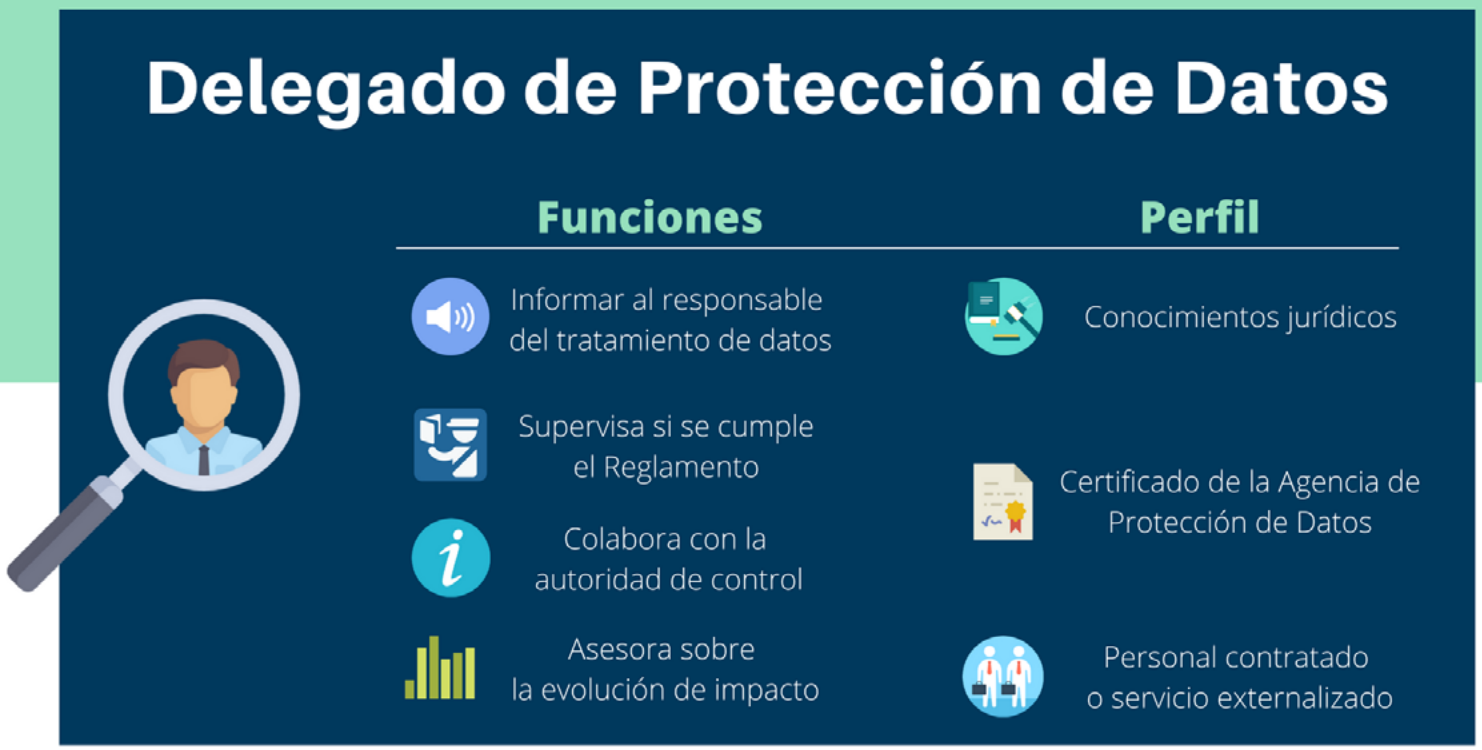
▷ Informar al responsable o a los responsables del tratamiento de datos sus obligaciones en el tratamiento.

▷ Supervisar el correcto cumplimiento de la normativa y las labores derivadas de la misma como la asignación de responsabilidades o la formación del personal.

▷ Asesorar sobre la evaluación de impacto relativa a la protección de datos y cerciorarse de la aplicación conforme a la normativa europea y la propia ley orgánica de protección de datos.

▷ Colaborar con la autoridad de control comunitaria y nacional encargada de velar por la aplicación de la normativa y ser punto de contacto.

En líneas generales, el delegado de Protección de Datos es una figura novedosa certificada para custodiar el procedimiento que siguen las empresas para el control de datos personales de sus clientes.



