GUÍA PRACTICA
SOBRE protección de datos para pymes y autónomos

CEA
Confederación de
Empresarios de Andalucía

Confederación de Empresarios
de Andalucía

Título: Guía practica sobre protección de datos para PYMES y autónomos.

Proyecto: Fomento de la Cultura Emprendedora 2023.

Financia: Andalucía TRADE.

Coordinación: Confederación de Empresarios de Andalucía (CEA).

Autor/es: Jesús Fernández Acevedo

Depósito Legal: SE 850-2024

01

Presentación de la Guía sobre Protección de Datos.

01 Presentación de la Guía sobre Protección de Datos.

En el actual entorno empresarial, la ciberseguridad y la protección de datos personales se han convertido en elementos cruciales para mantener y mejorar la competitividad de cualquier empresa. La transformación digital, caracterizada por una conectividad sin precedentes, nos ha proporcionado inmediatez en las comunicaciones y una presencia global indudable, ofreciendo oportunidades enormes para el crecimiento y la innovación en los negocios. Sin embargo, esta transformación digital también nos ha traído desafíos significativos, especialmente en lo que respecta a la seguridad de la información y la privacidad de los datos personales.

Para los responsables de empresas, entender y adaptarse a los cambios en las normativas de protección de datos se ha vuelto una prioridad estratégica. Estos cambios no solo son una respuesta a los riesgos emergentes en el ciberespacio, sino también una oportunidad para fortalecer la confianza de los clientes y los socios comerciales en cuanto al tratamiento de los datos que los conciernen. En la escena global, la transformación digital ha cobrado un papel primordial en las estrategias para alcanzar un crecimiento económico que sea a la vez inclusivo y sostenible.

Este fenómeno se ha acelerado notablemente en los últimos años, impulsado por la necesidad de adaptarse a un mundo cada vez más interconectado y tecnológicamente avanzado. Dentro de este contexto, la Unión Europea (UE) ha desempeñado un papel de liderazgo, enfocando sus esfuerzos en la creación de un espacio digital que no solo fomente la innovación y el desarrollo económico, sino que también garantice la equidad, la apertura y la seguridad. El enfoque de la UE hacia la transformación digital va más allá de la mera adopción tecnológica; busca equilibrar el avance tecnológico con la protección de los derechos de los ciudadanos y la promoción de una competencia justa y abierta.

Este compromiso se refleja en una serie de políticas y regulaciones que abarcan desde la protección de datos personales y la ciberseguridad hasta el fomento de una economía digital más inclusiva y accesible para todos. La UE reconoce que un entorno digital sólido y seguro es fundamental para el bienestar económico y social de sus ciudadanos, y trabaja activamente para establecer un marco que apoye un desarrollo digital equilibrado y sostenible en todos sus Estados miembros.

Esta Guía de Protección de Datos está diseñada específicamente para los autónomos y PYMES andaluzas que buscan navegar con éxito en este paisaje regulador en evolución. Aquí encontrará información clave y orientación práctica para implementar estrategias efectivas de protección de datos en su empresa. Desde comprender las normativas vigentes hasta adoptar las mejores prácticas en ciberseguridad, esta guía tiene como objetivo servir de apoyo a los empresarios para que tomen decisiones informadas y responsables, asegurando así la integridad y la seguridad de los datos en un mundo cada vez más digitalizado. La normativa de protección de datos, aunque supuestamente conocida en el mundo empresarial español, puede parecer un laberinto de términos y requisitos, especialmente para las PYMES y autónomos que no suelen disponer de los recursos necesarios para afrontar los retos que requieren las nuevas normativas propias de los derechos de nueva generación como pueden ser las relativas al Compliance como las propias de igualdad, canales de denuncia o protección de datos.

Desde que en Europa se empezó el 25 de mayo de 2018 a poner en marcha el RGPD y España adoptó su propia normativa en diciembre de ese mismo año, la protección de datos ha sido un tema candente durante estos cinco últimos años. Las grandes empresas suelen tener equipos dedicados a este tipo de cumplimiento, pero para los negocios más pequeños como pueden ser los propios de los autónomos y las PYMES, el cumplimiento razonable de estas normativas puede ser un auténtico desafío. Por ello es vital para cualquier negocio en España el poder entender estas reglas, no solo para evitar multas de cualquier índole, sino también para garantizar el cuidado de la información personal relativa a sus clientes, su personal o sus contactos con el fin de no dañar ni menoscabar su reputación y perder clientes por la desconfianza que un desastre de estas características pudiera casuar.

El 25 de mayo de 2018 representó un hito significativo en la evolución de la regulación sobre protección de datos en Europa y, por ende, en España. La implementación del Reglamento UE 2016/679, más conocido como el Reglamento General de Protección de Datos (RGPD), marcó la superación de la normativa anterior, la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (antigua LOPD), que había regido en España durante casi veinte años.

Esta transición normativa europea fue acompañada en España por la publicación de la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), publicada en diciembre de 2018. La LOPDGDD no solo consolida y complementa el RGPD en el ámbito nacional, sino que también introduce elementos específicos adaptados al contexto español, enfatizando la protección de datos personales y la garantía de derechos digitales.

La LOPDGDD amplía el alcance europeo de la protección de datos personales, abarcando aspectos como algunos de los derechos digitales de la ciudadanía española, incluyendo el derecho a la desconexión digital en el ámbito laboral, la protección de menores en internet, y determinadas garantías en el uso de videovigilancia y geolocalización en el contexto laboral.

En resumen, la entrada en vigor del RGPD y la posterior implementación de la LOPDGDD en España han transformado el panorama de la protección de datos personales, ofreciendo un marco más robusto y detallado que responde a los desafíos de la era digital y fortalece los derechos de privacidad de los ciudadanos. Este cambio no solo representa una adaptación a las nuevas normativas europeas, sino también un avance significativo en la forma en que deben de tratar y proteger los datos personales.

Por ello, el Reglamento General de Protección de Datos (RGPD) de la Unión Europea se consolida como una normativa de amplio espectro que afecta a empresas de todos los sectores y tamaños pertenecientes a un entorno en el que la interacción entre los usuarios y las empresas está cada vez más condicionada por la tecnología, ya sea a través del uso de las redes sociales, las aplicaciones móviles o las tiendas en línea. En estas plataformas, los usuarios están obligados a compartir una gran cantidad de información personal, que puede ir desde su correo electrónico hasta sus preferencias o hábitos de compra. Esta información se ha convertido en un activo fundamental para el éxito y la estrategia de crecimiento de las empresas, al permitirles personalizar sus servicios y mejorar la experiencia del cliente.

Sin embargo, este intercambio de datos no está exento de preocupaciones. Los usuarios son cada vez más conscientes del valor de su intimidad y están menos dispuestos a tolerar prácticas que consideren intrusivas o irrespetuosas con sus datos personales, incluyendo, el rechazo a la publicidad invasiva, la geolocalización no deseada, la discriminación basada en decisiones automatizas de datos o las consecuencias de fugas masivas de información que pueden causar perjuicios morales y económicos como pudieran ser los riesgos de robo de identidad o de datos bancarios.

La normativa aborda estas preocupaciones estableciendo normas estrictas sobre el tratamiento de datos personales, otorgando a los usuarios un mayor control sobre su información. Para ello, las empresas deben asegurarse que el tratamiento de datos personales sea transparente, informado y conforme a la ley. Esto no solo protege la privacidad de los usuarios, sino que también ayuda a las empresas

a ganar y mantener la confianza de sus clientes, un factor crítico en el éxito empresarial. En resumen, el RGPD representa un equilibrio entre la necesidad de las empresas de utilizar datos personales para sus operaciones y la creciente demanda de los usuarios por la protección de su privacidad.

Para atender a estos cambios en esta guía responderemos a las principales preguntas al respecto:

- ¿A quién afecta la normativa?
- ¿Quién debe supervisar el cumplimiento?
- ¿Qué se entiende por datos personales?
- ¿Qué nuevos derechos son reconocidos a la ciudadanía?
- ¿Qué es un Delegado/a de Protección de Datos o DPD?
- ¿Tengo obligación de nombrar a un DPD?
- ¿Cómo debo de informar a partir de ahora?
- ¿Qué tipo de contrato en materia de protección de datos debo firmar con mis proveedores en materia de protección de datos?
- ¿Cuáles son las prácticas recomendables para garantizar el cumplimiento activo?

La presente guía tiene como función entender la necesidad del cumplimiento efectivo respecto la protección de datos por parte de cualquier tipo de entidad o persona jurídica a la par de facilitar a todas las empresas andaluzas una guía simple y fácil a la que poder acudir para adaptar su realidad profesional tanto al Reglamento Europeo de protección de Datos como a Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

El incumplimiento de la normativa de protección de datos supone el riesgo de:

1º) Sanciones económicas que pueden llegar a multas de:

a) **Hasta 10 millones de euros o el 2% del volumen de facturación anual de la empresa en el caso de infracciones graves.**

b) **Hasta 20 millones de euros o el 4% del volumen de facturación anual de la empresa en el caso de las sanciones más graves.**

2º) Pérdida de confianza y reputación ya que en la actualidad, tanto la privacidad y como la protección de datos, han adquirido tal relevancia que los consumidores y usuarios están dispuestos a reemplazar y abandonar aquellos productos y servicios que no garanticen un cumplimiento razonable con la normativa, rechazando prácticas intrusivas como la publicidad agresiva, el rastreo de localización no consentido, la discriminación basada en perfilados o las brechas de seguridad que puedan resultar fugas masivas de información personal que puedan causar daños y perjuicios a los afectados o en delitos de suplantación de identidad; por todo ello cumplir con la normativa de protección de datos ya no es sólo una obligación, sino que se define incondicionalmente como una ventaja competitiva en el mercado con respecto a la competencia.

3º) El uso ético y legítimo de la analítica de datos, supone una ventaja competitiva para conocer mejor a los clientes, mejorar la experiencia de usuario y por tanto fidelizar y aumentar la facturación de nuestra empresa con técnicas como el Data Mining, el Big Data, el análisis de perfiles, o simplemente el uso de redes sociales para que una empresa pueda ser más competitiva en el mercado.

Por todo ello, es imperativo para cualquier tipo de organización empresarial el revisar y auditar tanto sus políticas de protección de datos como sus sistemas de gestión de seguridad de la información (SGSI) y con la presente Guía se pretende configurar una pequeña hoja de ruta que sirva como revisión y, en el caso de nuevas empresas o incluso de startups, como un punto de partida en el que poder apoyarse.

02

El falso cumplimiento en materia de protección de datos y cómo evitar prácticas engañosas y fraudulentas.

02

El falso cumplimiento en materia de protección de datos y cómo evitar prácticas engañosas y fraudulentas.

Desde antes de la entrada en vigor del RGPD, han sido muy habituales las prácticas fraudulentas para comercializar servicios de protección de datos. Así por ejemplo, la conocida como “LOPD Coste 0” fue una estrategia comercial que se utilizó en España para promocionar servicios de adaptación a la Ley Orgánica de Protección de Datos (LOPD) mediante la adaptación a la normativa supuestamente sin coste alguno o “bonificados” por subvenciones por fondos a la formación. Sin embargo, este término era engañoso y podría dar lugar a malentendidos importantes ya que en realidad los proveedores de servicios que promocionaban la “LOPD Coste 0” a menudo incluían costes ocultos o vinculaban este servicio “gratuito” a la contratación de otros servicios de pago. Por ejemplo, una empresa podía ofrecer la adaptación a la LOPD sin coste directo, pero a cambio exigía la firma de un contrato de servicios de asesoramiento o mantenimiento a largo plazo, que sí tenía un coste.

Este tipo de prácticas, además de ser potencialmente engañosas, a menudo resultaban en un servicio de baja calidad o en una adaptación incompleta o inadecuada a la normativa de protección de datos. Esto podía dejar a las empresas en riesgo de incumplir con la legislación de protección de datos, lo que podría acarrear sanciones

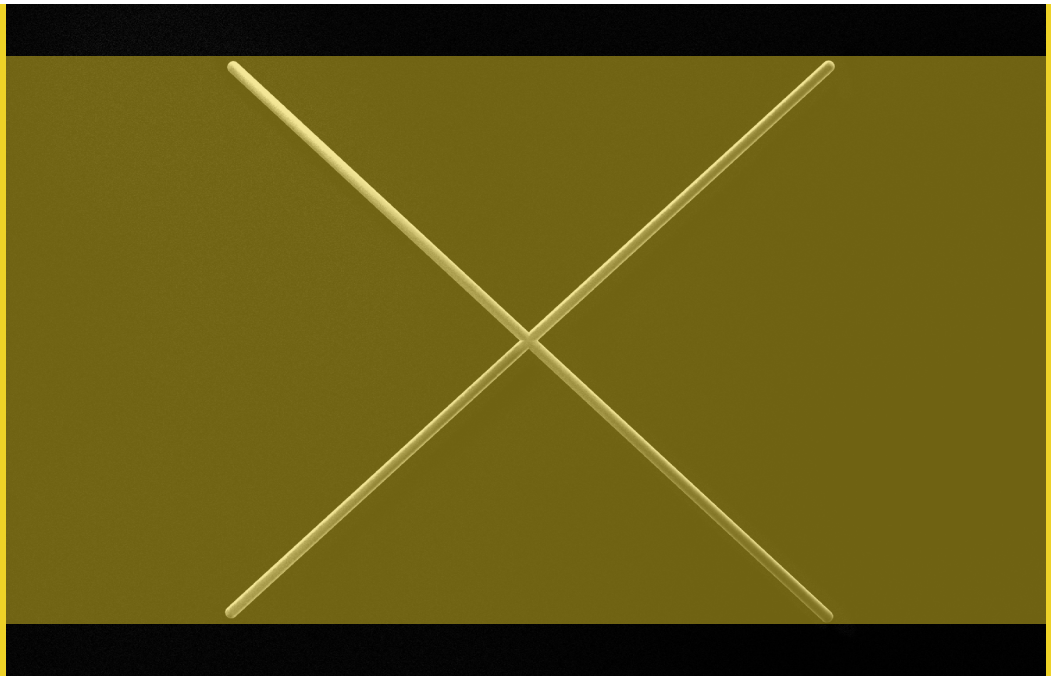
significativas como las que se han señalado anteriormente. Es crucial que las empresas comprendan que la adaptación a la normativa de protección de datos, ya sea la LOPD en su momento o el actual RGPD, requiere una inversión adecuada en recursos y una especialización para garantizar una implementación completa y conforme a la ley. La protección de datos personales es un aspecto crítico que va más allá de una simple formalidad administrativa, y debe ser tratada con la seriedad y el profesionalismo que merece. Por ello las empresas han de tener en cuenta que el cumplimiento con la normativa de protección de datos requiere:

- Un cumplimiento activo, así como revisiones, auditorías y actualizaciones constantes, por lo que el simple pago de una cuota periódica a un proveedor de servicios no garantiza un adecuado cumplimiento a la normativa de protección de datos.

- El uso de bonificaciones destinadas a la formación del personal de la empresa para cubrir una obligación legal de la empresa puede suponer el enfrentarse a multas de más de 180.000 euros por fraude a la Seguridad Social, así como de la Agencia Tributaria en su caso por fraude en el pago del IVA.

- No existen certificados de cumplimiento de la normativa de protección de datos a organizaciones por entidades privadas. Distinto es que determinados clientes que se configuren como responsables de tratamiento de datos personales exijan determinadas garantías a los proveedores con los que hayan firmado un contrato de encargado de tratamiento. Por ello se recomienda no confiar ciegamente o revisar certificados de cumplimiento que aseguren que la empresa cumple con todas y cada una de las obligaciones en materia de protección de datos ya que no tienen ninguna validez externa.

- Desconfíe de ciertas prácticas agresivas en donde determinadas suplantan a la Agencia Española de Protección de Datos y prometen evitar una inspección de dicha autoridad únicamente si contrata a determinados proveedores para adecuarse adecuación a la normativa.



En cualquier caso, la Agencia Española de Protección de Datos advierte sobre el riesgo de las prácticas fraudulentas y por ello es conveniente informarse por los medios oficiales de la autoridad de control o equivalente[1]. La Agencia recuerda la conveniencia de que las pymes y autónomos que quieran o tengan que contratar servicios de adecuación a la normativa de protección de datos se aseguren de que los servicios que se les ofrecen no incurren en las prácticas mencionadas con anterioridad.

1 Puede consultar la nota de prensa que la AEPD publicó al respecto en: https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-aepd-alerta-pymes-y-autonomos-de-los-riesgos-de-contratar

03

Cuestiones y aspectos generales en protección de datos personales.

03 Cuestiones y aspectos generales en protección de datos personales.

3.1 ¿Qué es un dato de carácter personal?

El art. 4.1 del RGPD considera dato personal:

> «toda información relativa a una persona física identificada o identificable».

Se considera persona identificable la persona que puede ser identificada directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de esta persona.

Las empresas pueden tratar a modo de ejemplo datos personales de sus clientes (datos bancarios o de facturación), de su personal (datos de nómina o de control de presencia), de sus contactos (datos de contacto como correo electrónico o redes sociales) o de sus visitantes (por videovigilancia o control de acceso).

En consecuencia, la normativa de protección de datos no aplica cuando afecta a la información relativa a personas jurídicas (como puede ocurrir con

proveedores que sean personas jurídicas) o información anónima, es decir, cuando no se puede relacionar con una persona física.

Por tanto, dato de carácter personal es cualquier tipo de información relacionada con una persona identificada o identificable, el cual tendrá la consideración de titular de los datos, pero que según las circunstancias podrá ser afectado o interesado. Es decir, un nombre, un apellido, un número de teléfono, una firma, una foto o una imagen de un individuo, son considerados datos identificativos de las personas; el estado civil, la edad, las aficiones o la pertenencia a asociaciones de una persona son datos referidos a características personales o de circunstancias sociales los datos académicos y profesionales; los datos de profesión, puestos de trabajo, historial del empleado o el CV de una persona son datos académicos o relacionados con el empleo, así como un número de cuenta corriente es información comercial, económica, financiera y de seguros. Existen además datos especialmente sensibles como pueden ser la ideología, religión, creencias, salud o vida sexual de una persona, que merecen una protección reforzada o más delicada.

Ejemplos en donde las empresas tratan información personal que hacen que una persona sea identificada o identificable:

- Nombre y apellidos para identificar a un usuario o cliente.
- Foto de un trabajador para tarjeta identificativa de control laboral.
- DNI que se solicita en un hotel para registro de huéspedes.
- Dirección o domicilio donde enviar un pedido a un cliente.
- Número de teléfono para llamar a un contacto o enviarle un WhatsApp.
- Mail para hacer una consulta a una entidad.

- CV para un proceso de selección de personal.
- Historia Médica relativa a un paciente de un hospital.
- Fotografías de un evento presencial organizado por la empresa en donde aparecen personas físicas.
- Número de Cuenta Corriente o tarjeta bancaria de un cliente.
- Datos de la Nómina de un trabajador.

Igualmente, el RGPD amplía la concepción anterior respecto a lo que se considerará persona física identificable cualquier persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona", como pueda ser el avatar en una red social, identificadores de sesión en forma de "cookies" u otros identificadores, como etiquetas de radiofrecuencia.

Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser usados para elaborar perfiles de las personas físicas e identificarlas, así como aplicaciones móviles que geolocalizan al usuario del dispositivo electrónico o simplemente el nombre de usuario o nickname de una persona en una red social.

Dependiendo del tipo de datos que se traten, éstos pueden ser, por ejemplo, identificativos (nombre, apellidos, número del documento nacional de identidad), referidos a tu situación laboral, financiera o de salud.

También existen las categorías especiales de datos como los datos de salud o los que pueden revelar el origen étnico o racial de una persona, o tal vez sus opiniones políticas, convicciones religiosas o fisiológicas,

o afiliación sindical, así como aquellos que revelan datos genéticos, biométricos o los relativos a la vida sexual u orientación sexual.

3.2 ¿De quiénes son los datos de carácter personal?

Los datos son de la persona física titular de los mismos, como los clientes, proveedores, usuarios, contactos o personal de administración y servicios. Son los afectados o interesados en su caso por el tratamiento de sus datos.

3.3 ¿Qué entidades están obligadas a cumplir con el RGPD?

Deberán cumplir con las obligaciones que impone el RGPD toda organización pública o privada, independientemente de que estén establecidos o no en la Unión Europea, si tratan datos de carácter personal de ciudadanos europeos o dirigen sus productos y servicios a interesados que se encuentren en la Unión Europea. Es por ello que las entidades andaluzas están obligadas al cumplimiento más estricto del RGPD, entendiendo como tal cualquier empresa, PYME, autónomo o emprendedor que trate datos de personas físicas como clientes, empleados, proveedores, candidatos o contactos de cualquier índole.

En ningún caso será de aplicación el RGPD si el tratamiento correspondiente se realiza respecto a datos de personas fallecidas, o si realiza el tratamiento una persona física en su ámbito estrictamente personal o doméstico, sin relación con ninguna actividad profesional o comercial alguno, como pueda ser una cuenta en redes sociales de un individuo si es para un uso estrictamente privado o si una persona utiliza una aplicación de mensajería instantánea para comunicarse con su familia o amigos, o dispone de una cámara de videovigilancia en su domicilio particular, es decir, si realiza tratamientos de datos personales para un ámbito estrictamente privado o doméstico (supuestos conocidos como “exención doméstica”); si no exceden del ámbito estrictamente doméstico (como publicar una fotografía de una persona menor de edad en una

red social de forma disponible para cualquier usuario de esa red social o enfoca las cámaras de videovigilancia al exterior del domicilio pudiendo grabar a cualquier transeúnte o vecino) no pueden ser multados por la autoridad de control en materia de protección de datos.

Las PYMES, autónomos y emprendedores actúan como responsables o encargados de tratamiento en el desarrollo de la mayoría de sus actividades de tratamiento, y por ello, en consecuencia, se verán obligadas a respetar los principios y obligaciones específicas que el RGPD contempla para el sector privado. Por ello se exige a las PYMES, autónomos o emprendedores que sea responsables del tratamiento de diversos datos personales relacionados con personas físicas identificadas e identificables, esfuerzos más evidentes y evaluables, para cumplir los nuevos requisitos en materia de protección de datos.

Los responsables del tratamiento de datos del sector privado que incurran en incumplimientos pueden ser sancionados con hasta 20 millones de euros o con una sanción equivalente hasta el 4 % de sus ingresos globales, implicando un sistema sancionador más justo y equitativo que el anterior régimen sancionador al poder sancionar la autoridad de control competente de Protección de Datos según la facturación de la empresa en cuestión, siempre y cuando no respete los derechos de la ciudadanía.

Ejemplo

No se va a imponer la misma sanción a una pequeña tienda que dispone de una cámara de videovigilancia orientada a la vía pública, que a un gran centro comercial que dispone de un número considerable de cámaras que captan la imagen de una calle peatonal muy concurrida, en primer lugar, por la diferenciación en cuanto al número de afectados y en segundo lugar por la diferencia de facturación entre ambas entidades.

3.4 ¿Las personas jurídicas están protegidas por la protección de datos?

Las personas jurídicas no están protegidas por la normativa de protección de datos, sino que están obligadas a cumplir con la misma para proteger la información que tratan concerniente a personas físicas durante el desempeño de su actividad profesional.

Dichas personas jurídicas que realicen una oferta de bienes o servicios ya sean empresas, autónomos o emprendedores, si tienen su residencia o domicilio social en la Unión Europea están obligados a cumplir con el RGPD. En caso de que tales personas jurídicas no residan en la Unión Europea, si destinan su oferta de bienes o servicios a ciudadanos europeos o personas que se encuentren en la Unión Europea, estarán igualmente obligados a cumplir con el RGPD.

3.5 ¿Cuáles son los datos especialmente protegidos en el RGPD?

Se suelen relacionar los datos especialmente protegidos únicamente con aquellos datos relacionados con la salud, y, sin embargo, los datos de salud forman parte de la categoría de "datos especialmente protegidos", junto con aquellos:

- Que revelen ideología, afiliación sindical, religión y creencias.
- Que hagan referencia al origen racial, o a la vida sexual.
- Que se refieran a la comisión de infracciones penales o administrativas.

De igual forma, el RGPD amplía la definición de "dato de salud", "datos genéticos" y "datos biométricos" de la siguiente forma:

- **"Datos relativos a la salud"**: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

- **“Datos genéticos”**: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona”. Los datos genéticos ya tenían la consideración de datos especialmente protegidos en el marco de la Directiva 95/46, únicamente si estaban relacionados con la salud, algo que ya no es así con el RGPD, el cual les otorga sustantividad propia en casos como pueden ser los de filiación.

- **“Datos biométricos”**: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos. En cualquier caso únicamente tendrán la condición de datos sensibles cuando sean utilizados para identificar unívocamente a una persona, y no cuando puedan aparecer de forma accesoria en un tratamiento como pueda ser en el caso de una fotografía de un individuo, en donde aunque se contengan los datos biométricos del afectado, los mismos no serán utilizados como regla general salvo que se utilice para individualizar o identificar a alguien dentro de un colectivo más amplio, como pudieran ser los sistemas de reconocimiento facial en redes sociales.

3.6 ¿Cuál es la autoridad que sanciona a las entidades responsables de tratar datos personales en caso de incumplimiento?

El Reglamento europeo señala que “cada Estado miembro de la Unión establecerá que sea responsabilidad de una o varias autoridades públicas independientes, supervisar la aplicación del presente Reglamento, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales” en la Unión Europea”.

Respecto a España, la autoridad de control es la Agencia Española de Protección de Datos AEPD). La propia Agencia dispone de una web oficial (www.aepd.es) en donde publica guías y recursos de forma periódica al tratarse de la autoridad de control independiente que vela por el cumplimiento de la normativa sobre protección de datos, garantizando con todo ello la tutela el derecho fundamental a la protección de datos de carácter personal.

Cabe señalar que la AEPD tiene personalidad jurídica propia y plena capacidad pública y privada. Ejerce sus funciones por medio de su Director/a, que debe actuar, igualmente, con plena independencia. Es evidente pues, que la AEPD actúa con total independencia de las Administraciones Públicas en el ejercicio de sus funciones y se relaciona con el Gobierno a través del Ministerio de Justicia.

En cuanto a sus funciones, el objetivo principal de esta autoridad de control es encargarse de velar por el cumplimiento de la legislación sobre Protección de Datos y controlar su aplicación en el territorio nacional, en concreto en lo relativo a los derechos que asisten a los ciudadanos, prestando especial atención al derecho de información y a los conocidos como derechos de acceso, rectificación, supresión (anterior derecho de cancelación) y oposición.

Es su cometido atender las peticiones y reclamaciones formuladas por los afectados o interesados, sin perjuicio de las vías de recurso procedentes; para ello, informa a las personas sobre sus derechos y promueve campañas de difusión a través de los medios. Igualmente, se encarga de proporcionar información a las personas sobre sus derechos en materia de tratamiento de los datos de carácter personal.

Asimismo, tutela el cumplimiento de los derechos y garantías de los usuarios en el ámbito de las comunicaciones electrónicas, incluyendo el envío de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico o medios de comunicación electrónica equivalente, en los términos que establece la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico.

La propia LOPD recoge que una de las funciones más importantes de la Agencia es su potestad de inspección con el fin de comprobar la legalidad de los tratamientos. Para ello, la Ley habilita a la AEPD para inspeccionar los tratamientos a los que hace referencia la LOPD, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos, pudiendo solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que estén depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a instalaciones donde se encuentren ubicados estableciendo que los funcionarios que ejerzan la inspección tendrán la consideración de autoridad pública en el desempeño de sus cometidos, y estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

3.7 ¿Existe en Andalucía una autoridad competente en protección de datos?

Las agencias autonómicas de protección de datos tienen la misma misión y finalidad que la AEPD: garantizar y proteger los derechos fundamentales de las personas físicas respecto al honor e intimidad familiar y personal, en lo relativo al tratamiento de sus datos personales aunque sus competencias versan, exclusivamente, sobre los tratamientos de titularidad pública creados o gestionados por la Comunidad Autónoma a la que pertenecen, entes que integran la Administración Local de su ámbito territorial, Universidades públicas y corporaciones de derecho público.

En Andalucía existe el *Consejo de Transparencia y Protección de Datos de Andalucía (CTPDA)*, creado por el artículo 43 de la Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía, y que se configura la autoridad independiente de control en materia de transparencia y protección de datos en la Comunidad Autónoma de Andalucía.

Tiene la consideración de Administración Institucional, lo que significa que posee personalidad jurídica propia y plena autonomía e independencia en el ejercicio de sus funciones: su función es la de velar por el cumplimiento de la normativa de transparencia pública, tanto en lo que se refiere a publicidad activa como a la defensa y salvaguarda del derecho de acceso a la información pública así como velar por el cumplimiento de la normativa de protección de datos en al ámbito de sus competencias.

En la Disposición transitoria tercera del Decreto 434/2015, de 29 de septiembre, por el que se aprueban los Estatutos del Consejo de Transparencia y Protección de Datos de Andalucía se señala en el primer apartado de esta Disposición transitoria tercera:

> *"El Consejo asumirá las funciones en materia de protección de datos que tiene atribuidas de conformidad con lo que establezcan las disposiciones necesarias para su asunción y ejercicio por la Comunidad Autónoma. En tanto se lleve a cabo la aprobación y ejecución de dichas disposiciones continuarán siendo ejercidas por la Agencia Española de Protección de Datos".*

Pueden consultarse las publicaciones y la actividad del Consejo de Transparencia y Protección de Datos de Andalucía en: http://www.ctpdandalucia.es/es

3.8 ¿Tienen las PYMES y autónomos que seguir notificando sus ficheros a la Agencia Española de Protección de Datos?

Con la anterior normativa de protección de datos al RGPD se establecía la obligación de inscribir los ficheros que contenían datos de carácter personal, todo ello para conseguir un sistema que ayudase a percibir el grado de adecuación de la normativa por parte de las empresas además de servir al ciudadano como un repositorio en donde pudiera recabar información sobre las entidades que realizaban un tratamiento de sus

datos; sin embargo, el propio RGPD ha reconocido en su considerando 89, el fracaso de dicha obligación, ya que no sólo no contribuyó a mejorar el cumplimiento en materia de protección de datos personales, sino que incentivó a cumplir únicamente con esta obligación meramente burocrática o formal, preocupándose en mayor medida las empresas y especialmente las PYMES, en disponer de sus ficheros debidamente registrados en vez de respetar y cumplir con el resto de obligaciones inherentes a la LOPD.

Es por ello que, a partir del 25 de mayo de 2018, desapareció la obligación de inscribir ficheros en el Registro de Ficheros de la AEPD, u registro de la autoridad autonómica competente. Es decir, con el RGPD desaparece la obligación de inscribir ficheros en esta AEPD. Esta obligación general de notificación, al no responder al cumplimiento efectivo, se ha eliminado desde Mayo de 2018, y se ha sustituido por otra serie de obligaciones más eficaces como puede ser el Registro de Actividades de Tratamientos que exige un compromiso interno además de una revisión constante por cada organización.

3.9 ¿Cuáles son los conceptos básicos en materia de protección de datos necesarios para poder comprender esta guía?

Los conceptos más relevantes son:

3.9.1 Tratamiento de datos Un tratamiento es cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no. El aspecto más importante que define a un tratamiento es su finalidad como pueda ser la gestión de clientes, la gestión de recursos humanos o el control de la videovigilancia.

Ejemplos de tratamientos más frecuentes:

a. Gestión de Clientes.

b. Gestión de Redes Sociales.

c. Gestión de Recursos Humanos.

d. Selección de Personal.

e. Videovigilancia.

f. Gestión de Historias Clínicas.

g. Control horario y/o laboral.

3.9.2 Afectado o interesado persona física titular de los datos que sean objeto del tratamiento. Por tanto, una persona jurídica no es la titular de los datos que trata, desde un punto de vista conceptual, sino que será responsable o encargado de los tratamientos de datos.

Ejemplos:

- Clientes (Gestión de Clientes).
- Contactos (Gestión de Redes Sociales).
- Personas trabajadoras (Gestión de Recursos Humanos).
- Personas candidatas a un puesto de trabajo (Selección de Personal).
- Personas videovigiladas (Videovigilancia).
- Pacientes (Gestión de Historias Clínicas).
- Usuarios (Gestión de una APP).

3.9.3 Responsable del tratamiento Un responsable del tratamiento es, la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o juntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

Ejemplos de responsables de tratamientos:

1. Si una empresa decide crear un comercio electrónico, tratará los datos personales de sus clientes para los fines de cumplimiento y desarrollo de la relación contractual o la venta online correspondiente, siendo dicha empresa el responsable del tratamiento de datos de sus CLIENTES.

2. Una startup lanza una APP, dicha startup responsable del tratamiento de los datos que registren sus USUARIOS.

3. Una asociación será responsable de tratamiento de datos de sus ASOCIADOS.

4. Una academia será responsable de tratamiento de los datos de los ALUMNOS del centro.

5. Un centro médico será el responsable de tratamiento de sus PACIENTES.

6. Si un autónomo o una empresa dispone de personal laboral, será responsable del tratamiento de los datos de nómina del PERSONAL.

7. En caso de abrirse un proceso de selección de personal, será responsable del tratamiento de los datos de las personas candidatas que envíen su CV al departamento de Recursos Humanos para SELECCIÓN DE PERSONAL

.

8. Si una empresa instala cámaras de video para vigilancia y control de las instalaciones será responsable del tratamiento VIDEOVIGILANCIA.

3.9.4 Encargado del tratamiento es la persona física o jurídica, pública o privada, u órgano administrativo que, solo o junto con otros, trate datos personales por cuenta del responsable del tratamiento, como consecuencia de la existencia de una relación jurídica que le vincula con éste y delimita el ámbito de su actuación para la prestación de un servicio. También, pueden ser encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

Ejemplos de proveedores que actúan como encargados de tratamiento según la normativa de protección de datos:

a. Asesoría laboral que confecciona las nóminas de los trabajadores.

b. Asesoría contable que gestiona la contabilidad de otra empresa.

c. Empresa de seguridad que accede a las cámaras de videovigilancia.

d. Servicio de Cloud que alberga las copias de seguridad de los datos de otras entidades.

e. Empresa de destrucción documental para eliminar tanto el papel como los soportes digitales que tengan datos personales.

3.9.5 Responsable de seguridad persona o personas a las que el responsable del fichero según la LOPD 15/1999 asigna

formalmente la función de coordinar y controlar las medidas de seguridad aplicables. Esta figura ya no existe en el RGPD como tal, y se ha sustituido por la figura del Delegado de Protección de Datos en determinadas entidades, ya que requiere mayor formación y capacitación para desempeñar sus funciones en relación con la antigua figura del Responsable de Seguridad.

3.9.6 Delegado de protección de datos o DPD Es una figura nueva que deberá realizar sus funciones en la empresa con total imparcialidad e independencia. Será designado por el responsable y el encargado del tratamiento cuando este sea obligatorio por ley o como medida de prevención de riesgos en materia de privacidad. También se le conoce por su denominación anglosajona como DPD (Data Protection Officer).

3.9.7 Cesión o comunicación de datos tratamiento de datos que supone su revelación a una persona distinta del interesado.

3.9.8 Seudonimización tratamiento de datos personales que no permite identificar a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable. La aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos según establece el RGPD.

3.9.9 Limitación del tratamiento El nuevo derecho a la limitación del tratamiento consiste en que el interesado pueda

pedir al responsable del tratamiento que utilice medios técnicos para que los datos personales no sean objeto de operaciones de un tratamiento ulterior determinado ni puedan modificarse.

3.9.10 Destinatario La persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento.

3.9.11 Tercero La persona física o jurídica, autoridad pública, servicio u otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

3.9.12 Brecha de seguridad de los datos personales Toda brecha de seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados por terceros a dichos datos. Tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales debe, sin dilación indebida y, de ser posible, dentro de las 72 horas posteriores a que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar,

atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas.

3.9.13 Transferencia internacional de datos tratamiento de datos que supone una transmisión de estos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

3.9.14 Exportador de datos personales la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el RGPD, una transferencia de datos de carácter personal a un país tercero.

3.9.15 Importador de datos personales la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

3.9.16 Autoridad de control La autoridad independiente establecida por un Estado miembro que se encarga de desarrollar el marco en el que los Estados miembros han de regular la constitución, organización y funcionamiento de las autoridades de control, configurándose en España como autoridad de control la Agencia Española de Protección de Datos.

04

Principios relativos a los tratamientos de datos personales en Pymes y Autónomos

04 Principios relativos a los tratamientos de datos personales en Pymes y Autónomos

En la era digital actual, la protección de los datos personales se ha convertido en una cuestión de suma importancia y el RGPD establece un marco legal robusto para garantizar que la privacidad y los derechos de las personas sean respetados en el tratamiento de sus datos personales. Cabe destacar que los principios rectores del RGPD no son meras recomendaciones, sino fundamentos legales que todas las empresas y organizaciones empresariales que manejan datos personales dentro de la UE deben cumplir.

Estos principios no solo proporcionan hoja de ruta clara sobre cómo deben ser tratados los datos personales, sino que también representan un compromiso con la transparencia, la seguridad y la responsabilidad. El cumplimiento de estos principios es esencial no solo para evitar sanciones legales, sino también para fomentar la confianza de los consumidores y mantener la integridad de las operaciones empresariales.

A continuación, exploraremos cada uno de estos principios en detalle, desglosando su significado y su aplicación práctica en el ámbito empresarial con el objetivo de proporcionar una comprensión completa de qué implican estos principios y cómo

pueden las empresas implementar medidas efectivas para garantizar su cumplimiento, protegiendo así tanto a las personas como a la propia organización.

4.1 Principio de Responsabilidad Proactiva o Cumplimiento Proactivo (Accountability): El eje vertebrador de la filosofía de la nueva norma se recoge en el artículo 5 del RGPD que consolida los principios relativos al tratamiento, configurándose el principio de "Responsabilidad proactiva" "Accountability" que viene regulado en al art. 5.2 y 24 así como en el considerando 74 del RGPD, como el más novedoso en cuanto a la regulación anterior. Dicha novedad del Reglamento Europeo de Protección de datos señala que el principio de responsabilidad activa implica que las entidades responsables de tratamientos de datos no tienen que esperar a cumplir con lo mínimo exigible por la normativa para no ser sancionadas: están obligadas a ir más allá y crear una cultura de protección de datos que garantice las buenas prácticas de todo el personal con el objetivo de demostrar que existe una política de tratamiento de datos adecuada a la normativa.

El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo ("responsabilidad proactiva").

Y así continúa el artículo 24 RGPD en cuanto a la Responsabilidad del responsable del tratamiento, señalando que *"teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas*, ***el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme***

con el presente Reglamento. ***Dichas medidas se revisarán y actualizarán cuando sea necesario***.

La norma europea entiende que actuar únicamente cuando ya se haya producido una infracción es absolutamente insuficiente como estrategia, dado que esa infracción puede causar daños a los interesados que pueden ser muy difíciles de compensar o reparar.

Existe pues un cambio muy radical en cuanto al enfoque con respecto a la Directiva 95/46/CE anterior al RGPD, ya que se busca la anticipación a la infracción o lesión de derechos mediante el cumplimiento con antelación para evitar así la lesión o infracción del derecho o libertad del interesado.

Por tanto, es un cambio de enfoque con consecuencias reales, ya que el hecho de la falta de adopción de alguna de las medidas u obligaciones establecidas por el RGPD puede originar la imposición de una sanción al responsable o encargado de tratamiento sin que previamente exista una lesión de los derechos y libertades del afectado o interesado.

Hay que tener en cuenta que las medidas ya no dependen de las directrices que se recojan en la norma, sino que ahora cada entidad tiene que evaluar cuáles son sus riesgos con el fin de poder decidir cuáles son las medidas que más se ajustan a su realidad, desapareciendo por ello los niveles bajo, medio y alto, y reforzando la posición de un delegado de protección de datos que realice las recomendaciones necesarias en las entidades que realicen tratamientos de determinados riesgos así como las evaluaciones de impacto en la privacidad, o el modo en que se apliquen, dependiendo de factores tales como el tipo de tratamiento (no es lo mismo que se traten datos sensibles que datos de contacto, o que afecten a una gran cantidad de afectados), los costes de implantación de las medidas o el riesgo que el tratamiento presenta para los derechos y libertades de los titulares de los datos, así como

la idoneidad de adherirse a códigos de conducta que reflejan la voluntad real de querer acometer buenas prácticas dentro de la organización.