4.2 ANÁLISIS DE RIESGOS Y EVALUACIÓN DE IMPACTO

Una vez que tienes claro si tienes o no que contar con un DPD, tienes que establecer los posibles riesgos que podrían afectar al tratamiento de los datos recabados para intentar minimizarlos o eliminarlos por completo, evitando consecuencias negativas para ti y/o tu empresa.

Para diagnosticar el nivel de riesgo, piensa en qué amenazas pueden afectar a los datos que manejas teniendo en cuenta la probabilidad y la gravedad de las consecuencias que podrían desarrollarse.

Lo mejor es que lo hagas con cuidado y dejando anotado todo lo que vayas pensando y analizando, así no se escapará ningún detalle para saber si tienes activados los "mecanismos de defensa" adecuados.

Lo ideal es que comiences haciendo un listado donde detalles:

▷ El tipo de datos que manejas.

▷ El contexto en el que se mueven esos datos.

▷ Los elementos más relevantes que intervienen en ellos.

"La AEPD ha creado la herramienta llamada "Facilita RGPD" que te orientará a la hora de hacer una buena Gestión de Riesgos"

Si andas perdido en este proceso, la AEPD ha creadola herramienta llamada "Facilita RGPD" que te orientarán. Esta herramienta genera diversos documentos adaptados para cada empresa, cláusulas informativas que debes incluir en tus formularios de recogida de datos personales, cláusulas contractuales para anexar a los contratos de encargado de tratamiento, el registro de actividades de tratamiento y un anexo con medidas de seguridad orientativas.

Eso sí, ten en cuenta que hay determinadas empresas que no podrán usar esta herramienta. Si la actividad que realizas con los datos recabados implica un alto riesgo para los derechos y libertades de las personas, porque incluye datos de salud o tratamientos masivos de datos, entre otros, estás excluido de su uso.

Y si, ese riesgo es considerado, efectivamente, alto, el RGPD te obliga también a realizar una evaluación de impacto.

La Evaluación de Impacto es un proceso con el que puedes llegar a las conclusiones que te indiquen el camino que has de seguir a partir de ese análisis de riesgos previo. Y esto porque, conocido el escenario, puedes identificar los peligros que pueden atacar a la actividad que desarrollas en el tratamiento de datos más fácilmente y atacarlos antes de que se produzca la infracción.

"Con la Evaluación de Impacto llegarás a las herramientas o mecanismos que te ayudarán a evitar o minimizar el peligro para ti y tu negocio"

Es decir, te permite afrontar y gestionar los peligros antes de que lleguen a materializarse poniendo en marcha las medidas de control más adecuadas para cada caso y evitando sus negativas consecuencias.

Es necesario que introduzcas en esta Evaluación:

▷ Para qué y cómo se usarán los datos objeto de protección.

▷ Evaluación y tratamiento de los potenciales riesgos a asumir.

▷ Elaboración de un plan de acción donde incluir las medidas de control que garantices los derechos y libertades de las personas.

5. SANCIONES PREVISTAS POR EL RGPD

El tratamiento y la comercialización de los datos personales que recaban las empresas se ha convertido en un gran negocio de compraventa de información. De hecho, se ha acuñado el término "Big Data" para, groso modo, aglutinar el amplio volumen de datos (estructurado o no) que manejan los negocios a diario.

Y la importancia de esa enorme agenda (que, obviamente, es más grande cuanto más volumen de negocio tiene una empresa) reside en que, con ella, se puede analizar el comportamiento del mercado. De ese modo, una organización puede decidir cómo y cuándo montar su estrategia de negocio en base a los datos obtenidos de ese Big Data. Para decirlo de un modo cercano, se trata del "santo grial" de nuestros días para cualquier empresa.

Pero no solo las grandes organizaciones recaban datos a diario que hay que saber gestionar y tratar, también autónomos y pymes tratáis a diario con este tipo de información. Lo hacéis cuando abrís fichas con los datos de vuestros clientes, cuando pedís vía telefónica información personal o cuando solicitáis la identificación de un cliente en vuestra página web.

¿Y qué pasará si llega el día 25 de mayo y no te has adecuado a la normativa europea? Pues que podrías enfrentarte a duras sanciones. Un castigo que puede llegar a ser realmente doloso, ya que, según la infracción, las multas administrativas que se contemplan pueden alcanzar cantidades comprendidas entre 10 y 20 millones de euros, o entre el 2 ó el 4% del volumen de negocio anual global.