En consecuencia, el RGPD sigue señalando en el mismo articulado que cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos, reconociendo que la adhesión a códigos de conducta aprobados a tenor del artículo 40 del RGPD o a un mecanismo de certificación aprobado según las indicaciones de dicha norma podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.

Es sólo una forma de gestionar la protección de datos distinta de la que se viene empleando ahora, más cercana a la figura del Compliance Penal o prevención de riesgos normativos, pero que, en todo caso, busca una mayor sensibilidad a la hora de tratar datos de empleados, candidatos, clientes, usuarios y/o afectados en el tratamiento de su información privada y personal.

En último lugar cabe señalar que es fundamental entender cómo el principio de responsabilidad proactiva, un pilar clave del RGPD, se entrelaza estrechamente con el concepto de Compliance o cumplimiento normativo en el ámbito empresarial. El cumplimiento normativo se refiere a la necesidad de que una empresa evite sanciones, multas y daños a su reputación, que pueden surgir como consecuencia de no respetar las leyes y regulaciones aplicables a su sector, incluyendo aquellas relacionadas con la protección de datos.

Por ello, en el contexto de la protección de datos, es crucial que las empresas integren la normativa de protección de datos en su estrategia de Compliance o de su programa de cumplimiento. Esto significa que el programa de cumplimiento normativo de cualquier empresa no solo debe estar alineado con el RGPD, sino que debe

ser una herramienta activa para asegurar la responsabilidad proactiva. Esto implica una gestión y un tratamiento de los datos personales de forma que se pueda demostrar en todo momento el cumplimiento de las normativas de protección de datos.

Al incorporar el principio de responsabilidad proactiva en el programa de Compliance, la empresa no solo minimiza el peligro de los riesgos legales y financieros, sino que también afirma su compromiso con la seguridad y la privacidad de los datos, un aspecto cada vez más valorado por clientes y socios comerciales.

4.2 Principio de Licitud, Lealtad y Transparencia: es decir, tratar los datos de manera lícita, leal y transparente:

Los principios relativos a la licitud, lealtad y transparencia implican que los datos han "tratados de manera lícita, leal y transparente en relación con el interesado".

- ***Licitud***: el requerimiento de licitud se desarrolla en el artículo 6 del RGPD, estableciendo seis bases de legitimación para justificar legalmente un tratamiento de datos personales, consolidándose el consentimiento como una de ellas, y prohibiendo la normativa cualquier tipo de legitimación diferente a las señaladas en el punto de esta guía relativo a la Licitud del tratamiento.

- ***Lealtad***: el responsable ha de ser leal al titular de los datos y no engañar al mismo sobre la finalidad del tratamiento y en ningún caso ocultar posibles finalidades distintas, aunque sean complementarias, no ocultando ninguna finalidad por obvia que la misma pueda parecer o por similitud a una ya existente o por mucho que fuere una práctica habitual en la forma de proceder de las empresas. Este principio de licitud está muy vinculado a la información y a la transparencia como derechos del interesado, ya que la misma debe facilitarse de forma comprensible y

accesible por parte de cualquier titular de los datos afectados. Por tanto, el tratamiento no será leal y lícito si la información no está accesible debidamente o no es comprensible para los destinatarios.

- ***Transparencia:*** el responsable del tratamiento está obligado a ser muy transparente acerca de sus intenciones en cuanto al tratamiento de datos del usuario e informar convenientemente al titular de los datos. El RGPD establece la obligación de facilitar al interesado toda la información relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, implicando que no es suficiente con entregar al usuario la información, sino que el lenguaje y medios utilizados juegan también un papel importante. Se desarrolla así un concepto clave que no es otro que la expectativa razonable de privacidad del afectado. Atendiendo al contexto en el que se realiza la recogida de datos y las circunstancias en las que se contextualizará el tratamiento, el responsable debe considerar:

    1. Cuál es la expectativa del interesado al entregarle sus datos,

    2. Qué espera recibir en contraprestación y,

    3. Cuál es el uso que entiende razonable a cambio de sus datos al responsable del tratamiento. Las finalidades accesorias a la principal que el responsable pretenda realizar han de estar, por tanto, muy claramente definidas en la información proporcionada y no se debe dar por sentado que el usuario otorga su consentimiento a las mismas, debiendo legitimar el tratamiento para finalidades accesorias por medio de alguna de las bases de legitimación del tratamiento previstas.

Ejemplo

Una empresa no puede ceder los datos de sus clientes a otra empresa sin que exista una base de legitimación (como el consentimiento) y sin informar a los afectados.

Cabe mencionar que la normativa de protección de datos considera como infracción muy grave:

El tratamiento de datos personales sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el art. 6 del Reglamento (UE) 2016/679».

4.3 Principio de Minimización de datos: Implica que los datos personales tienen que ser "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados"; lo cual no deja de ser una actualización del principio de calidad de los datos recogidos en la LOPD, el cual establecía que los datos deben de ser adecuados pertinentes y no excesivos en relación con la finalidad y el ámbito para la que fueron recabados. Sin embargo, en el caso del RGPD no se limita por el exceso si no por la necesidad. Es decir, los datos personales serán adecuados pertinentes y limitados a la necesidad.

Ejemplo

Una empresa por regla general no puede preguntar por el estado civil de una candidata en un proceso de selección de personal.

4.4 Principio de Limitación de la finalidad: Implica que el responsable debe recoger los datos con fines determinados, explícitos y legítimos, limitándose su uso posterior a dichos fines y no serán tratados ulteriormente de manera incompatible con dichos fines.

Ejemplo

Una empresa no puede instalar cámaras de videovigilancia informando que la finalidad de la misma sea controlar el acceso y garantizar la seguridad en sus instalaciones y posteriormente utilizar las grabaciones con el fin de controlar la productividad de los trabajadores o ejercer el control disciplinario.

4.5 Principio de Exactitud: Mantener los datos exactos y actualizados, adoptándose las medidas necesarias para su supresión o rectificación sin dilación, evitando en todo momento que los datos sean inexactos con respecto a los fines para los que se tratan.

Ejemplo

Una empresa no conservará por regla general curriculums de candidatos de procesos de selección de personal que se celebraron en años anteriores debido a que esos CV posiblemente estarán obsoletos y el candidato haya mejorado sus habilidades mediante formación o mediante el desempeño de nuevos puestos de trabajo.

A este respecto señala también el considerando 39 del RGPD que:

> *"Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos."*

4.6 Principio de Limitación del plazo de conservación: Este principio establece que los datos personales no deben ser almacenados por más tiempo del estrictamente necesario para cumplir con los fines para los cuales fueron recopilados. Únicamente se pueden conservar los datos personales por parte del responsable durante el tiempo estrictamente necesario para los fines de tratamiento.

¿Qué Implica este Principio?

1. **Definición Clara del Periodo de Conservación**: Las empresas deben establecer previamente y de manera clara el tiempo durante el cual los datos personales serán conservados. Este periodo debe estar justificado basándose en la finalidad de la recogida de datos.
2. **Evaluación y Revisión Periódica**: Es importante revisar periódicamente los datos almacenados, así como eliminar aquellos que ya no sean necesarios. Esto implica también reevaluar los plazos de conservación establecidos, ajustándolos si las circunstancias o los propósitos cambian.
3. **Informar a los Interesados**: La empresa debe informar a las personas de cuánto tiempo se conservarán sus datos o, si esto no es posible, los criterios utilizados para determinar este plazo.

Si bien en nuestra normativa ya se establece que deberán ser cancelados cuando los datos dejen de ser útiles para la finalidad en la que fueron recabados, el RGPD además de limitar el plazo de conservación establece la obligación al responsable de incluir

plazos para la supresión o revisión periódica, dependiendo de cada normativa específica.

Determinados plazos de conservación pueden ser:

- 6 años como mínimo respecto a libros de contabilidad y facturas desde la fecha de creación de los documentos. (art. 30 Código de Comercio);

- 4 años como mínimo respecto a obligaciones tributarias (arts. 66 y ss Ley General Tributaria);

- 4 años respecto a documentación laboral y de la Seguridad Social (artículo 21 del Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social).

- 30 días como máximo respecto a las grabaciones de cámaras de videovigilancia (Instrucción 1/2006 de la AEPD)

- 5 años para las acciones personales sin plazo especial (art. 1964 Código Civil);

- 10 años para las acciones derivadas de la Ley 10/2010, de 28 de abril, de Prevención de Blanqueo de Capitales y Financiación del Terrorismo (art. 25);

- 15 años como mínimo para acuerdos de confidencialidad y de no competencia (si hay una sanción asociada a las cláusulas de no competencia o confidencialidad)

4.7 Principio de Integridad y confidencialidad: Las empresas deben proteger los datos personales de manera adecuada para

evitar accesos no autorizados, pérdidas o daños, es por ello que deben de garantizar en la medida de lo posible una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas. Siendo consciente el responsable de tratamiento de la valoración del riesgo de los datos personales que trata, y también conociendo el estado de la técnica, los costes de la aplicación y los fines del tratamiento. El RGPD en base a la responsabilidad proactiva propone entre otras medidas:

- La seudonimización y el cifrado de datos personales;
- La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
- La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
- Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Además de éstas, no debe olvidarse aquella medida tanto técnica como organizativa tendente a garantizar que cualquier persona, ya sea el encargado o el responsable del tratamiento, sólo acceda a los datos pertinentes y siguiendo las instrucciones de éste.

La organización debe velar en todo momento por que se cumplan las directrices establecidas por el responsable del tratamiento.

05

¿Cuándo es legal un tratamiento? Licitud de los tratamientos.

05 ¿Cuándo es legal un tratamiento? Licitud de los tratamientos.

Como se ha señalado anteriormente, el principio de licitud del RGPD establece que todo tratamiento de datos personales tiene que ser lícito, lo cual implica, que además de respetar las leyes, como cualquier otra actividad profesional de las PYMES o autónomos, sólo se puede llevar a cabo si se fundamenta en alguna de las bases jurídicas que establece el artículo 6.1 del mismo RGPD.

Estas bases jurídicas no mantienen entre sí ninguna relación de prioridad entre ellas e incluso un mismo tratamiento puede contar con más de una base jurídica. La elección de la base jurídica del tratamiento por parte del responsable debe hacerse siempre antes de empezar las operaciones de tratamiento, teniendo en cuenta su finalidad con el fin de incluirla en la información que se facilita a la persona afectada y cumplir así convenientemente con el principio de información.

Las bases jurídicas en las que se deben de argumentar la legalidad de cualquier tratamiento pueden ser las siguientes:

1) El **consentimiento** del interesado;

2) El tratamiento es necesario para la **ejecución de un contrato** en el que el interesado es parte;

3) El tratamiento es necesario para el **cumplimiento de una obligación legal** aplicable al responsable del tratamiento;

4) El tratamiento es necesario para proteger **intereses vitales** del interesado o de otra persona física;

5) El tratamiento es necesario para el cumplimiento de una misión realizada en **interés público** o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

6) El tratamiento es necesario para la **satisfacción de intereses legítimos** perseguidos por el responsable del tratamiento o por un tercero.

Para cumplir con el principio de licitud, la empresa deberá basar el tratamiento de los datos en alguna de las bases jurídicas expuestas en cumplimiento con el principio de licitud. Conforme al principio de licitud del tratamiento, expuesto en el apartado anterior, la empresa deberá tratar los datos en virtud de una base jurídica (o incluso varias en su caso) que legitime la posibilidad de llevar a cabo un tratamiento de datos personales.

A continuación, detallamos cada una de las bases de legitimación:

5.1 Cuando la persona afectada presta su consentimiento.

El consentimiento constituye una de las seis bases jurídicas establecidas en el RGPD en las que el responsable puede fundamentar el tratamiento de datos personales. La principal novedad que se introduce en el RGPD con respecto a la anterior normativa es que el consentimiento debe de consistir en una declaración afirmativa o expresa, no admitiéndose por tanto el consentimiento tácito de ninguna forma. De esta manera, el consentimiento debe de ser claro de tal forma que refleje una

manifestación de voluntad libre, específica, informada e inequívoca del interesado.

El consentimiento sólo es una base jurídica adecuada si reúne los requisitos establecidos, ya que dicho consentimiento debe ser:

a) **Informado**. Antes de que la persona afectada otorgue el consentimiento, es necesario facilitarle la información suficiente para que comprenda cual es la finalidad para la que está consintiendo el tratamiento de sus datos consintiendo realmente. En este sentido, tiene especial importancia la información sobre la identidad del responsable (PYME o autónomo) y las finalidades del tratamiento, sin perjuicio de los otros aspectos a los cuales nos referiremos en el apartado relativo a la información necesaria.

b) **Libre**. La persona titular de los datos tiene que disponer de una capacidad de elección y control real de sus datos personales, de modo que si decide no dar el consentimiento o retirarlo en cualquier momento no puede ser víctima de consecuencias negativas o perjuicios de ningún tipo. No se puede considerar que el consentimiento ha sido prestado libremente cuando:

- Hay un desequilibrio evidente entre el titular de los datos y el responsable del tratamiento, en particular cuando este responsable es empleador y el titular de los datos es una persona trabajadora del responsable.

Si una empresa quiere usar datos biométricos (como huellas dactilares o reconocimiento facial) para controlar las horas de trabajo o el acceso al trabajo de las personas trabajadoras, debe seguir unas reglas específicas. La Agencia de Protección de Datos advierte que, en estos casos, no es suficiente con que las personas trabajadoras den su consentimiento. Esta restricción surge debido a la existencia de un desequilibrio inherente de poder entre la persona titular de los datos (empleados) y el responsable (autónomo o PYME), lo cual compromete

la capacidad de libertad sobre el consentimiento, y, por lo tanto, el consentimiento no sirve para justificar el uso de datos biométricos en este contexto al ser de alto riesgo.

- No permite autorizar por separado las diferentes operaciones de tratamiento de datos, a pesar de ser adecuado en el caso o finalidad concreta.

Expresamente indica el RGPD la posibilidad de utilizar casillas para la obtención del consentimiento, estableciendo que una casilla marcada por el responsable previamente o la inacción no constituye una forma de prestar el consentimiento. Igualmente, también se establece en dicho considerando que cuando existan varios fines para el tratamiento se deberá recabar el consentimiento para todos ellos.

- La ejecución de un contrato se supedita al consentimiento para tratar datos que no son necesarios para el contrato mencionado.

Por ejemplo, cuando se publican fotos del personal laboral de una PYME, la publicación de la imagen de las personas trabajadoras no puede fundamentarse en el contrato de trabajo con carácter general y deberá de publicarse bajo consentimiento de las mismas.

c) **Específico**. El consentimiento podrá ser requerido para toda actividad de tratamiento que responda a una misma finalidad concreta y determinada. Si el tratamiento tiene varias finalidades el consentimiento deberá requerirse de forma separada para cada una de ellas: es lo que se conoce como consentimiento granular.

Así, por ejemplo, si un gimnasio quiere publicar imágenes de sus clientes y quiere felicitarle por su cumpleaños para remitirle ofertas especiales, se hace necesario solicitar dos consentimientos diferenciados: uno para la publicación de la imagen y otro para la remisión de comunicaciones comerciales en base a la fecha de cumpleaños.

d) **Inequívoco**. Cuando la base de legitimación se fundamente en el consentimiento, la empresa está obligada a poder acreditar que cuenta con el consentimiento del interesado para dicho tratamiento. De modo que el consentimiento prestado por el interesado deberá ser, en todo caso, inequívoco, mediante un acto afirmativo claro o una manifestación de voluntad de aceptar el tratamiento de datos que le afectan.

Además de inequívoco, el consentimiento tiene que ser explícito en los supuestos siguientes:

A) El tratamiento de datos de categorías especiales,
B) La adopción de decisiones automatizadas basadas en los datos del interesado, o
C) La posibilidad de realizar transferencias internacionales de sus datos personales.

La empresa no podrá, por tanto, recabar el consentimiento del interesado por omisión, por silencio o mediante casillas previamente marcadas. De hecho, el Considerando 171 del RGPD exige que, si el tratamiento prestado antes de la entrada en vigor de la norma se prestó tácitamente, sea necesario que el interesado lo preste de nuevo, de manera inequívoca, para continuar con el tratamiento, ya que esa forma de consentimiento ya no es compatible con el RGPD, al basarse en la inacción del interesado.

¿Es válido el consentimiento prestado antes de la entrada en vigor al RGPD?

El RGPD señala también que los tratamientos iniciados con anterioridad al inicio de su aplicación sobre la base del consentimiento seguirán siendo legítimos siempre que ese consentimiento se hubiera prestado del modo en que prevé el propio RGPD, es decir, mediante una manifestación o acción afirmativa.

El consentimiento "tácito", no basado en ninguna acción de la persona afectada o incluso en el uso de casillas premarcadas, no es admisible, por lo tanto. En cambio, sí es conforme al RGPD el uso de una declaración por escrito o la marcación de casillas en un sitio web. Si se utiliza una declaración escrita que también haga referencia a otros asuntos, la parte referida a la protección de datos tiene que quedar claramente diferenciada del resto de declaraciones.

En cualquier caso, la persona afectada tiene derecho a retirar el consentimiento en cualquier momento, del mismo modo, o incluso de una forma más sencilla que la fórmula utilizada para prestarlo, sin que eso afecte a la licitud del tratamiento previo a la revocación basado en el consentimiento.

Corresponde al responsable del tratamiento demostrar en todo momento que la persona afectada ha otorgado el consentimiento y que éste es válido, necesitando evidencias de la recopilación de dicho consentimiento de forma libre, inequívoca, específica e informada.

¿Puede publicar una peluquería o un establecimiento de hostelería una foto o un video de sus clientes?

Si un comercio quiere publicar la imagen de un cliente en sus redes

sociales necesita el consentimiento de la persona: no es válido el consentimiento verbal como ocurre en muchas ocasiones que establecimientos de restauración como bares o discotecas, o incluso peluquerías y centros de estudios publican fotos y/o videos de sus clientes, usuarios, alumnos o incluso personal laboral sin disponer de evidencias de que han otorgado el consentimiento para ello libremente, lo cual puede ser motivo de sanción económica

5.2 Cuando el tratamiento sea necesario para el mantenimiento de una relación contractual.

El RGPD considera lícito el tratamiento de datos cuando es necesario para ejecutar un contrato en que la persona afectada es parte o para aplicar medidas precontractuales a petición de esta persona.

¿Las PYMES y los autónomos pueden tratar los datos de su personal laboral sobre la base jurídica relativa a la ejecución de un contrato?

Cuando una PYME o un autónomo tiene que pagar la nómina a una persona trabajadora, el tratamiento de los datos personales de la persona está legitimada en el contrato que regule la relación laboral.

5.3 Cuando el tratamiento es necesario para el cumplimiento de una obligación legal.

De acuerdo con el RGPD, el tratamiento de datos también puede ser lícito cuando es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. En cualquier caso, es necesario que esta obligación esté prevista en una norma con rango de ley o en el derecho de la Unión Europea.

¿Las PYMES y los autónomos pueden comunicar los datos de su personal a la Tesorería General de la Seguridad Social, como por ejemplo al solicitar la afiliación de una persona trabajadora a la Seguridad Social?

Sí, ya que la legislación sectorial específica en la materia establece expresamente la obligación del empresario, en este caso de la PYME o autónomo, de solicitar la afiliación de quien ingrese en su servicio.

5.4 Cuando el tratamiento sea necesario para proteger los intereses vitales del interesado u otra persona física.

En principio, esta base de legitimación tiene un carácter excepcional y por tanto subsidiario, ya que sólo tiene que utilizarse cuando el tratamiento de datos no se pueda fundamentar en ninguna de las otras bases jurídicas. No es una base de legitimación propia de los tratamientos habituales de las PYMES o autónomos ya que responde a finalidades humanitarias, incluyendo el control y la propagación de epidemias, o en situaciones de emergencia humanitaria.

5.5 Cuando el tratamiento sea necesario para proteger el interés público o garantizar el ejercicio de los poderes públicos.

El RGPD permite el tratamiento de datos personales cuando sea necesario para cumplir con una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. La misión de interés público o, si procede, los poderes públicos mencionados tienen que derivar de una función atribuida al responsable por una norma con rango de ley.

5.6 Cuando el tratamiento sea necesario para satisfacer un interés legítimo.

El tratamiento de datos personales también puede ser lícito cuando sea necesario para satisfacer intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que no deban prevalecer los intereses o los derechos y las libertades fundamentales de la persona afectada que requieren la protección de datos personales, especialmente si la persona afectada es un niño. A estos efectos, el responsable del tratamiento tiene que llevar a cabo la ponderación apropiada, acreditando la concurrencia de un interés legítimo en el tratamiento en los casos necesarios y poder justificarlo mediante un informe de Análisis de Interés Legítimo o LIA. En cuanto al interés legítimo el RGPD en sus Considerandos 47, 48, 49 y 50, aporta ejemplos de casos donde el tratamiento puede justificarse mediante el interés legítimo:

1. La prevención del fraude y la mercadotecnia directa.

2. El tratamiento de datos personales de clientes y empleados en grupos empresariales con diferentes filiales.

3. Para impedir atentados contra la seguridad de la red y la información ante eventuales ataques de «denegación de servicio» o «DDoS» o la distribución malintencionada de códigos o virus informáticos.

4. Los tratamientos con fines de interés público, de investigación científica e histórica o fines estadísticos.

En cualquier caso, para poder basar un tratamiento en el interés legítimo, el responsable del tratamiento tiene la obligación de demostrar que se ha llevado a cabo la ponderación del interés legítimo, siendo lo más recomendable disponer de un informe LIA al respecto.

¿Puede una PYME o autónomo ofertar a un cliente productos y/o servicios similares a los adquiridos a través de comunicaciones comerciales en base al interés legítimo?

Sí, se puede ofrecer a los clientes descuentos y ofertas sobre cualquier producto ofrecido por la entidad o beneficio asociado a los productos o gestión del servicio, respetando siempre la expectativa de privacidad, como, por ejemplo, no ofrecerle esos productos si el cliente se ha negado previamente.

06

Comunicaciones de datos y encargados de tratamiento.

06 Comunicaciones de datos y encargados de tratamiento.

El Reglamento (UE) 2016/679 define al responsable del tratamiento o responsable como “la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros”.

Por ejemplo,

- Una empresa que presta servicios a sus clientes es responsable del tratamiento de datos de sus clientes.
- Un centro médico es responsable del tratamiento de sus pacientes.
- Un centro educativo es responsable de tratamiento de los datos de sus alumnos.
- Una empresa que contrata personal es responsable del tratamiento de los datos asociados a las personas trabajadoras, como puedan ser la nómina o su CV.

Es decir, responsable del tratamiento es aquella persona jurídica o física que decida sobre la finalidad de sus tratamientos, así como los medios para llevar a cabo los mismos.

Dicho responsable de tratamiento puede ceder datos a terceros:

- Para que dichos terceros utilicen los datos para finalidades propias al del responsable del tratamiento, lo que se conoce como una comunicación de datos propiamente dicha.

- Para que dichos terceros realicen la prestación de un servicio o encargo al responsable y para ello necesitan acceder a los datos, conociéndose estos terceros como "encargados del tratamiento".

El RGPD, a diferencia de la normativa anterior, no prevé habilitaciones específicas para las comunicaciones de datos personales, sino que se les aplica el régimen general previsto para el resto de los tratamientos. Por lo tanto, cualquier comunicación de datos requiere alguna de las bases jurídicas referidas anteriormente. Si, además, conlleva el tratamiento de categorías especiales de datos, también debe concurrir alguna de las excepciones previstas en el artículo 9.2 del RGPD.

Existirá pues una comunicación de datos si el tercero que recibe los datos puede destinarlos a sus propias finalidades, decidiendo sobre el objeto y finalidad del tratamiento.

Ejemplo.

Si una empresa decide vender o alquilar su base de datos de clientes a un tercero, con el fin de que éste último envíe publicidad por su cuenta de sus propios productos o servicios existirá una cesión de datos, en la que la empresa será el cedente y el tercero el cesionario. En este caso, deberá informar a los afectados y con cumplir los requisitos legales de la cesión de datos, siempre y cuando puede existir una base de legitimación que posibilite dicha cesión.

En caso de que el tercero no pueda decidir sobre el objeto o finalidad de tratamiento porque es un proveedor de servicios entonces nos encontramos ante un encargado de tratamiento que tiene que seguir las directrices marcadas por el responsable de tratamiento al que presta servicios

Ejemplo.

Una PYME contrata los servicios de una asesoría fiscal y/o laboral para la llevanza de la contabilidad o de las nóminas del personal. Esta asesoría es un proveedor de servicios que se configura como encargado de tratamiento ya que tiene que acceder a los datos de los clientes o de las personas trabajadoras de la PYME.

El Reglamento (UE) 2016/679 define, en el artículo 4.8), al encargado del tratamiento como

> "la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento". Lo relevante, por tanto, es que el encargado del tratamiento, a diferencia de lo que ocurre con la figura de responsable del tratamiento, no decide sobre el tratamiento de los datos personales.

Ejemplo.

Si una empresa encarga la gestión de las nóminas a un asesor externo y para ello comunica los datos personales de sus trabajadores a dicho asesor, existirá un acceso a datos necesario para la prestación de un servicio, en el que su empresa será el responsable del tratamiento de estos datos y el asesor será el encargado del tratamiento (pero no un cesionario de los datos).

En la práctica puede haber multitud de encargados del tratamiento, tales como un prestador de servicios de nube que trata datos personales por cuenta del responsable del tratamiento, la empresa que ofrece servicios de hosting y que también trata datos personales por cuenta del responsable, la empresa que ofrece servicios de call center al responsable, una asesoría laboral que elabora las nóminas para una empresa a la que presta sus servicios. En todos los casos, se trata de una persona, física o jurídica, ajena a la organización del responsable del tratamiento que accede o trata datos personales por cuenta de este para prestarle un servicio mediante una relación contractual.

La realización de una prestación de servicios con acceso a datos requiere la existencia de un contrato escrito que establezca expresamente las obligaciones del encargado del tratamiento. Con el RGPD, la responsabilidad última sobre el tratamiento sigue estando atribuida al responsable, que es quien determina la existencia del tratamiento y su finalidad. Ahora bien, el RGPD introduce cambios importantes en las relaciones responsable-encargado que su empresa deberá tomar en consideración independientemente de la posición que ocupe en el tratamiento de los datos.

De esta manera, si su empresa es el responsable:

a) Tendrá que elegir únicamente encargados que ofrezcan garantías suficientes de que aplicarán medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con el RGPD.

b) Tendrá que indicar si permite o no la existencia de subencargados, es decir, si el encargado puede a su vez subcontratar a otro encargado del tratamiento, y en caso afirmativo, exigirle las mismas garantías que al encargado.

c) Es aconsejable que exija una declaración al encargado comprometiéndose a cumplir con las exigencias del RGPD y

solicitarle además pruebas o evidencias del cumplimiento del RGPD antes de firmar el contrato y durante su vigencia.

Si, en cambio, su empresa es el encargado del tratamiento, tenga en cuenta:

a) Considere la idoneidad de mantener un registro de las actividades del tratamiento que refleje todos los tratamientos a los que accede como encargado.

b) Determine todas las medidas de seguridad aplicables a los tratamientos que realice.

c) Deberá designar un delegado de protección de datos si accede a tratamientos de datos de un responsable que está obligado a disponer de un DPD.

d) Si destina los datos a una finalidad distinta a la establecida en el contrato suscrito con el responsable (o si los comunica o utiliza incumpliendo las estipulaciones de dicho contrato), responderá de las infracciones, pues se le considerará un responsable del tratamiento a estos efectos, exonerando al responsable del tratamiento de cualquier tipo de responsabilidad.

Respecto a los contratos entre responsable y encargado que hayan sido firmados con anterioridad al 25 de mayo de 2018, dejaron de tener validez en mayo de 2022, habiendo sido necesario la firma de un nuevo contrato de encargado de tratamiento.

La AEPD ha elaborado una guía para la elaboración de los contratos entre responsables y encargados de tratamiento según las exigencias del RGPD[2] cuya revisión es aconsejable.

2 Dicha guía para elaborar un contrato de encargado de tratamiento con un proveedor de servicios puede ser descargada en el enlace: https://www.aepd.es/media/guias/guia-directrices-contratos.pdf

Respecto a las comunicaciones de datos a los cuerpos policiales, la Ley Orgánica 7/2021 de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, dispone la obligación de cualquier persona física o jurídica de proporcionar a las autoridades competentes los datos, los informes y los justificantes necesarios que les soliciten, de manera motivada, concreta y específica, en los supuestos siguientes:

- Para la investigación y el enjuiciamiento de infracciones penales o para la ejecución de penas por parte de las autoridades judiciales, el ministerio fiscal o la policía judicial. De las solicitudes de información realizadas por la policía judicial, se tiene que dar cuenta en todo caso a la autoridad judicial y fiscal. La comunicación de datos que lleven a cabo la Administración tributaria, la Inspección de Trabajo y la Administración de la Seguridad Social debe hacerse de acuerdo con su legislación específica.

- Para la prevención, la detección y la investigación de infracciones penales por las autoridades competentes.

- Para la prevención y la protección enfrente de un peligro real y grave para la seguridad pública por las autoridades competentes.

Estas obligaciones no eximen de obtener la autorización judicial pertinente, cuando sea exigible así de recopilar las evidencias necesarias por escrito. Incumplir este deber de colaboración, o facilitar información a las personas afectadas por estas comunicaciones, se tipifica como infracción los arts. 58.j y 59.j de la Ley Orgánica 7/2021 protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

07

Obligaciones de las PYMES y autónomos antes de iniciar un tratamiento.

07 Obligaciones de las PYMES y autónomos antes de iniciar un tratamiento.

7.1 Análisis del ciclo de vida del tratamiento.

Antes de emprender cualquier tratamiento de datos que implique el tratamiento de datos personales, la PYME o el autónomo responsable tiene que llevar a cabo una serie de consideraciones como hacer un análisis del "ciclo de vida" o recorrido de los datos a lo largo de su tratamiento, con el fin de identificar:

- Cuáles son los datos personales hay que recoger y para qué finalidad.
- Cómo se recogerán los datos personales ya sea a través de formularios en papel, digitalmente, telefónicamente o de cualquier otra fórmula reconocida en derecho.
- Quién dentro de la empresa los va a tratar (áreas, departamentos o personal responsable).
- Cómo se van a manejar dentro de la entidad (en soporte papel, telemáticamente, o digitalmente).
- A que otras personas jurídicas o físicas distintas del responsable del tratamiento se cederán o si se van a realizar transferencias internacionales.

- Cómo se van a conservar los datos y durante cuánto tiempo y cómo se destruirán cuando finalice el plazo de conservación.

7.2 Aplicación del principio de minimización y proporcionalidad de los datos.

Las PYMES y los autónomos debe tener muy en cuenta el principio de minimización en el contexto de la protección de datos, un aspecto crucial dentro de la normativa de protección de datos personales. Este principio, como una manifestación del principio de proporcionalidad, establece directrices claras sobre cómo deben manejarse los datos personales, asegurando que su tratamiento sea siempre justo, relevante y restringido a lo estrictamente necesario. Para ello se debe tener siempre en consideración:

- Adecuación y Pertinencia de los Datos: El principio de minimización dicta que los datos personales recopilados deben ser estrictamente los adecuados y pertinentes para el propósito para el cual se están procesando. Esto significa que cualquier información que no sea esencial para el objetivo declarado no debe ser recopilada o almacenada.

- Limitación y Necesidad en el Tratamiento de Datos: Este principio enfatiza la importancia de limitar el tratamiento de datos personales. Implica evitar la recopilación y el uso de datos de manera generalizada, excesiva o indiscriminada. Solo se deben tratar los datos personales cuando sean estrictamente necesarios para alcanzar una finalidad específica, y siempre utilizando la menor cantidad de datos posible.

- Implementación de la Seudonimización: Una estrategia efectiva que se alinea con el principio de minimización

- es la seudonimización. Este método consiste en tratar los datos de tal manera que no puedan asociarse directamente con una persona específica sin la utilización de información adicional. La seudonimización permite que los datos se traten de manera más segura, minimizando los riesgos asociados con el tratamiento de datos personales y limitando el acceso a la información identificativa.

En resumen, el principio de minimización actúa como un guardián en el tratamiento de los datos personales, asegurando que solo se utilicen los datos estrictamente necesarios para un fin determinado y fomentando prácticas como la seudonimización para una mayor seguridad y privacidad.

7.3 Protección de Datos por Diseño y por Defecto.

La protección de datos desde el diseño implica que la PYME o el autónomo responsable, tanto en el momento de determinar los medios de tratamiento como en el momento del tratamiento, tendrá en cuenta el estado de la técnica, el coste de la aplicación, la naturaleza, el ámbito, el contexto y las finalidades del tratamiento, así como los riesgos que entraña el tratamiento para los derechos y las libertades de las personas, mediante las siguientes directrices:

- Implantar las medidas técnicas y organizativas adecuadas para aplicar de forma efectiva los principios de protección de datos (como puede ser la seudonimización).

- Integrar las garantías necesarias en el tratamiento, para proteger los derechos de las personas afectadas.

La protección de datos por defecto obliga a la PYME o autónomo responsable del tratamiento a aplicar las medidas técnicas y organizativas adecuadas para garantizar que, por defecto, el tratamiento afecta de la menor forma posible a las personas afectadas:

- Únicamente se tratan los datos personales necesarios para cada una de las finalidades específicas del tratamiento.

- El alcance del tratamiento es sólo el estrictamente necesario para conseguir la finalidad perseguida.

- Los datos sólo se conservan durante el plazo necesario para alcanzar la finalidad perseguida.

- Los datos personales no son accesibles a un número indeterminado de personas físicas, sino que los accesos a los mismos están controlados y únicamente acceden los mismos el personal debidamente autorizado por el Responsable de tratamiento.

7.4 Análisis de Riesgos.

Ni el RGPD ni la LOPD recogen una lista detallada de las medidas de seguridad que la PYME o el autónomo tienen que adoptar para cumplir. La normativa obliga a los responsables a llevar a cabo un análisis de riesgos a partir del cual se definirán las medidas técnicas y organizativas que necesita el responsable para establecer un nivel de seguridad adecuado y no ser sancionado en caso de que se produzcan los riesgos.

Para proporcionar una explicación más técnica del análisis de riesgos en la protección de datos, podemos desglosarlo en tres etapas clave, cada una con sus propias complejidades y metodologías específicas:

- Identificación de Amenazas y Vulnerabilidades: En esta primera etapa, el responsable del tratamiento de datos realiza una exhaustiva identificación de posibles amenazas de riesgos. Esto abarca desde vulnerabilidades de seguridad cibernética, como brechas de seguridad o ciberataques que podrían conducir a fugas de datos, hasta riesgos operacionales y ambientales, como fallos en

- la infraestructura de TI o desastres naturales que pongan en peligro la conservación de los datos. La identificación también implica comprender cómo estas amenazas podrían explotar las debilidades existentes en el sistema y afectar la integridad, disponibilidad y confidencialidad de los datos.

- Evaluación Cuantitativa y Cualitativa de Riesgos: En este paso, se realiza una evaluación del riesgo asociado a cada amenaza identificada, considerando dos dimensiones principales: la probabilidad de ocurrencia y el impacto potencial. El objetivo es clasificar los riesgos en términos de su severidad y priorizarlos en consecuencia para prestar mucha atención a los riesgos más probables o a los que puedan generar consecuencias más graves a los titulares de los datos personales.

- Poder mitigar y minimizar los riesgos: Basándose en la evaluación de riesgos realizada, el responsable del tratamiento debe diseñar e implementar un conjunto de medidas técnicas y organizativas para mitigar los riesgos identificados. Esto puede incluir la implementación de soluciones de seguridad robustas, como cifrado de datos, autenticación multifactor y sistemas de detección y prevención de intrusiones, así como políticas y procedimientos organizativos, como la formación y sensibilización del personal en seguridad de la información, políticas “Bring Your Own Device” y planes de recuperación ante desastres.

Es importante destacar que el análisis de riesgos no es un proceso estático, sino dinámico. Requiere una revisión y actualización de forma periódica para adaptarse a los cambios en el entorno tecnológico, las prácticas operativas y el panorama de amenazas, garantizando así un nivel de seguridad de datos adecuado y actualizado.

Para poder evaluar los riesgos, hay que tener especialmente en cuenta si el tratamiento puede provocar alguna de estas situaciones en las personas afectadas:

- Discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

- Privación a los afectados de sus derechos y libertades o que se les pueda impedir ejercer el control sobre sus datos personales.

- Tratamiento no meramente incidental o accesorio de las categorías especiales de datos, de datos relacionados con infracciones o condenas penales o relacionados con la comisión de infracciones administrativas.

- Evaluación de aspectos personales de las personas afectadas con la finalidad de crear o utilizar sus perfiles personales, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

- Tratamiento de datos de grupos de afectados en una situación de especial vulnerabilidad y, en particular, de menores de edad o personas con discapacidad.

- Tratamiento masivo que implique un gran número de afectados o comporte la recogida de una gran cantidad de datos personales.

- Tratamiento de datos personales que tengan que ser objeto de una transferencia, con carácter habitual, a terceros estados u organizaciones internacionales respecto de los cuales no se haya declarado un nivel adecuado de protección.

- Cualquier otra que, en opinión del responsable o del encargado, pueda tener relevancia y, en particular, las previstas en códigos de conducta y estándares definidos por esquemas de certificación.

El análisis de riesgos debe de aplicarse a todos los tratamientos de una PYME o un autónomo, con independencia de que el tratamiento se tenga que someter o no a una evaluación de impacto sobre la protección de datos. Si se hace una evaluación de impacto sobre la protección de datos, el análisis de riesgos tiene que formar parte de él.

7.5 Evaluación de Impacto.

Una evaluación de impacto en la protección de datos (o EIPD) es un procedimiento que pretende identificar y controlar los riesgos para los derechos y las libertades de las personas, asociados a un tratamiento de datos cuando este genere un alto riesgo para los datos personales.

El responsable del tratamiento tiene la obligación de hacer una evaluación del impacto antes del tratamiento, cuando sea probable que por su naturaleza, alcance, contexto o fines suponga un alto riesgo para los derechos y libertades de las personas físicas, especialmente cuando se utilicen nuevas tecnologías. Por lo tanto, siempre hay que verificar este aspecto a la hora de determinar la necesidad de hacer o no una EIPD.

Entre otros supuestos, de acuerdo con el RGPD es obligatorio realizar una evaluación de impacto cuando exista:

- Evaluación sistemática y exhaustiva de aspectos personales de personas físicas basada en un tratamiento

automatizado, como la elaboración de perfiles, sobre la base de la cual se toman decisiones que producen efectos jurídicos para las personas físicas o que las afectan significativamente de manera similar.

- Tratamiento a gran escala de las categorías especiales de datos, o de los datos personales relativos a condenas e infracciones penales. A efectos de determinar si el tratamiento se hace a gran escala se pueden tener en cuenta los elementos siguientes:

  i. El número de personas afectadas ya sea en términos absolutos o como proporción de una determinada población.
  ii. El volumen y la variedad de datos tratados.
  iii. La duración o permanencia de la actividad de tratamiento.
  iv. La extensión geográfica de la actividad de tratamiento.
  v. Observación sistemática a gran escala de una zona de acceso público.

Estas no son listas cerradas. Además de tener que ser el responsable quien determine si los tratamientos deben de ser analizados por una EIPD, la propia autoridad AEPD ha publicado un listado de tratamientos exentos de realizar una Evaluación de Impacto como aquellos otros que sí están obligados a llevar a cabo un EIPD.

Están obligados en todo caso a llevar a cabo una EIPD:

1. Tratamientos que impliquen perfilado o valoración de sujetos, incluida la recogida de datos del sujeto en múltiples ámbitos de su vida (desempeño en el trabajo, personalidad y comportamiento), que cubran varios aspectos de su personalidad o sobre sobre sus hábitos.

2. Tratamientos que impliquen la toma de decisiones automatizadas o que contribuyan en gran medida a la toma de tales decisiones, incluyendo cualquier tipo de decisión que impida a un interesado el ejercicio de un derecho o el acceso a un bien o un servicio o formar parte de un contrato.