El régimen sancionador del RGPD es aplicable cuando el tratamiento de los datos de carácter personal que maneja la empresa no se adecua a la norma. En su artículo 83.2 se especifica que las multas se adecuarán a la infracción de que se trate. Y es que, a diferencia de la actual LOPD no existe una tipología establecida de infracciones en leves, graves o muy graves.

"Se aplica el régimen sancionador del RGPD cuando se producen infracciones o incumplimientos de su articulado"

Para establecer la cuantía de las sanciones se atenderá al caso particular y se tendrá debidamente en cuenta:

1º La naturaleza, gravedad y duración de la infracción, estudiando la naturaleza, alcance o propósito de la misma, así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido.

2º La intencionalidad o negligencia en la infracción.

3º Cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados.

4º El grado de responsabilidad del encargado del tratamiento de los datos, habida cuenta de las medidas técnicas u organizativas que hayan aplicado para salvaguardar la información.

5º Toda infracción anterior cometida por el responsable o el encargado del tratamiento.

6º El grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción.

7º Las categorías de los datos de carácter personal afectados por la infracción.

8º La forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida.

9º Que el responsable o el encargado de que se trate, en relación con el mismo asunto, ya haya sido sancionado, entre otras, con una advertencia o apercibimiento al cumplimiento de dichas medidas.

10º La adhesión a códigos de conducta o a mecanismos de certificación aprobados con arreglo al articulado del propio RGPD.

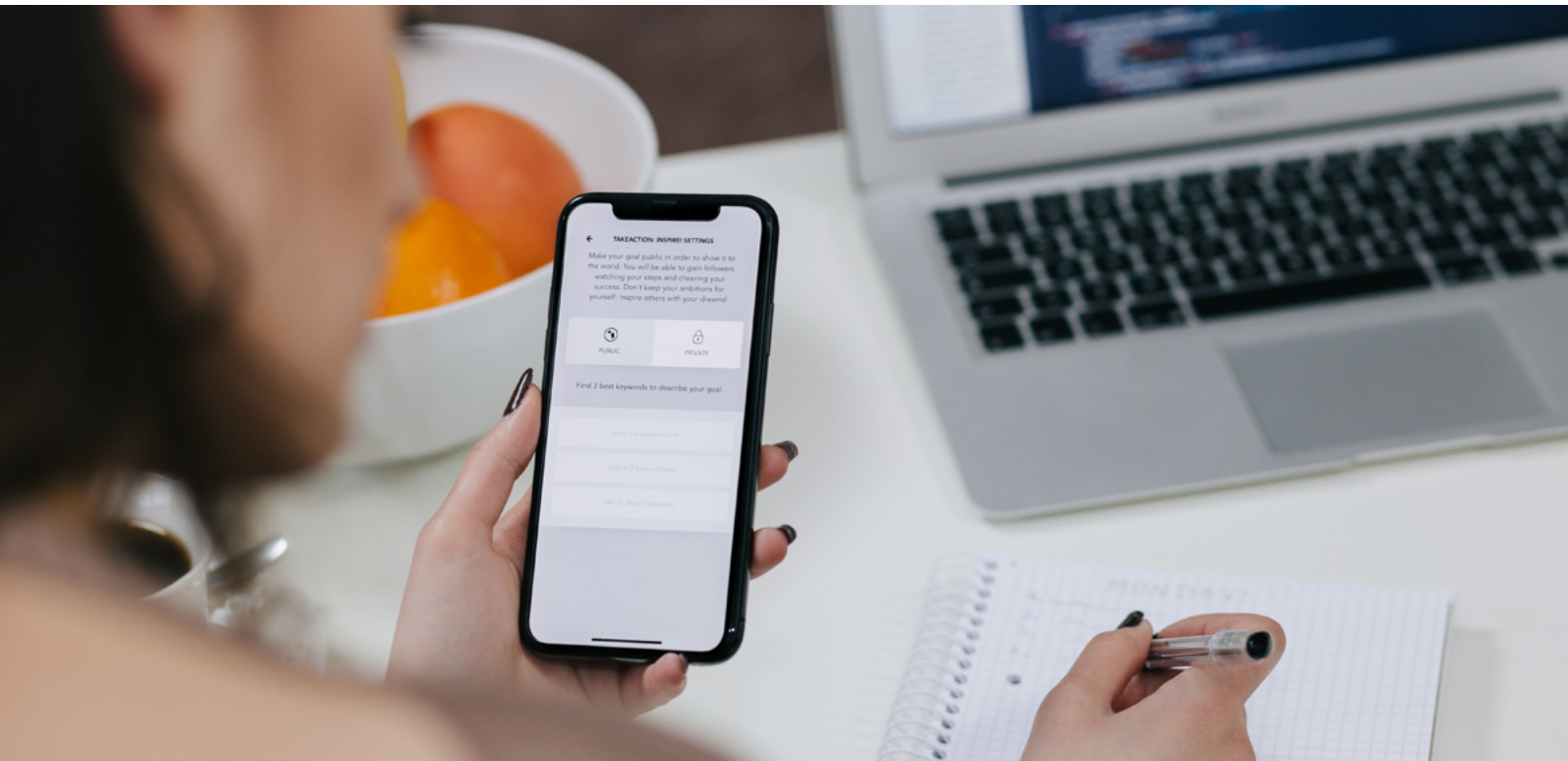
"Entre las novedades del RGPD están la posibilidad de establecer sanciones penales por los países de la UE y el derecho a recibir indemnizaciones por parte de los afectados"