3. Tratamientos que impliquen la observación, monitorización, supervisión, geolocalización o control del interesado de forma sistemática y exhaustiva, incluida la recogida de datos y metadatos a través de redes, aplicaciones o en zonas de acceso público, así como el procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, TV interactiva, aplicaciones móviles, etc.

4. Tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos.

5. Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física.

6. Tratamientos que impliquen el uso de datos genéticos para cualquier fin.

7. Tratamientos que impliquen el uso de datos a gran escala.

8. Tratamientos que impliquen la asociación, combinación o enlace de registros de bases de datos de dos o más tratamientos con finalidades diferentes o por responsables distintos.

9. Tratamientos de datos de sujetos vulnerables o en riesgo de exclusión social, incluyendo datos de menores de 14 años, mayores con algún grado de discapacidad, discapacitados, personas que acceden a servicios sociales y víctimas de violencia de género, así como sus descendientes y personas que estén bajo su guardia y custodia.

10. Tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo para los derechos y libertades de las personas.

11. Tratamientos de datos que impidan a los interesados ejercer sus derechos, utilizar un servicio o ejecutar un contrato, como por ejemplo tratamientos en los que los datos han sido recopilados por un responsable distinto al que los va a tratar y aplica alguna de las excepciones sobre la información que debe proporcionarse a los interesados según el artículo 14.5 (b,c,d) del RGPD.

Están exentos de llevar a cabo una EIPD en el caso de PYMES y autónomos:

- Tratamientos que sean necesarios para el cumplimiento de una obligación legal, cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, siempre que en el mismo mandato legal no se obligue a realizar una EIPD, y siempre y cuando ya se haya realizado una EIPD completa.

- Tratamientos realizados en el ejercicio de su labor profesional por trabajadores autónomos que ejerzan de forma individual, en particular médicos, profesionales de la salud o abogados, sin perjuicio de que pueda requerirse cuando el tratamiento que lleven a cabo cumpla, de forma significativa, con dos o más criterios establecidos en la lista de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos publicada por la AEPD.

- Tratamientos obligatorios por ley y realizados con relación a la gestión interna del personal de las PYMES con finalidad de contabilidad, gestión de recursos humanos y nóminas, seguridad social y salud laboral, pero nunca relativos a los datos de los clientes.

- Tratamientos realizados por comunidades y subcomunidades de propietarios tal como se definen en el artículo 2 (a, b y d) de la Ley 49/1960 de Propiedad Horizontal.

- Tratamientos realizados por colegios profesionales y asociaciones sin ánimo de lucro para la gestión de los datos personales de sus propios asociados y donantes, y en el ejercicio de su labor, siempre que no incluyan en el tratamiento de datos sensibles tales como los que

se establecen en el artículo 9.1 del RGPD y no sea de aplicación el artículo 9.2(d) de dicho Reglamento.

En cualquier caso, la AEPD puede actualizar las listas orientativas sobre los tratamientos tanto obligados como exentos de tener que realizar una Evaluación de Impacto y por ello es muy recomendable consultar periódicamente sus publicaciones en su web (https://www.aepd.es/) en donde publicará dichos listados en el momento oportuno.

La obligación de realizar la evaluación de impacto corresponde al responsable del tratamiento, con la colaboración del encargado del tratamiento en su caso, y con el asesoramiento del delegado de protección de datos en cada supuesto. La evaluación tiene que incluir, como mínimo:

- Una descripción sistemática de las operaciones de tratamiento previstas y de las finalidades del tratamiento, incluido, si procede, el interés legítimo perseguido.
- Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento, en relación con su finalidad.
- Una evaluación de los riesgos para los derechos y las libertades de las personas afectadas.
- Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garantizan la protección de datos personales y para demostrar la conformidad con la normativa de protección de datos, teniendo en cuenta los derechos y los intereses legítimos de las personas afectadas.

En cualquier caso la AEPD pone a disposición de las PYMES y autónomos la herramienta EVALÚA_RIESGO RGPD, que tiene como objeto servir de ayuda a responsables y encargados a identificar los factores de riesgo para los derechos y libertades de los interesados cuyos datos están presentes en el tratamiento, hacer una primera evaluación del riesgo intrínseco, incluyendo la necesidad de realizar una EIPD, y estimar el riesgo residual si se utilizan medidas y garantías para mitigar los factores de riesgos específicos[3].

Si como conclusión de la EIPD se determina que el tratamiento previsto puede infringir el RGPD o entrañaría un alto riesgo si no se toman medidas adecuadas para mitigarlo, el responsable tiene que formular una consulta previa a la Agencia Española de Protección de Datos, a través del trámite electrónico específico que figura en su sede electrónica.

7.6 Registro de Tratamientos.

El art. 30 del RGPD elimina la obligación de identificar los ficheros y notificar los mismos a la autoridad de control nacional, pero obliga a las empresas y administraciones públicas a elaborar un registro de actividades de tratamiento (RAT). Dicho registro, aunque sea de naturaleza interna tiene que estar siempre a disposición de la autoridad de control pertinente, ya que se configura como instrumento documental que permite tener una imagen actualizada de los tratamientos que lleva a cabo la PYME o el autónomo, siendo esencial para la gestión de riesgos, para el cumplimiento de los principios y las obligaciones, y para que la autoridad de control lo pueda supervisar.

Se debe de considerar que el RAT no es obligatorio para los responsables de tratamiento que cuenten con menos de 250 trabajadores siempre que:

a) No se realicen tratamientos que entrañen riesgos para los afectados;

3 La referida herramienta está disponible en la web https://evalua-riesgo.aepd.es/

b) Los tratamientos sean ocasionales;

c) El tratamiento no se refiera a datos de categorías especiales (art. 9 del RGPD), entre otros, los relativos a la etnia, raza, creencia religiosa o política, salud u orientación sexual o relativas a infracciones y condenas penales y que no puedan suponer un riesgo para los derechos y libertades de las personas afectadas.

Es por ello que, en la práctica se recomienda disponer de un RAT, aunque no sea obligatorio para el responsable, en aras del cumplimiento activo y de poder evidenciar la preocupación por cumplir con la normativa de protección de datos ante el posible requerimiento de la autoridad de control pertinente.

El registro de actividades de tratamiento, que tiene que constar en formato electrónico, debe incluir la información siguiente:

- La identificación y datos de contacto del responsable de tratamiento, y si procede del corresponsable en caso de que existan tratamientos cuya responsabilidad haya sido compartida, así como los datos del DPD en caso de que el responsable del tratamiento haya designado a uno.

- Las finalidades del tratamiento.

- Descripción de las categorías de datos personales tratados, así como las categorías de personas afectadas.

- Las categorías de destinatarios de las comunicaciones de datos, incluidas las que se prevean internacionalmente en el caso de transferencias internacionales, con identificación de los países destinatarios si procede.

- El plazo previsto para la supresión de los datos en función de su categoría, en caso de que sea posible.

- Descripción de las medidas técnicas y organizativas que adoptadas para cumplir con la normativa en caso de que sea posible.

El registro de actividades de tratamiento debe de mantenerse actualizado, tanto antes de iniciar el tratamiento y cada vez que se produzca un cambio significativo en el mismo. Hay que comunicar al delegado de protección de datos cualquier adición, modificación o exclusión en su contenido en caso de que se haya designado a uno.

En todo momento el registro de tratamientos actualizado tiene que estar a disposición de la Agencia Española de Protección de Datos para el ejercicio de sus funciones como autoridad de control.

Cuando la PYME o el autónomo actúe como encargado del tratamiento, también debe llevar un registro de actividades del tratamiento diferenciado, en el cual conste:

- El nombre y los datos de contacto del encargado y de cada responsable por cuenta del cual actúa el encargado y, si procede, del representante del responsable o del encargado y del delegado de protección de datos.

- Las categorías de tratamientos efectuados por cuenta de cada responsable.

- Las transferencias internacionales de datos personales previstas, incluida la identificación del tercer país u organización internacional de destino. Si se basa en garantías adecuadas, también hay que identificar la documentación donde constan.

- La descripción general de las medidas técnicas y organizativas de seguridad cuando sea posible.

¿Cómo puede el responsable organizar el registro de actividades del tratamiento?

Un punto de partida para organizar este registro pueden ser los ficheros anteriores al RGPD que se hubieran podido notificar a la Agencia Española de Protección de Datos, y detallar todas las operaciones que se efectúan sobre cada conjunto estructurado de datos. También se puede organizar entorno a operaciones de tratamiento concretas, vinculadas a una finalidad básica común de todas ellas (por ejemplo “clientes”, “gestión contable”, “videovigilancia”, “selección de personal” o “gestión de recursos humanos y nóminas”), o de acuerdo con otros criterios diferentes que determine la PYME o el autónomo responsable del tratamiento.

En cualquier caso y aunque no hay que notificar el registro de tratamientos ante la Agencia Española de Protección de Datos, es obligación de la PYME o el autónomo responsable disponer de dicho registro actualizado en caso de que la autoridad de control se lo pueda requerir en cualquier momento. Al final de la presente guía se recoge un modelo de registro de actividades de tratamiento según la herramienta la AEPD disponible en la web de la autoridad de control denominada “FACILITA RGPD”.

08

Obligaciones de las PYMES y autónomos durante el tratamiento.

08 Obligaciones de las PYMES y autónomos durante el tratamiento.

8.1 Informar a las personas afectadas.

Corresponde al responsable del tratamiento cumplir la obligación de informar a las personas afectadas y estar en condiciones de demostrar que lo ha cumplido, ya que las personas afectadas tienen derecho a ser informadas sobre las condiciones en que el responsable llevará a cabo el tratamiento de sus datos, sin necesidad de solicitarlo y tienen derecho igualmente a la transparencia en el tratamiento de sus datos personales.

Tanto el derecho de transparencia como de información a las personas afectadas se configuran como obligaciones ineludibles para las PYMES y autónomos que sean responsables de tratamiento, de tal modo que tienen que cumplir con las siguientes obligaciones:

- Facilitar la información de forma clara, precisa, comprensible y de fácil acceso.

- Utilizar un lenguaje claro y sencillo, especialmente cuando la información se pueda dirigir a menores de edad, evitando fórmulas enrevesadas y que incorporen remisiones a textos legales o que no se distingan de la información sobre otras cuestiones.

- Por escrito o por otros medios, incluidos los electrónicos, debiendo acreditar en todo momento que se ha facilitado la información necesaria.

- Facilitar a las personas interesadas el ejercicio de sus derechos, salvo en el supuesto de la imposibilidad de identificar a los mismos.

- Establece el plazo de un mes para contestar a peticiones de interesado, para en caso contrario, abrir vía de la reclamación ante la autoridad.

- Carácter gratuito de las peticiones, salvo que, por reiteración o carácter infundado o excesivo, donde podrá establecer un canon o negarse a ellas

- En su caso, la persona interesada puede solicitar información adicional

Con respecto al contenido de la información, hay que diferenciar si los datos se obtienen de la persona afectada o no. Si los datos se obtienen de la persona afectada, en el momento de su obtención es obligatorio informar sobre:

A) La identidad y los datos de contacto del responsable y/o su representante;

B) Los datos de contacto del delegado de protección de datos en su caso;

C) La finalidad del tratamiento y la base jurídica del tratamiento;

D) Cuando el tratamiento se base en el interés legítimo, identificar claramente el referido interés legítimo, en su caso;

E) Los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

F) Si existen transferencias internacionales de los datos, así como el lugar donde se puede obtener una copia de las garantías adecuadas, en su caso;

G) el plazo durante el cual se conservarán los datos personales o los criterios para fijarlos;

H) el derecho a solicitar el acceso a los datos, la rectificación o la supresión de los datos, la limitación del tratamiento, la oposición al tratamiento y la portabilidad de los datos,

I) el derecho a retirar en cualquier momento el consentimiento si el tratamiento se fundamenta en esta base jurídica, y sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo;

J) el derecho a presentar una reclamación ante una autoridad de control;

K) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, de las consecuencias en el caso de no cederlos;

l) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, y la información sobre la lógica aplicada y sus consecuencias.

En el caso de que la información no sea obtenida directamente de la persona interesada, se deberá informar adicionalmente, además de los puntos antes indicados:

- Las categorías de datos personales que se tratan.
- La fuente de donde proceden los datos personales.

En cualquier caso, la normativa ha previsto la posibilidad de utilizar un mecanismo de doble capa para informar a las personas afectadas.

Las fórmulas para informar a las personas interesadas pueden ser diversas:

- Locución pregrabada.
- Entrevista telefónica.
- Formularios en papel, incluso en el reverso del documento.
- Formularios online, de forma visible en el formulario.
- Folletos explicativos.
- Aplicaciones móviles.
- SMS o mensajería instantánea.
- En la política de privacidad de la web.

Ejemplo de información por capas.

En la primera capa, que se puede incluir por ejemplo como una pequeña leyenda en los formularios en papel de recogida de datos, tiene que constar la información básica junto con una remisión a una dirección electrónica (correo o web) u otro medio que permita a la persona afectada acceder de manera sencilla a la segunda capa, con el resto de información prevista en la normativa de forma más extensa.

8.2 Atender los derechos de las personas interesadas.

El RGPD reconoce a la persona afectada el poder de control sobre sus datos personales y le otorga la posibilidad de ejercer los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad de los datos, oposición y a no ser objeto de decisiones individuales automatizadas. Ya sea el responsable de tratamiento un autónomo o una PYME el responsable de tratamiento, es crucial entender y cumplir con las obligaciones impuestas por la normativa de protección de datos en cuanto a la atención de los derechos que se reconocen a cualquier personada afectada. Como responsable del tratamiento de estos datos, la actividad profesional tiene obligaciones específicas en cuanto a la atención de los derechos:

1. **Derechos de las personas interesadas**: La normativa reconoce a cualquier persona interesada o afectada por el tratamiento de datos de un responsable los derechos de acceso, rectificación, oposición, supresión (o “derecho al olvido” cuando el mismo se aplica a las búsquedas por internet), limitación del tratamiento, portabilidad de los datos, y el derecho a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de sus datos.

2. **Gratuidad del Ejercicio de Derechos**: El responsable debe garantizar que las personas interesadas pueden ejercer estos derechos de forma gratuita salvo supuestos muy justificados. En supuestos muy concretos si las solicitudes son manifiestamente infundadas o excesivas, particularmente por su carácter repetitivo, la empresa puede:

    - Cobrar un canon proporcional a los costes administrativos generados.
    - Negarse a actuar sobre la solicitud. Sin embargo, esta decisión debe tomarse con cautela y estar debidamente justificada.

3. **Plazos de Respuesta**: Las solicitudes de los titulares de los datos deben ser atendidas en un plazo máximo de un mes desde su recepción por regla general. Este plazo puede extenderse hasta dos meses adicionales, dependiendo de la complejidad y el número de solicitudes. En tal caso, es obligatorio informar al interesado de esta prórroga dentro del primer mes.

4. **Facilidad de Medios para Ejercer Derechos**: Es responsabilidad de la empresa proporcionar medios accesibles para que los individuos puedan ejercer sus derechos. En cualquier caso, no se debería negar el derecho de cualquier persona a optar por un medio diferente al ofrecido por la empresa en caso de que los mismos no sean fácilmente accesibles.

5. **Obligación de Informar en Caso de No Actuación**: Si se decide no atender a una solicitud de derechos, debe informar a la persona afectada, a más tardar en un mes desde la recepción de la solicitud, explicando las razones de su no actuación y la posibilidad de presentar una reclamación ante la Autoridad de Control competente (la Agencia Española de Protección de Datos en el caso de las PYMES y autónomos).

Al tratarse de derechos personalísimos, tiene que ejercerlos la persona afectada o un tercero por representación, ante el responsable del tratamiento. La solicitud se puede presentar por cualquier medio que permita dejar constancia de la identidad de la persona que la formula, así como de su presentación.

El responsable tiene que tomar las medidas razonables para verificar la identidad de la persona afectada que ejerce un derecho. Si tiene dudas razonables en cuanto a la identidad de quien presenta la solicitud, puede pedir información adicional para confirmarla. Estos derechos sólo pueden limitarse mediante una norma con rango de ley o el derecho de la Unión y son los siguientes:

8.2.1 Derecho de acceso.

La persona afectada tiene derecho a saber si el responsable del tratamiento trata sus datos personales y, en ese caso, tiene derecho a acceder a estos datos y a obtener la información siguiente:

a) Los fines del tratamiento; o para que se están tratando o usando sus datos

b) Las categorías de datos personales que se tratan como identificativos, salud, biométricos, videovigilancia por señalar algunos ejemplos.

c) Los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales.

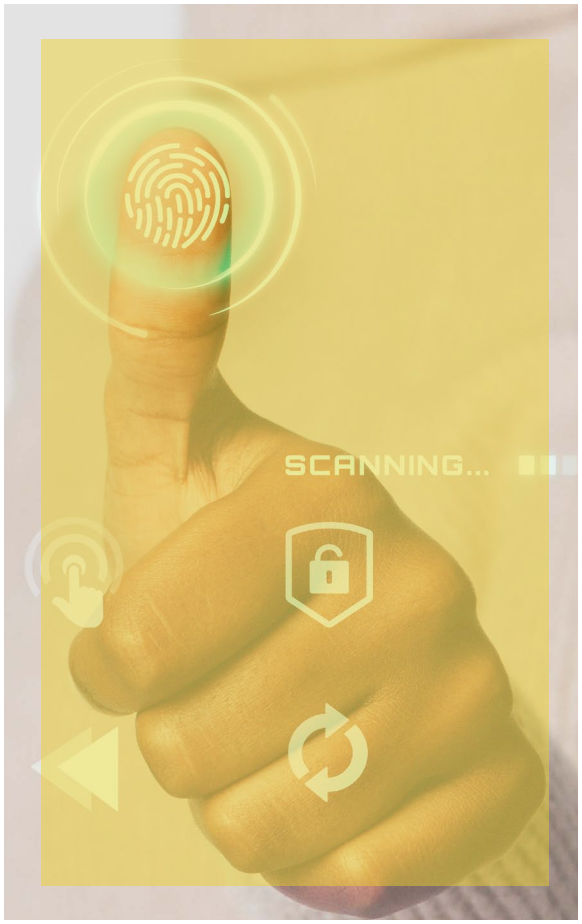
d) Plazo de conservación o plazo previsto para ello o los criterios utilizados para determinarlo.

e) El derecho a solicitar al responsable del tratamiento la rectificación o la supresión de los datos, la limitación del tratamiento o el derecho a oponerse.

f) El derecho a presentar una reclamación ante una autoridad de control.

g) El origen de los datos, cuando no se han obtenido de la persona afectada.

h) La existencia de decisiones automatizadas, incluida la elaboración de perfiles, información sobre el algoritmo aplicado y sus consecuencias para el interesado a nivel de privacidad.



Este punto es tan novedoso como interesante en materia de los diferentes usos de la Inteligencia Artificial, ya que implica la transparencia algorítmica y que la persona afectada pueda saber si se utiliza un algoritmo para tratar los datos personales, y en que medida le puede afectar a la persona titular de los datos

i) En caso de transferencias internacionales de datos, las garantías adecuadas que se ofrecen.

Debe a su vez acompañarse de una copia de los datos personales objeto del tratamiento. La persona afectada puede solicitar que el derecho de acceso se haga efectivo a través de los sistemas de consulta siguientes:

- Visualización en pantalla.
- Escrito, copia o fotocopia, por correo certificado u ordinario.
- Correo electrónico u otros sistemas de comunicación electrónica.
- Cualquier otro sistema que sea adecuado a las características del tratamiento.

Si se solicita por medios electrónicos, la persona afectada tiene derecho a recibir la información en este mismo formato.

Además, tiene derecho a obtener una copia gratuita de los datos objeto del tratamiento, siempre que no afecte negativamente a los derechos y las libertades de otras personas. Para copias posteriores, se puede establecer un canon según los costes operativos y de gestión.

8.2.2 Derecho de rectificación.

La persona afectada tiene derecho a obtener la rectificación de sus datos personales que sean inexactos y a que se completen sus datos incompletos.

El responsable debe:

- Comunicar la rectificación efectuada a cada uno de los destinatarios a quienes se hayan comunicado los datos, a no ser que sea imposible o exija un esfuerzo desproporcionado.

- Informar a la persona afectada sobre los destinatarios, si lo solicita.

La rectificación de los datos personales tiene que generar el bloqueo de los datos rectificados.

8.2.3 Derecho de Supresión (O Derecho al Olvido).

La supresión de los datos personales del interesado sin dilación siempre y cuando se den alguna de las siguientes circunstancias:

- los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

- se retire el consentimiento en que se basa el tratamiento;

- el interesado se oponga al tratamiento con arreglo al derecho de oposición, por motivos particulares o por mercadotecnia, y no prevalezcan otros motivos legítimos para el tratamiento;

- los datos personales hayan sido tratados ilícitamente;

- los datos personales deban suprimirse para el cumplimiento de una obligación legal;

- los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información.

En el caso de que los datos hayan sido cedidos a terceros, se deberá solicitar a dichos terceros que procedan su cancelación por parte del responsable.

No obstante, todo ello no aplicará cuando los tratamientos sean necesarios para:

- Ejercer el derecho a la libertad de expresión e información;
- Cumplir una obligación legal;
- Por razones de interés público o fines de archivo publico estadístico, etc...
- Para la formulación del ejercicio o la defensa de reclamaciones.

La supresión de los datos da lugar al bloqueo de los datos suprimidos.

8.2.4 Derecho a la limitación del tratamiento.

El es el derecho de la persona interesada a que no se realice tratamiento con respecto a alguna de sus finalidades durante un tiempo determinado si se dan las circunstancias para ello Se podrá ejercitar la limitación del tratamiento cuando se cumpla alguna de las siguientes circunstancias:

- Cuando la persona afectada ha ejercido los derechos de rectificación u oposición y mientras el responsable determina si procede atender la solicitud.
- Cuando el tratamiento es ilícito, pero la persona afectada se opone a la supresión y solicita la limitación.
- Cuando los datos ya no son necesarios para el tratamiento, pero la persona afectada se opone a la supresión porque los necesita para formular, ejercer o defender reclamaciones.

- En caso de interés legítimo, mientras se acredita que interés prevalece

Cuando una persona afectada ha obtenido la limitación del tratamiento, hay que informarle antes de que se levante la medida. Cuando se ha limitado el tratamiento, el responsable debe:

- Hacer constar la limitación de forma clara en sus sistemas de información.
- Comunicar la limitación efectuada a cada uno de los destinatarios a quienes se hayan comunicado los datos, a no ser que resulte imposible o exija un esfuerzo desproporcionado.
- Informar a la persona afectada sobre los destinatarios, si lo solicita.

8.2.5 Derecho a la portabilidad de datos.

En virtud del derecho a la portabilidad, la persona afectada tiene derecho a recibir, en un formato estructurado, de uso común y de lectura mecánica, sus datos personales que ha facilitado a un responsable del tratamiento.

Este derecho también incluye la posibilidad de que se transmitan directamente del responsable a otro responsable, si es técnicamente posible. Para que el derecho de portabilidad sea viable, se deberán cumplir las condiciones siguientes:

- La recogida de los datos está fundamentada en el consentimiento o en un contrato.
- El tratamiento se realiza con medios automatizados.

8.2.6 Derecho de oposición.

El derecho de oposición otorga al interesado la capacidad de oponerse al tratamiento de sus datos personales cuando este tratamiento se base en el cumplimiento de una misión de interés público, en el ejercicio de poderes públicos, o en la satisfacción de intereses legítimos,

incluyendo la elaboración de perfiles basada en dichas bases jurídicas. Esto significa que una persona puede solicitar que se deje de tratar sus datos personales al responsable, incluso si el tratamiento se realizaba legalmente bajo ciertas condiciones.

Para ejercer este derecho, la persona interesada debe presentar una solicitud al responsable del tratamiento, explicando sus razones específicas relacionadas con su situación particular, que justifiquen la oposición al tratamiento. El responsable está obligado a dejar de tratar los datos, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, derechos y libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

Ejemplo
En el caso del tratamiento de datos para fines de mercadotecnia directa o marketing, el derecho de oposición es absoluto, lo que significa que las personas afectadas tienen el derecho a oponerse en cualquier momento al tratamiento de sus datos personales para este fin, incluyendo la elaboración de perfiles en la medida en que esté relacionada con dicha mercadotecnia directa.

8.2.7 Derecho a no ser objeto de decisiones basadas en tratamientos automatizados.

Este derecho permite a las personas no ser objeto de una decisión basada únicamente en el tratamiento automatizado de sus datos personales, incluida la elaboración de perfiles, que produzca efectos jurídicos que les conciernan o les afecten de manera significativa. Esto es especialmente relevante cuando se trata de sistemas de IA que procesan grandes cantidades de datos personales para tomar decisiones o hacer predicciones.

No obstante, este derecho no es absoluto, sino que se exceptúa en caso de que estén autorizadas por la ley (que debe establecer medidas adecuadas para salvaguardar los derechos del interesado), si se basan en el consentimiento explícito del interesado o si son necesarias para la ejecución o celebración de un contrato. En estos casos, se deben implementar medidas adecuadas para proteger los derechos y libertades de los individuos, incluyendo el derecho a obtener intervención humana, a expresar el punto de vista de la persona afectada y a impugnar la decisión.

Las decisiones no se pueden basar en categorías especiales de datos, a menos que:

- Se disponga del consentimiento de la persona afectada.
- Haya que tratarlos por razones de interés público esencial establecido por una ley o el derecho de la Unión.

8.3 Verificar que los datos personales son exactos y están actualizados.

La PYME o autónomo responsable de tratamiento está obligado a adoptar todas las medidas razonables para que los datos personales inexactos se supriman o se rectifiquen, sin dilación alguna. También los puede tener que rectificar, cuando proceda, como consecuencia de que las personas afectadas hayan ejercido el derecho de rectificación. Eso hace necesario que, para mantener la información actualizada, la PYME o el autónomo que disponer de unos mecanismos individualizados de actualización a instancia de las personas interesadas, así como procedimientos periódicos de actualización y, si procede, de supresión de los datos.

Los datos rectificados están sometidos al deber de bloqueo.

8.4 El contrato de encargo de tratamiento.

Un responsable a la hora de escoger a terceras entidades como proveedores (asesorías laborales, gestorías, servicios de cloud, etc..) tiene que firmar con ellos un contrato de encargado de tratamiento como se ha señalado anteriormente; es por ello que el responsable del tratamiento tiene que velar por que el encargado al que contrate reúna las garantías necesarias para llevar a cabo el tratamiento de datos personales.

En estos casos, cuando el acceso del tercero a los datos personales del responsable es necesario para prestar el servicio, y se ha formalizado el encargo del tratamiento mediante un contrato, no se considera comunicación de datos.

Como la regulación de la relación entre el responsable y el encargado tiene que establecerse a través de un contrato, convenio, acuerdo, o acto jurídico que los vincule, siempre tiene que constar por escrito, incluyendo el formato electrónico.

El contrato o acto jurídico debe tener el contenido mínimo siguiente:

- El objeto.
- La duración.
- La naturaleza.
- La finalidad del tratamiento.
- El tipo de datos personales.
- Las categorías de personas afectadas.
- Las obligaciones y los derechos del encargado, en particular:
- Seguir las instrucciones del responsable.
- Garantizar el respeto al deber de confidencialidad.
- Tomar todas las medidas de seguridad necesarias para garantizar un nivel de seguridad adecuado al riesgo.
- Respetar el régimen de subcontratación, obligando a los posibles subcontratistas a garantizar las mismas garantías que deben de asegurar al responsable de tratamiento.

- Asistir al responsable siempre que sea posible, de acuerdo con la naturaleza del tratamiento y mediante las medidas técnicas y organizativas adecuadas.
- Ayudar al responsable a garantizar el cumplimiento de las obligaciones de seguridad.
- Poner a disposición del responsable la información necesaria para demostrar que cumple sus obligaciones y permitir y contribuir a la ejecución de auditorías.
- A elección del responsable, devolver, suprimir o entregar los datos a otro encargado. En todo caso, el encargado del tratamiento puede conservar los datos bloqueados, mientras se puedan derivar responsabilidades de su relación con el responsable del tratamiento.

El encargado del tratamiento puede subcontratar otros encargados a su vez, pero siempre con la autorización previa del responsable del tratamiento. Dicha autorización tiene que ser por escrito y puede ser específica o general. El subencargado debe vincularse con el encargado mediante un contrato análogo al establecido entre el encargado y el responsable, y está sometido a las mismas obligaciones que el encargado, por lo que, si incumple las obligaciones de protección de datos, el encargado inicial sigue siendo plenamente responsable ante el responsable del tratamiento respecto al cumplimiento de las obligaciones del subencargado.

En cualquier caso, se recomienda consultar la Guía de la Agencia de Protección de Datos en cuanto a las directrices necesarias para la correcta elaboración de un contrato de encargo de tratamiento[4].

8.5 Funciones del Delegado de Protección de Datos (DPD).

El RGPD regula la necesidad de que determinados responsables de tratamiento designen a un Delegado de Protección de Datos (DPD) o

4 Disponible en https://www.aepd.es/documento/guia-directrices-contratos.pdf

en su denominación española según la AEPD, debido a la magnitud, relevancia, riesgos adheridos o sensibilidad de los tratamientos que manejan en su día a día.

La introducción de la figura del DPP evidencia el interés de la normativa europea en reforzar el verdadero cumplimiento del derecho fundamental a la protección de datos personales por parte de las empresas y las instituciones públicas, configurando un perfil similar al del Compliance Officer o Responsable de Cumplimiento enfocado exclusivamente al cumplimiento real de las leyes de privacidad europeas, garantizando una objetividad y una posición en el seno de las organizaciones que tiene que responder ante la alta Dirección del organigrama de cualquier entidad pública o privada, y demostrar que goza de independencia absoluta para salvaguardar los derechos y libertades fundamentales de los titulares de los datos.

¿Es obligatorio designar a un DPD?

La designación de un Delegado de Protección de datos no es obligatoria para todo tipo de entidades responsables, sino que únicamente en los casos en los que el responsable y/o encargado de tratamiento se encuadren en cualquiera de los siguientes supuestos:

a) Sean Administraciones Públicas, porque el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial.

b) Sean entidades cuyas actividades principales consisten en operaciones de tratamiento que, debido a su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o

c) Sean entidades cuyas actividades principales consisten en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales.

El artículo 34 de la Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos personales y garantía de los derechos digitales (LOPDPGDD) detalla los responsables y encargados que, en todo caso, han de proceder a la designación obligatoria de DPD:

- Los colegios profesionales y sus consejos generales.
- Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.
- Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.
- Los prestadores de servicios de la sociedad de información cuando elaboren a gran escala perfiles de las personas usuarias del servicio.
- Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.
- Los establecimientos financieros de crédito.
- Las entidades aseguradoras y reaseguradoras.
- Las empresas de servicio de inversión reguladas por la legislación del Mercado de Valores.
- Los distribuidores y comercializadores de energía eléctrica, así como los distribuidores y comercializadores de gas natural.
- Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.

- Las entidades que desarrollen actividades de publicidad y prospección comercial incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de las personas afectadas o realicen actividades que impliquen la elaboración de perfiles de las mismas.

- Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes, se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.

- Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.

- Las personas operadoras que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.

- Las empresas de seguridad privada.

- Las federaciones deportivas cuando traten datos de menores de edad.

El resto de las entidades que no estén obligadas a designar un DPD, podrán nombrarlo voluntariamente, lo cual será debidamente valorado por la correspondiente Autoridad de Control, configurándose en cualquier caso las mismas obligaciones y funciones para este DPD; aclarándose pues que una vez designado, no existirá diferencia entre el carácter obligatorio o voluntario en cuanto a la designación del mismo.

¿Cuál es el perfil profesional que debería de exigirse a un DPD?

En cuanto a la titulación exigida para ser DPD, el RGPD no exige ni una titulación específica ni un certificado concreto, pero reincide de forma notoria en designar a un perfil que ostente un gran conocimiento

demostrado tanto en derecho como en la práctica de la protección de datos.

Señala el RGPD que el Delegado de Protección de Datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas.

¿El DPD debe de ser externo o interno?

El DPD podrá ser externalizado mediante un contrato de servicios (para lo cual deberá de firmar un contrato de encargado de tratamiento) o formar parte de la plantilla del responsable o, incluso del encargado de tratamiento, siempre que se acrediten las competencias profesionales a que hace referencia el RGPD, se garantice que no hay ningún conflicto de interés.

¿El DPD tiene que ser una persona física o puede ser una persona jurídica?

Surge aquí la disyuntiva sobre si el DPD debe ser una persona física o si debiese configurarse como algún tipo de persona jurídica (por ejemplo, un Consejo o un comité, o una empresa consultora en caso de que el responsable decida recurrir a un asesoramiento externo) que ejerciera las funciones de DPD.

En la práctica difícilmente una pequeña organización podrá nombrar a un DPD interno que cumpla con los requisitos que se le exigen a esta figura en cuanto absoluta independencia o ausencia de conflicto de intereses, por lo que en principio lo más recomendable debe ser contratar a un DPD externo que esté sujeto a un código ético, certificación en la materia o a una exigible deontología profesional, para que establezca unas mínimas garantías en cuanto a su profesionalidad e independencia; y todo ello porque difícilmente va a poder demostrar tal independencia el personal que habitualmente suele supervisar el cumplimiento de la protección

de datos que trabajan en otras áreas de la empresa o que pueda estar vinculada a diferentes tratamientos o responsabilidades colindantes, como pudieran ser los responsables de las áreas de informática, recursos humanos o incluso de legal, debiendo delimitar y evidenciar que dedican determinadas horas de trabajo de forma periódica y exclusiva al cumplimiento del RGPD. Es necesario establecer cuántas horas dedica el DPD en exclusiva a la supervisión del cumplimiento en la materia porque dicha evidencia puede ser exigida por la autoridad de control.

¿Cuáles son las funciones del DPD?

Las funciones que el DPD en base al cumplimiento activo son las siguientes:

- Informar y asesorar al responsable o al encargado del tratamiento de las obligaciones que les corresponden en materia de protección de datos.

- Supervisar el cumplimiento de la normativa y de las políticas en materia de protección de datos personales, incluida la asignación de responsabilidades.

- La concienciación y formación del personal que participe en las operaciones de tratamiento.

- Ofrecer el asesoramiento que le sea solicitado acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.

- Cooperar con la correspondiente autoridad de control cuando sea necesario.

- Disponibilidad para actuar como punto de contacto entre la autoridad de control correspondiente y el responsable de tratamiento en el sentido de que podrán dirigirse al DPD cualquier cliente o persona afectada, y por ello se debe incluir el canal para

poder contactar con el DPD tanto en la política de privacidad como en los formularios y en la documentación donde se deba de incluir la información preceptiva.

- Revisar el cumplimiento de la privacidad por diseño y por defecto en todos los tratamientos que realice la empresa a través de sus productos o servicios.

- Asesorar de forma crucial en las posibles brechas de seguridad, así como en la gestión de las mismas, en el sentido de que el DPP tendrá que configurarse como punto crucial de contacto con la autoridad de control, con el objetivo de ir obteniendo y transmitiendo la información que vaya recabando sobre las brechas y seguir tanto las instrucciones que establezca la normativa como las indicaciones de la autoridad de control.

- Revisión, control y supervisión en la implantación de las medidas de seguridad conforme a la responsabilidad proactiva.

- Supervisar, controlar y desarrollar cuando sea necesario, las auditorías correspondientes para el cumplimiento de la normativa.

Dichas funciones deberán de delimitarse o incluso ampliarse dependiendo de cada organización.

¿Cuál ha de ser la posición del DPD dentro de la organización?

A) En primer lugar, la empresa debe asegurar que no existe ningún tipo de conflicto de intereses con el desempeño de las funciones encomendadas, y para ello debería aportar un informe concluyendo sobre la idoneidad del DPD.

B) Debe de gozar de absoluta independencia de modo que no reciba instrucción alguna en cuanto al desempeño sus funciones.

C) Debe de ser nombrado por un periodo razonable de tiempo con el objetivo de que puedan llevarse a cabo medidas a corto, medio y largo plazo.

D) No puede ser destituido ni sancionado por el desempeño de sus funciones.

E) Tiene obligación de confidencialidad el secreto en lo que respecta al desempeño de sus funciones.

F) Ha de rendir cuentas directamente al más alto nivel jerárquico de la organización, ya sea del responsable o del encargado de tratamiento.

¿Tiene la empresa obligación de publicar los datos del DPD?

Los datos de contacto del DPD deberán ser publicados por el responsable del tratamiento de forma adecuada, y comunicados la Autoridad de Control competente (en nuestro caso actualmente a la estatal, pero teniendo en cuenta que en un futuro el Consejo de Transparencia y Protección de Datos de Andalucía puede que tenga competencias al respecto en cuanto a los DPD de las Administraciones Públicas).

En este sentido se hace necesario aclarar que no necesariamente hay que publicar el nombre y apellidos del Delegado de Protección de Datos, sino que es suficiente con publicar los datos de contacto como pueda ser un correo corporativo (dpd@empresa.com) de forma que los interesados puedan comunicarse directamente y de forma ágil accesible con dicho DPD, teniendo en cuenta además de que si la persona que pudiera ejercer de DPD es sustituida por otra, puede causar indefensión en el ejercicio de los derechos del ciudadano, la necesidad de actualizar el canal de contacto con la nueva denominación, así como el actualizar todas las cláusulas preceptivas.

En resumidas cuentas, una PYME o autónomo debe:

1º Determinar si necesita DPD porque le obliga la normativa o porque decide asumir dicha medida de forma voluntaria.

2º Si designa a un DPD, el mismo debe cumplir los requisitos de demostrar conocimientos en derecho y en la práctica de protección de datos, independientemente de que sea interno o externo, así como que se configure como persona física o jurídica.

3º Comunicar la designación del mismo o su cese a la AEPD en un plazo máximo de 10 días.

4ª No necesariamente utilizar el nombre y apellidos de la persona que pudiera ejercer de DPD debido a la problemática que todo ello puede causar a medio plazo, y si recurrir a datos de contacto que permitan una comunicación con el mismo de forma fácil y accesible. Sin embargo, tales datos identificativos del DPD sí deberán recogerse en el registro de tratamientos.

09

Transferencias Internacionales de datos

09 Transferencias Internacionales de datos.

Cuando las PYMEs o autónomos necesiten transferir datos fuera del Espacio Económico Europeo se encontrarán ante una Transferencia Internacional de Datos (por ejemplo, porque han contratado como encargada del tratamiento a una empresa fuera de este ámbito, han externalizado determinados servicios en la nube o utilizan determinadas plataformas de servicios, como puede ser una cuenta de Gmail, servicios de copia de seguridad como Dropbox, o simplemente se usan redes sociales como Instagram o Facebook entre otros supuestos).

Queda prohibida cualquier transferencia internacional que no se adapte a los parámetros determinados por los artículos 45 y siguientes del RGPD. Por ello se hace necesario tener en cuenta que los datos personales sólo se pueden comunicar fuera del Espacio Económico Europeo en los casos siguientes:

- A países, territorios o sectores específicos sobre los cuales la Comisión Europea ha adoptado una decisión que reconoce que ofrecen un nivel de protección adecuado. Se pueden consultar los países con decisión de adecuación en la página web de la Comisión Europea[5].

5 Se pueden consultar los países y territorios que están declarados como adecuados en la web de la AEPD: https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/transferencias-internacionales

- Cuando se han ofrecido garantías adecuadas sobre la protección que los datos recibirán en su destino. El responsable o el encargado del tratamiento sólo pueden hacer una transferencia internacional si el destinatario ofrece garantías adecuadas y las personas afectadas cuentan con derechos exigibles y acciones legales efectivas. Estas garantías se pueden ofrecer mediante:

  a) Un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos; es decir, una autoridad de control u órgano análogo al que poder acudir ante la existencia de incumplimientos;

  b) Normas corporativas vinculantes de conformidad con el artículo 47 RGPD;

  c) Cláusulas tipo de protección de datos adoptadas por la Comisión Europea.

  d) Cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión Europea;

  e) Un código de conducta aprobado, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o

  f) Un mecanismo de certificación aprobado con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.

  g) Por autorización de la autoridad de control (AEPD), siempre que se haga por estas vías:

    a) Cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional.

b) Disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para las personas interesadas.

- Cuando sea de aplicación alguna de las excepciones siguientes:

◦ Cuando la persona afectada ha dado explícitamente su consentimiento a la transferencia propuesta, después de haber sido informada de los riesgos de estas transferencias a causa de la ausencia de una decisión de adecuación y de garantías adecuadas.