11º Cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

Por poner algún ejemplo, ahora la cesión de datos a un prestador de servicios sin que se haya suscrito previamente el correspondiente acuerdo, con las medidas de seguridad necesarias y establecidas por el RGPD, que actualmente es castigado con hasta 300.000€, pasará a ser multado hasta con 10 millones de euros o un 2% del volumen de negocio total anual del año anterior.

Esta nueva normativa establece, por primera vez, la posibilidad de que los Estados miembro puedan instaurar sanciones penales por el incumplimiento del RGPD, trascendiendo la vía administrativa.

Además, el afectado que haya sufrido daño y/o perjuicio, ya sea material o inmaterial, como consecuencia de una infracción de su articulado, tendrá derecho a recibir una indemnización del encargado o responsable del tratamiento de los datos.



6. DERECHOS PARA PROTEGER TUS DATOS PERSONALES

"Por primera vez se articula el Derecho al Olvido con el que podrás eliminar tu rastro de Internet"

Pero no solo como autónomo o pyme tienes obligaciones con respecto al RGPD, sino que también como persona física posees derechos sobre tus propios datos (información personal), que podrás exigir a otros autónomos, pymes o grandes empresas.

Entre ellos el derecho a conocer para qué se utilizarán tus datos y a solicitar al responsable la portabilidad de estos, aunque sea a otra empresa que le haga la competencia. También vas a poder rectificarlos y oponerte al tratamiento de los mismos e, incluso, solicitar que sean suprimidos de sus bases de datos.

Además, por primera vez se contempla la figura del derecho al olvido con la que podrás eliminar tu rastro o parte de él de Internet. De hecho, Google ya ha implementado una herramienta para que los ciudadanos de la Unión Europea puedan solicitar la eliminación de aquella información propia que consideren censurable.

1º Derecho a conocer

• Para qué utilizan tus datos: quién los tiene, para qué los va a usar, a quién se los va a ceder y quiénes son sus destinatarios.

• Hasta cuándo conservarán tus datos o hasta cuándo van a ser utilizados.

• Que puedes interponer una reclamación ante la Agencia Española de Protección de Datos.

• La existencia de decisiones automatizadas, la elaboración de perfiles y sus consecuencias.

2º Derecho a solicitar al responsable

• La suspensión del tratamiento de tus datos mientras se verifica la exactitud de los mismos o se resuelve nuestro derecho de oposición.

• La conservación de tus datos si su tratamiento es ilícito y nos oponemos a su supresión solicitando la limitación de su uso, o se necesitan para la formulación, ejercicio o defensa de reclamación.

• La portabilidad de tus datos a otros proveedores de servicios en un formato estructurado, técnicamente posible para su portabilidad y cuando los hayan utilizado con tu consentimiento o por existir un contrato.

3º Derecho a rectificar tus datos

- Cuando sean inexactos.
- Cuando estén incompletos.

4º Derecho a suprimir tus datos

- Por el tratamiento ilícito de los mismos.
- Porque desaparezca la finalidad que motivó su recogida o tratamiento.
- Cuando revoques tu consentimiento.
- Cuando te opones a que se traten.

5º Derecho a la oposición al tratamiento de tus datos

- Por motivos personales salvo que quien los trate demuestre un interés legítimo.
- Cuando el objeto del tratamiento sea el marketing directo.