◦ La transferencia es necesaria para ejecutar un contrato entre la persona afectada y el responsable del tratamiento, o para ejecutar medidas precontractuales adoptadas a solicitud de la persona afectada.

◦ La transferencia es necesaria para formalizar o ejecutar un contrato entre el responsable del tratamiento y otra persona física o jurídica, en interés de la persona afectada.

◦ La transferencia es necesaria por razones importantes de interés público, que tiene que estar reconocido por el derecho de la Unión o de los estados miembros, que se aplica al responsable del tratamiento.

◦ La transferencia es necesaria para formular, ejercer o defender reclamaciones.

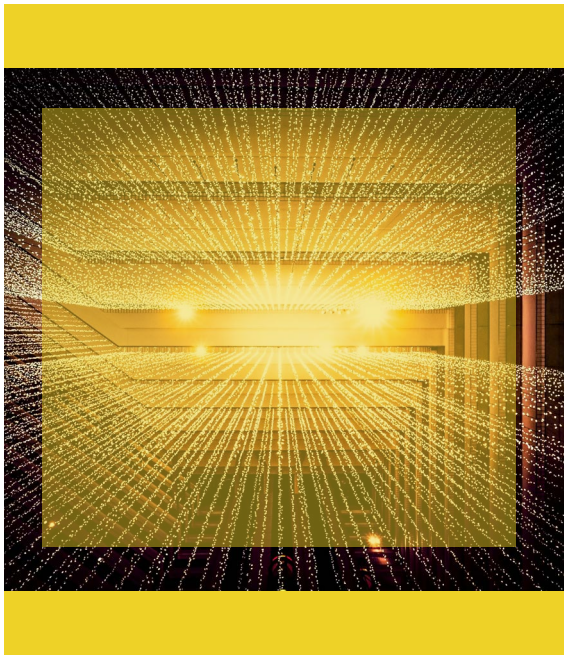
◦ La transferencia es necesaria para proteger derechos vitales de la persona afectada o de otras personas, cuando la persona afectada está física o jurídicamente incapacitada para dar el consentimiento.

◦ La transferencia se efectúa desde un registro público que, de conformidad con el derecho de la Unión o de los estados miembros, tiene por objeto facilitar información al público y está abierto a la consulta del público en general o de cualquier persona que acredite

un interés legítimo, pero sólo si se cumplen, en cada caso particular, las condiciones que establece el derecho de la Unión o de los estados miembros para hacer la consulta. En este caso, no tiene que abarcar la totalidad de los datos personales ni categorías enteras de datos personales que contiene el registro.

- Si no se da ninguna de las condiciones anteriores, la transferencia internacional de datos sólo se puede realizar si se cumplen todas las condiciones siguientes:
    - No es repetitiva.
    - Sólo afecta a un número limitado de personas afectadas.
    - Es necesaria para las finalidades de intereses legítimos imperiosos perseguidos por el responsable del tratamiento.
    - El responsable del tratamiento ha evaluado todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ha ofrecido garantías adecuadas respecto de la protección de datos personales.

En cualquier caso, las PYMES y autónomos que sean responsables de tratamiento deberán de ser muy precavidos a la hora de contratar a proveedores como encargados de tratamiento que sean contratados de fuera del Espacio Económico Europeo, debiendo analizar los riegos inherentes a las transferencias internacionales de datos.



10

Medidas de seguridad

10 Medidas de Seguridad.

10.1 Integridad, confidencialidad y disponibilidad.

El responsable del tratamiento de datos y el encargado de este están obligados, conforme a la normativa vigente, a asegurar que el tratamiento de los datos personales se realice de manera que garantice su seguridad adecuada. Esto incluye la protección frente a cualquier forma de acceso a los datos no autorizado o ilícito, así como contra la pérdida, destrucción o daño accidental de los datos. Dicha garantía debe materializarse mediante la implementación y mantenimiento de medidas técnicas y organizativas apropiadas.

Además, es imperativo que tanto el responsable como el encargado del tratamiento de datos aseguren de manera inequívoca la confidencialidad, integridad y disponibilidad de los datos personales. Para ello, es preciso llevar a cabo una identificación y evaluación exhaustiva de los riesgos potenciales que puedan afectar a los datos personales tratados. En base a esta evaluación, se deben establecer y aplicar las medidas de seguridad necesarias para mitigar, o en su caso, eliminar dichos riesgos, en cumplimiento de las obligaciones legales pertinentes.

- La obligación de confidencialidad implica evitar la divulgación, ya sea accidental o intencionada, de dicha información a terceros no autorizados, salvo en los casos en que legalmente se establezca lo contrario. Este deber de confidencialidad no se limita a la prohibición de divulgar datos a terceros externos, sino que también impone la restricción de acceso a la información personal, limitando dicho acceso a lo estrictamente necesario para el desempeño de las funciones de cada persona trabajadora. Esto incluye, entre otras medidas, la instalación de sistemas de control físico de acceso a la información (tales como cierres de oficinas y archivadores), la creación de una política de asignación de permisos de acceso (por ejemplo, mediante el uso de claves o certificados digitales), y la implementación de sistemas de control de accesos.

  Para reforzar el cumplimiento del deber de confidencialidad, es aconsejable incluir cláusulas específicas en los contratos laborales, así como en los protocolos de compliance o regulaciones internas de la organización. Cabe destacar que la obligación de confidencialidad por parte del personal se mantiene incluso después de la finalización de la relación laboral. Esta obligación de confidencialidad prevista en la normativa de protección de datos es complementaria del deber de secreto profesional para determinadas profesiones, como pudiera ser la de la abogacía o la del sector farmacéutico o sanitario.

- La obligación de integridad de la información responde al principio de exactitud en el sentido que la información personal no puede sufrir modificaciones no autorizadas. Así, los datos personales deben tratarse de forma que se garantice la protección contra la alteración, pérdida, destrucción o daño accidental, mediante la aplicación de las medidas técnicas u organizativas adecuadas.

- La obligación de disponibilidad hace referencia a la necesidad de que los datos estén siempre disponibles. La falta, incluso temporal, de información necesaria para tomar decisiones puede afectar seriamente los derechos, libertades e intereses de las personas

involucradas. Por ello, tanto el responsable como el encargado del tratamiento de datos personales deben implementar medidas técnicas y organizativas. Estas medidas incluyen la realización de copias de seguridad y la preparación de soluciones alternativas para casos de fallos, como interrupciones del suministro eléctrico, para garantizar el acceso constante a la información.

Medidas de seguridad básicas:

Actualización de ordenadores y dispositivos: Los dispositivos y ordenadores utilizados
para el almacenamiento y el tratamiento de los datos personales siempre deberán mantenerse actualizados.

Malware: En los ordenadores y dispositivos donde se realice el tratamiento automatizado
de los datos personales se dispondrá de un sistema de antivirus que garantice en la
medida posible, el robo y/o destrucción de la información que deberá ser actualizado convenientemente de forma periódica.

Cortafuegos o Firewall: Para evitar accesos remotos indebidos a los datos personales se
velará por garantizar la existencia de un firewall activado en aquellos ordenadores y
dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales.

Cifrado de datos: Cuando se precise realizar la extracción de datos personales fuera del
recinto donde se realiza su tratamiento, ya sea por medios físicos o por medios electrónicos,
se deberá valorar la posibilidad de utilizar un método de encriptación

para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la
información.

Copia de seguridad: Periódicamente se realizará una copia de seguridad en un segundo
soporte distinto del que se utiliza para el trabajo diario. La copia se almacenará en lugar
seguro con el fin de permitir la recuperación de los datos personales en caso de pérdida
de la información.

10.2 Gestión de brechas de datos personales.

Una brecha de datos personales es un incidente de seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de los datos personales tratados por un responsable, o bien la comunicación o acceso no autorizados a los mismos.

Una brecha de datos personales puede tener una serie de efectos adversos considerables en las personas, susceptibles de ocasionar daños y perjuicios físicos, materiales o inmateriales; por lo que los responsables de tratamiento tienen que demostrar medidas proactivas para intenta evitarlas y en caso de que sucedan gestionarlas adecuadamente, especialmente cuando puedan poner en riesgo los derechos y libertades de las personas físicas.

El artículo 33 del RGPD impone a los responsables de un tratamiento de datos personales la obligación de notificar a la autoridad de control competente las brechas de datos personales cuando sea probable que constituyan un riesgo para los derechos y libertades de las personas.

Que hacer en Caso de Brecha de Datos Personales:

1. **Evaluación de Riesgo:** El responsable del tratamiento de los datos debe de aplicar las medidas previstas al haber evaluado el nivel de riesgo que conlleva la brecha de datos personales.

2. **Notificación Obligatoria:** Si la brecha representa un riesgo para los derechos y libertades de las personas, debe notificarse a la AEPD. Esta notificación es obligatoria y debe hacerse dentro de las 72 horas desde que la organización tiene conocimiento de la brecha.

3. **Comunicación a Afectados:** En situaciones donde la brecha de datos supone un alto riesgo, es necesario informar también a las personas afectadas. Esta comunicación debe realizarse de acuerdo con lo establecido en el artículo 34 del RGPD.

En caso de una brecha de seguridad, la notificación realizada debe contener información esencial, que incluye:

1. **Naturaleza de la Violación:** Descripción detallada del incidente de seguridad.

2. **Datos Personales y Personas Afectadas:** Categorías de los datos personales y el grupo de personas afectadas por la brecha.

3. **Contacto del Responsable:** Datos del delegado de protección de datos o, en su ausencia, de una persona de contacto relevante.

4. **Posibles Consecuencias:** Impacto potencial y consecuencias de la violación para las personas afectadas.

5. **Medidas Tomadas:** Acciones emprendidas por el responsable para remediar la brecha.

6. **Medidas de Mitigación:** Si es aplicable, estrategias para minimizar efectos negativos en las personas afectadas.

Esta información es fundamental para una comunicación transparente y efectiva con la autoridad de control y las personas afectadas, en línea con los requerimientos del RGPD.

Para facilitar la gestión y respuesta ante brechas de datos personales, la AEPD proporciona una herramienta muy útil para PYMES y autónomos conocida como ASESORA BRECHA. Esta herramienta es de gran ayuda en la evaluación y toma de decisiones relacionadas con brechas de seguridad[6].

La herramienta ASESORA BRECHA y la cumplimentación de estas obligaciones son fundamentales para garantizar una respuesta adecuada ante cualquier incidente de seguridad, salvaguardando así los derechos de los individuos y cumpliendo con la normativa vigente. En caso de haber designado un DPD, será fundamental la supervisión de éste en la toma de decisiones a la hora tanto de gestionar la brecha como de comunicar la misma ante las personas afectadas como ante las autoridades pertinentes.

6 Disponible en la web de la AEPD en: https://www.aepd.es/guias-y-herramientas/herramientas/asesora-brecha

11

Obligación de bloquear los datos al finalizar el tratamiento.

11 Obligación de bloquear los datos al finalizar el tratamiento.

El responsable del tratamiento está obligado a bloquear los datos cuando los rectifique o los suprima. Esta obligación está prevista en la LOPDGDD, y hay que aplicar tanto cuando se suprimen como cuando se rectifican los datos.

El bloqueo de datos es un procedimiento clave en la gestión de la privacidad y protección de datos. Consiste en la identificación y reserva de datos personales, aplicando medidas técnicas y organizativas para evitar su tratamiento, lo que incluye impedir su visualización. Este proceso es crucial excepto en los casos donde los datos deben estar disponibles para requerimientos legales como jueces, tribunales, el ministerio fiscal, administraciones públicas competentes o autoridades de protección de datos. Todo ello con el objetivo de determinar responsabilidades relacionadas con el tratamiento de datos y solo se mantiene durante el tiempo legalmente establecido para la prescripción de dichas responsabilidades. Durante este periodo, los datos bloqueados no deben utilizarse para ningún otro propósito y, una vez finalizado, deben ser destruidos.

En situaciones donde el bloqueo no es posible debido a limitaciones del sistema de información o si su implementación requiere un esfuerzo

desproporcionado, se debe realizar una copia segura de la información. Esta copia debe garantizar una evidencia digital o de otro tipo que asegure su autenticidad, la fecha de bloqueo y que los datos no han sido alterados durante este periodo.

Cuando una persona interesada ejerce su derecho de supresión de datos, el responsable del tratamiento debe bloquear los datos eliminados. Esto significa que los datos se tienen que conservar de forma que no se traten para ningún propósito, excepto para estar disponibles ante posibles requerimientos legales si es necesario. Hay excepciones a este bloqueo, como los datos de videovigilancia, denuncias internas no cursadas o casos exentos por la Autoridad de control.

Es importante informar a la persona afectada que, aunque sus datos han sido suprimidos, se conservarán en estado de bloqueo por un periodo legalmente definido, sin ser utilizados para otros fines.

12

Tratamientos específicos

12 Tratamientos específicos.

Tras poder comprender cómo se configuran los datos personales, sus tipos y cómo se tratan, es importante abordar los tratamientos específicos y habituales de las PYMES y autónomos que sirvan de guía para los mismos.

12.1 Datos sensibles y de alto riesgo.

Son aquellos en los que el tratamiento que versan sobre lo que el RGPD determina como datos especialmente protegidos, a los que se incluyen los datos genéticos y los datos biométricos.

Sobre los mismos el reglamento lo que determina es la prohibición de cualquier tratamiento que:

> *revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.*

Es decir, se trata de un numerus clausus donde a los datos ya conocidos como especialmente protegidos por la LOPD, se le suman dos nuevos:

- **Datos genéticos**: Entendiendo como los datos que revelen la genética de un individuo, concepto mucho más complejo de lo que puede parecer, toda vez que en función de distintas normas encontramos definiciones de dicho dato de genotipo, y que, a los efectos, dejaremos para otra ocasión, dada la especialidad del ámbito al que hace referencia.

- **Datos biométricos**: Son los datos referidos a la «autentificación biométrica» o «biometría informática» es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, para su autentificación, es decir, «verificar» su identidad a través de dichos rasgos físicos.

En todos estos casos, como ya hemos adelantado, el reglamento deja claro su prohibición de tratamiento, pero no en todo caso, sino que será posible en los siguientes casos, entre otros, siendo estos los más habituales:

- Exista consentimiento expreso del interesado;

- Derivado de obligaciones de tipo laboral o seguridad social del encargado o responsable;

- Interés vital del interesado;

- Que sean datos manifiestamente públicos por parte del interesado.

- Que el tratamiento sea necesario por razón de interés público, razones sanitarias generales o por medicina preventiva o laboral

En todos estos casos, el tratamiento será posible, eso sí, siempre con las precisiones indicadas al principio del presente apartado.

12.2 Personas Fallecidas.

El RGPD en su Considerando 27 señala que:

> *No se aplica a la protección de datos personales de personas fallecidas. Los Estados miembros son competentes para establecer normas relativas al tratamiento de los datos personales de éstas.*

En cuanto a que cada país miembro de la UE puede establecer criterios específicos en esta casuística, la LOPDGDD establece el derecho de acceso a los datos de personas fallecidas por parte de sus herederos, por lo que, en cualquier caso, podrán ejercitar estos derechos los albaceas o a las personas a las que el fallecido hubiera otorgado un mandato expreso para ello, y siempre y cuando que éste no lo hubiera prohibido expresamente o que así lo estableciera una ley. Así, podrán dirigirse al responsable o encargado del tratamiento para solicitar el acceso a los datos personales del fallecido y, en su caso, la rectificación o supresión de los mismos:

- Personas vinculadas al difunto por razones familiares o de hecho y sus herederos.
- Personas o instituciones designadas expresamente por el fallecido.
- Representantes legales de los menores o el Ministerio Fiscal, de oficio o a instancia de cualquier persona (física o jurídica) interesada.
- Representantes legales de las personas con discapacidad o su personal de apoyo.

12.3 Menores.

Si la persona afectada es menor de edad, el tratamiento de sus datos únicamente se puede fundamentar en la base de legitimación del consentimiento si tiene más de 14 años, a excepción de que se trate de

supuestos en que una ley exija la asistencia del titular de la potestad parental o tutela para llevar a cabo el acto o el negocio jurídico en el contexto del cual se solicita el consentimiento.

En este caso, es obligatorio informar en un lenguaje claro y sencillo para los menores de edad de qué manera se tratarán los datos personales. En caso de menores de edad de menos de 14 años, el tratamiento de datos fundamentado en el consentimiento requerirá el consentimiento del titular de la potestad parental o tutela.

12.4 Recursos Humanos y Selección de Candidatos.

El RGPD recoge en su artículo 88 la necesidad de regular los tratamientos de datos relativos al ámbito laboral, estableciendo que los Estados Miembros podrán desarrollar a través de normas o convenios colectivos, establezcan regulaciones específicas en cuanto a:

- A efectos de contratación de personal,
- ejecución del contrato laboral,
- incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo,
- gestión, planificación y organización del trabajo,
- igualdad y diversidad en el lugar de trabajo,
- salud y seguridad en el trabajo,
- protección de los bienes de empleados o clientes,
- así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral.

Una de las peculiaridades de la regulación en cuanto al tratamiento de datos de las personas dentro de una relación laboral es la existencia de un contrato laboral que actúa como base de legitimación y que desplaza al consentimiento (salvo supuestos específicos como podría ser la publicación de una foto de un trabajador en redes sociales, en donde posiblemente se haga necesario solicitar el consentimiento del trabajador si la publicación de su imagen no es directamente relevante para su trabajo o hacer una ponderación de derechos en caso de fundamentarse en el interés legítimo).

En cualquier caso, se hace necesario que el empleador pueda acreditar que se ha informado al trabajador convenientemente en cuanto al tratamiento de sus datos personales, pero en el caso de los candidatos a un puesto de trabajo al no existir una relación contractual previa, se hace indispensable obtener el consentimiento expreso e informado de los mismos, ya sea a través de la aceptación en un formulario o la firma de la política de privacidad de la empresa en cuanto al tratamiento de los datos de los candidatos, y en especial del plazo que conservarán los mismos y que en principio debería hasta que finalice el proceso de selección o de un año en todo caso, salvo que exista causa justificada para conservarlos durante más tiempo e informando siempre sobre ello al mismo.

En el caso de que la persona candidata pueda presentar su curriculum por cualquier vía, se hace necesario fijar procedimientos de información que supongan algún acuse, o confirmación que permita evidenciar que el candidato conocer las condiciones en las que se desarrollará el tratamiento relativa a su candidatura[7].

12.5 Videovigilancia.

La videovigilancia en el ámbito privado se rige por la Ley 5/2014, de 4 de abril, de Seguridad Privada (en adelante la LSP), así como en el Real

7 Se ha sancionado a empresas que han recibido un CV por una aplicación de mensajería instantánea como Whatssapp y no se ha contestado ni informado a la persona candidata sobre el tratamiento de sus datos. La multa de la AEPD ha sido en este caso de 2.000 euros.

Decreto 2364/1994, por el que se aprueba el Reglamento de Seguridad Privada (y que rige en todo lo que no sea contrario a la LSP).

Como la cuestión de la videovigilancia supone un tratamiento de datos específico y que adquiere muchos matices, la Agencia Española de Protección de datos tiene publicados diversos e imprescindibles documentos de apoyo:

- Instrucción 1/2006, de 8 de noviembre, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

- Guía de videovigilancia que analiza la utilización de los dispositivos destinados a videovigilancia tanto con fines de seguridad de personas, bienes e instalaciones, como para usos diferentes como el control de la actividad laboral, las grabaciones de sesiones de órganos colegiados o la captación de imágenes en eventos escolares. Dicha guía puede encontrarse en: https://www.aepd.es/media/guias/guia-videovigilancia.pdf.

Al igual que para el resto de los tratamientos de datos, deberá existir legitimación para el tratamiento de las imágenes de personas físicas identificadas e identificables que vayan a poder recabarse a través de las videocámaras, y la misma deberá fundamentarse en:

• Consentimiento del afectado o interesado, si bien no suele ser una base idónea debido a la dificultad de recabar el consentimiento de forma fehaciente o porque en muchas ocasiones dicho consentimiento no suele ser libre (caso de los trabajadores o de los clientes de un establecimiento).

• Una norma con rango de Ley que habilite el tratamiento como pueda ocurrir con la Ley de Seguridad Privada o el art. 20 del Estatuto de los Trabajadores para la finalidad de control laboral u horario.

• Cualquiera de las restantes bases de legitimación que recoge el Artículo 6 RGPD (necesario para la ejecución de un contrato, interés legítimo, o interés público).

La Instrucción 1/2006 de la AEPD establece un procedimiento concreto para informar a los interesados basándose en el sistema de información por capas:

A) En primer lugar, se hace necesario disponer del cartel reglamentario[8] en todos y cada uno de los accesos a la zona videovigilada en donde deberá identificarse al responsable del tratamiento de las imágenes, así como la base de legitimación, y en su caso, la ubicación de la segunda capa de información en donde pueda el interesado recabar la información adicional pertinente respecto al tratamiento.

8 Puede descargarse en la web de la AEPD: https://www.aepd.es/media/fichas/cartel-videovigilancia.pdf

B) La segunda capa de información puede recabarse de diversas formas, como pueden ser un folleto informativo o un enlace a la política de privacidad del responsable del tratamiento en donde debe de estar referida la información adicional con respecto al tratamiento de las cámaras de videovigilancia[9].

En cualquier caso, y además de la base de legitimación correspondiente, será necesario analizar la idoneidad, el principio de proporcionalidad entre la finalidad perseguida y la necesidad de la captación de imágenes o los principios de privacidad por diseño y privacidad por defecto, como pudieran ser supuestos más sensibles referidos a menores, aseos o baños, piscinas o gimnasios o simplemente el lugar de trabajo del personal (si se pueden captar las zonas de recreo o descanso, zonas en donde los usuarios puedan asearse o cambiarse de ropa, o simplemente que se capte la pantalla del dispositivo informático de trabajo de forma permanente).

Respecto a la videovigilancia en el ámbito empresarial, el Estatuto de los Trabajadores faculta al empresario para adoptar las medidas que estime más oportunas para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, que deberán guardar la consideración debida a la dignidad humana y tener en cuenta la capacidad real de los trabajadores con discapacidad.

En este sentido, los sistemas de videovigilancia para control empresarial sólo se adoptarán cuando exista una relación de proporcionalidad entre la finalidad perseguida y el modo en que se traten las imágenes y no haya otra medida más idónea.

Asimismo, se deberá informar personalmente a los trabajadores, o en su caso, a través de la representación sindical, por cualquier medio que garantice la recepción de la información.

9 Se hace recomendable visitar el apartado de la web de la AEPD: https://www.aepd.es/areas-de-actuacion/videovigilancia

La vigilancia en centros de trabajo no deberá abarcar lugares reservados al uso privado de los empleados o que no estén destinados a la realización de tareas de trabajo (como servicios, duchas, vestuarios, comedores o zonas de descanso) que establece el art. 89.2 de LOPDGDD, ni tampoco la grabación de sonidos al no superar el triple juicio de proporcionalidad.

La AEPD ha sancionado a empresas por disponer de una cámara de videovigilancia instalada en la zona de comedor de los empleados, o en otros casos por grabar audio y video en la videovigilancia al personal laboral.

12.6 Control laboral y horario.

Según el artículo 34.9 del Estatuto de los Trabajadores (ET), las empresas están obligadas a registrar la jornada de cada empleado de manera individual. Esta práctica no requiere el consentimiento del trabajador, ya que se basa en una obligación legal.

De acuerdo con el artículo 6.1.c del RGPD, el tratamiento de datos personales de las personas trabajadoras para el registro de jornada se considera necesario para cumplir con una obligación legal del responsable del tratamiento, en este caso, la empresa.

Sin embargo, la exención del consentimiento del trabajador no elimina la responsabilidad de las empresas de informar a los empleados sobre la existencia y finalidad del registro de jornada. Esto implica comunicar cómo y por qué se recopilan y tratan sus datos personales en el contexto del registro de la jornada laboral.

12.7 Contactos de Marketing y Publicidad.

El RGPD en los tratamientos de marketing y publicidad, prevalece la base de legitimación del consentimiento expreso para el envío de comunicaciones comerciales.

Ahora bien, se puede exceptuar el consentimiento cuando:

- Se trate de comunicaciones informativas, caso en el cual, no es necesario el consentimiento, ya que son aquellas que derivan de una relación jurídica previa y sin carácter comercial

- Que, en virtud del interés legítimo, se lleve a cabo una comunicación comercial para solicitar el consentimiento, pero obviamente, solo la primera para pedir dicho consentimiento a través de la misma.

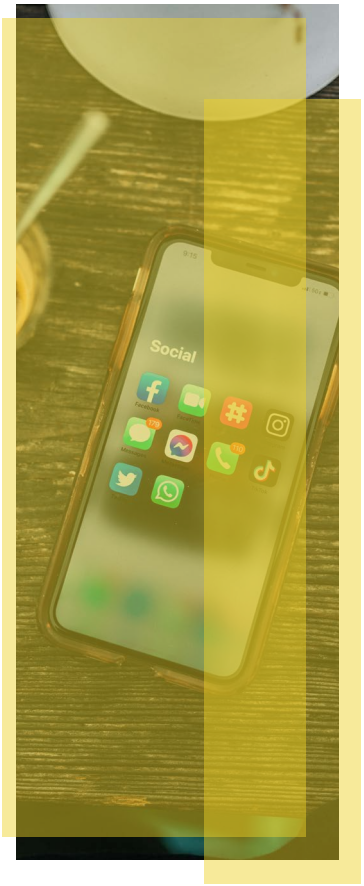
En el resto de los casos, si se llevan a cabo las comunicaciones comerciales las mismas pueden ser consideradas como no consentidas y, por tanto, SPAM, y pueden ser objeto de sanción por parte de la Agencia Española de Protección de datos.

12.8 Redes Sociales.

La relación entre la privacidad y las redes sociales por regla general, no ha sido demasiado complementaria desde la creación de estas últimas, hasta las polémicas surgidas con el caso Snowden y más recientemente con el caso de Cambridge Analítica o las recientes y cuantiosas sanciones económicas a empresas como TikTok (con una sanción de 345 millones de euros por tratar sin las debidas garantías datos de menores de edad) o Meta (con una sanción de 1.200 millones de euros por transferencias internacionales a EEUU sin las debidas garantías).

Por regla general, los responsables de tratamiento no suelen preocuparse de los datos personales referidos a sus seguidores en redes sociales, al

entender que la responsabilidad plena del cumplimiento de la normativa de protección de datos corresponde en cualquier caso a la red social y nunca al administrador de una página de empresa o similar.



Sin embargo, artículo 26 del RGPD, señala que cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento, serán considerados corresponsables del tratamiento; para ello dichas entidades corresponsables están obligadas suscribir un acuerdo que recoja sus respectivas funciones y responsabilidades en el cumplimiento de la normativa de protección de datos, en particular en cuanto al ejercicio de los derechos del interesado (que puede ejercerse frente a cualquiera de ellos) y a sus respectivas obligaciones de suministro de información. Es por ello que en algunas ocasiones podremos hablar de corresponsables del tratamiento, en cuanto a las obligaciones que pudieran tener los distintos responsables o empresas que participen en la elaboración de un tratamiento sujeto a una red social concreta, pero siempre y cuando suscriban un acuerdo en donde se regulen sus obligaciones, algo muy difícil hoy día.

En Junio de 2018, el Tribunal de Justicia de las Comunidades Europeas en el caso Wirtschaftsakademie Schleswig-Holstein, remarcó que el hecho de que un administrador de una página de fans utilice la plataforma ofrecida por Facebook para disfrutar de los servicios asociados a ésta, no le exime de cumplir sus obligaciones en materia de protección de datos personales y, por tanto, es tan responsable como Facebook de dicho tratamiento al establecer los fines del mismo. En efecto, dicho administrador de la página de fans participa, mediante su acción de configuración en determinar, en particular, su audiencia destinataria, así como los objetivos de gestión o de promoción de sus actividades, y, por lo tanto, en la determinación de los fines y de los medios del tratamiento de los datos personales de los visitantes de su página de fans.

En particular, el Tribunal de Justicia señala a este respecto que el administrador de la página de fans puede solicitar la obtención (de forma anonimizada) —y, por tanto, el tratamiento— de datos demográficos relativos a su audiencia destinataria (especialmente, de las tendencias en materia de edad, sexo, situación sentimental y/o profesión), información sobre el estilo de vida y los intereses de su audiencia (incluyendo información relativa a las compras y comportamiento de compras en línea de los visitantes de su página, así como a las categorías de productos o servicios que más les interesan), además de datos geográficos que permiten al administrador de la página de fans saber dónde efectuar promociones especiales u organizar eventos y, con carácter más general, dirigir de forma óptima su oferta de información.

En cuanto a los principios rectores relativos al RGPD, podemos evaluar:

a) La legitimación para el tratamiento de los datos por regla general podrá encontrarse en el consentimiento de los interesados.

b) En cuanto al principio de información, los proveedores de servicios de Redes Sociales así como los responsables de los tratamientos deben de informar a los usuarios proporcionándoles información clara y completa sobre las finalidades de cada tratamiento así como de las distintas maneras en que van a tratar los datos personales, en consonancia con lo establecido en nuestro artículo 5.1 de la LOPD, y en los artículos 13 y siguientes del RGPD, y especialmente en lo relativo a la identificación de cada responsable del tratamiento.

En los supuestos de recogida de datos online la AEPD ha considerado suficiente la existencia de una política de privacidad fácilmente accesible por el usuario como acreditación suficiente del cumplimiento del deber de información., dicha política podrá ser accesible desde un enlace perfectamente visible.

En este sentido el Grupo de trabajo del artículo 29 nos indica en dicho Dictamen 5/2009 que información a facilitar por los

proveedores del servicio de red social deberían informar a los usuarios de su identidad y de los distintos fines para los que tratan los datos personales, de conformidad con las disposiciones del artículo 10 de la Directiva relativa a la protección de datos, a saber, entre otras cosas:

- La utilización de los datos con fines de comercialización directa;
- La posible distribución de datos a categorías específicas de terceros;
- Una reseña de los perfiles: su creación y sus principales fuentes de datos;
- La utilización de datos sensibles.

c) En cuanto al consentimiento, el mismo como base de la legitimación, debe de prestarse mediante una clara acción activa o declaración por parte del interesado, siendo la práctica más extendida la marcación de una casilla en blanco (recordemos que esa casilla nunca podrá estar marcada por defecto) considerando la AEPD como prueba suficiente para la prestación del consentimiento, la acreditación de que la red social impide introducir los datos sin antes haber aceptado expresamente la política de privacidad relativa al tratamiento referido, vinculando en cuanto a las finalidades declaradas en dicha política de privacidad al responsable del tratamiento, y no pudiendo modificar sus términos sin obtener un nuevo y específico consentimiento informado por parte del interesado.

d) El tratamiento de los datos personales de menores se considerará lícito cuando tenga como mínimo 16 años, tal y como específicamente establece el artículo 8 RGPD, respecto a las "Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información"; si el niño es menor

de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó. El RGPD señala que los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años, siendo los 14 años la edad que se recoge en la normativa española. La AEPD señala que en caso de ponderación de derechos entre la normativa de protección de datos y la protección de los menores y la infancia, la balanza siempre ha de decantarse a favor del interés superior del niño, que debe prevalecer, en caso de intereses en conflicto, incluso frente al derecho a la protección de datos.

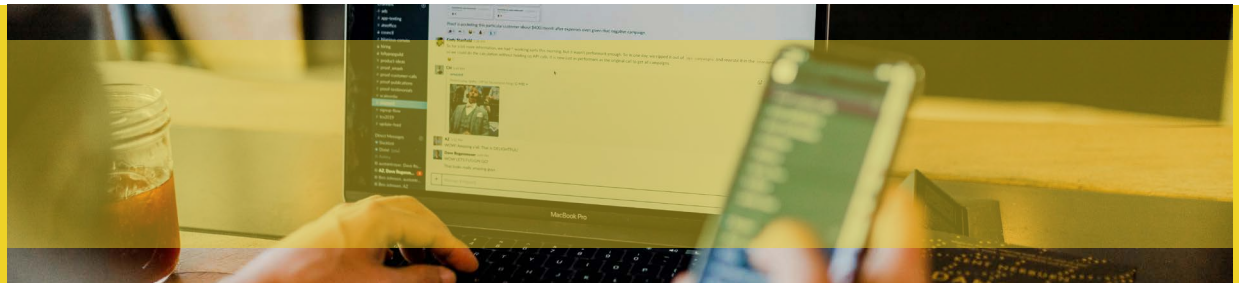
e) La información se configura en el RGPD como un derecho fundamental de los interesados, y encuentra su regulación en los artículos 12, 13 y 14 del mismo, donde se encuentran definidos los derechos de acceso, rectificación, cancelación, supresión/olvido, limitación y portabilidad; el ejercicio de estos derechos no debe estar restringido únicamente a los usuarios activos de la red social correspondiente, sino que deben de estar disponibles para cualquier persona cuyos datos se traten, a través de un medio sencillo y gratuito para ejercer dichos derechos, independientemente de que la persona sea usuario de la red social o no, ya que ocurre en muchas ocasiones que existen afectados que no son usuarios de redes sociales.

f) Es necesario evaluar la necesidad u obligatoriedad de disponer de un Delegado de Protección de Datos más allá de los casos reglamentariamente observados por la ley, ya que muy posiblemente nos encontremos ante un tratamiento especial de datos tanto a gran escala y/o que implique una observación sistemática de los interesados, lo cual a efectos prácticos y ante posibles inspecciones de la AEPD, será difícilmente justificable la ausencia de un delegado debidamente nombrado en muchas ocasiones.

g) Será necesario evaluar los posibles riesgos de cada red social, a la hora de gestionar los distintos análisis de riesgos en cuanto al tratamiento referido a REDES SOCIALES y especialmente a las medidas técnicas, jurídicas y organizativas adecuadas, como pueda ser una violación de datos que deba de ser comunicada a la autoridad de control.

h) En último lugar, es sumamente importante formar y, sobre todo, concienciar al personal recomendando con respecto a los empleados que gestionan las redes sociales, además de firmar su correspondiente contrato de trabajo o su conveniente documento de funciones y obligaciones o disponiendo de un documento específico respecto a sus obligaciones en relación con el especial cuidado que se ha de asumir por ser sus publicaciones plenamente accesibles por terceros que sigan las cuentas de redes sociales.

Cabe la posibilidad de la empresa responsable externalice la gestión de sus redes sociales a un Community Manager (en adelante CM), adoptando el CM el rol de encargado de tratamiento y estando obligado a firmar el correspondiente contrato de encargado de tratamiento. En cualquier caso, y en base especialmente al RGPD, el responsable debe adoptar las medidas oportunas, incluida la elección de encargados de forma que se garantice, y pueda demostrarlo, que el tratamiento se realiza conforme al RGPD, es decir, se exige una responsabilidad activa a la hora de elegir un CM o tercero que gestione la presencia en redes sociales.



Para que la relación entre responsable y encargado del tratamiento se ajuste a la Ley, es preciso que se cumplan los requisitos recogidos en el art. 33 del proyecto de la LOPD, y que el acceso a los datos por el CM se

efectúe con la exclusiva finalidad de prestar un servicio al responsable del fichero, esto es, la gestión de la imagen corporativa de la entidad en redes sociales, así como que dicha relación de servicios se encuentre contractualmente establecida, exigiendo el RGPD en su art. 28.1 que las relaciones entre un responsable y un encargado del tratamiento se regulen en un contrato específico.

Es por ello que en lo referido a dicho contrato se recomienda, siguiendo las exigencias del RGPD y del principio de responsabilidad activa:

A) Una descripción detallada de las prestaciones a realizar y la finalidad dentro del tratamiento de datos en redes sociales.

B) Señalar las redes sociales en las que se va a realizar un tratamiento de datos (Facebook, Twitter, Instagram, TikTok, Threads, etc..) y en base a ellas, señalar convenientemente a cuáles de ellas va a tener acceso el encargado de tratamiento.

C) Que el encargado del tratamiento únicamente trate los datos conforme a las instrucciones del responsable del tratamiento.

D) Indicar expresamente a qué tratamiento titularidad del responsable va a acceder el encargado de tratamiento. Normalmente se recomienda denominar al tratamiento específico como “REDES SOCIALES”, con el objetivo de plasmarlo debidamente en el contrato de encargado de tratamiento o en el registro de tratamientos si procede.

E) Si el servicio prestado por el encargado del tratamiento va a tener, o no, carácter remunerado.

F) Si la prestación va a ser temporal o indefinida.

G) Que el encargado del tratamiento de datos no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas, salvo previa indicación expresa del responsable del fichero.

H) La posibilidad de subcontratación de los servicios o su prohibición.

I) La obligación de guardar secreto respecto a los datos objeto de tratamiento durante y una vez finalizada ésta.

J) Establecer qué medidas de seguridad se imponen a ese tratamiento "REDES SOCIALES" una vez que se hayan evaluados los riesgos pertinentes, dependiendo de la finalidad de la red social o de la finalidad de la misma. Si por ejemplo la presencia online se va a realizar en Facebook o Twitter, suele ser exigible establecer unas medidas de Seguridad diferentes a si van a tratarse datos sensibles o no, o si pertenecen a grupos específicos que merezcan una especial protección. Todo ello se debe a que este tipo de tratamientos permiten obtener una información adicional sobre el usuario de la red social, a partir de los datos que se incluyen, pudiendo obtener en un momento dado un perfil muy detallado de su situación económica o familiar, su ideología política, sus creencias religiosas, así como aficiones, hábitos o preferencias de compra, por no entrar en materia de datos de salud o víctimas de cualquier tipo delictivo. En el caso del RGPD será necesario atender a los principios de responsabilidad activa.

K) Recibir una formación específica en cuanto a sus funciones y obligaciones no únicamente en protección de datos, sino igualmente en su condición específica de Community Manager. Entrando en materia de responsabilidad activa o Compliance Digital, es también recomendable que dicha formación incluya formación y sensibilización en materia de derechos fundamentales (libertad de expresión, honor y propia imagen personal y familiar) así como respeto a la propiedad intelectual e industrial tanto propia como de terceros, tipos penales relacionados e incluso en materia de publicidad y competencia desleal.

L) Reportar de cualquier tipo de incidencia, brechas de seguridad o violaciones de datos que pudiera afectar al cumplimiento de la normativa, al delegado de protección de datos o responsable competente, para adoptar las medidas preventivas y oportunas que

permitan paliar el daño o al menos no incrementarlo. Recordad que el RGPD se establece la obligación en determinados supuestos de brechas de seguridad de informar por parte del responsable del fichero en un plazo no superior a las 72 horas desde que se tenga conocimiento de la misma. Es por eso que la eficacia a la hora de implementar los tiempos es absolutamente fundamental.

M) Disponer de un canal de comunicación ágil y eficaz con el delegado de protección de datos, responsable de seguridad, responsable competente o asesor externo con el fin de poder consultar sobre las posibles dudas que pueda tener en cuanto a la publicación o tratamiento de un contenido que pueda afectar a la privacidad de los usuarios.

N) Establecer si puede contestar a los derechos LOPD a través de las redes sociales, o los nuevos derechos propios del RGPD, o si ha de remitir a los cauces más habituales, ya que muchas veces los usuarios piden a través de las redes sociales que se rectifiquen datos o incluso que se borren.

O) Establecer que, una vez finalizada la prestación, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato objeto del tratamiento. El encargado deberá conservar bloqueados los datos en tanto pudieran derivarse responsabilidades con ocasión de la prestación del servicio.

Por todo ello es necesario revisar los contratos pertinentes con las Agencias de comunicación o los CM que las PYMES y autónomos contraten para la gestión de sus redes sociales.

12.9 Cookies.

Por último, en referencia con los tratamientos con especial relevancia en el ámbito de la privacidad de los usuarios debemos pararnos en uno que

por sí mismo, no es un tratamiento propiamente, sino que hemos querido englobar en el mismo los tratamientos que se hacen a través de dicha herramienta, que son las cookies.

Lo primero, es definir a que hacemos referencia con el concepto cookies, y las mismas las podemos definir como señala la Wikipedia:

Un archivo creado por un sitio web que contiene pequeñas cantidades de datos y que se envían entre un emisor y un receptor. En el caso de Internet el emisor sería el servidor donde está alojada la página web y el receptor es el navegador que usas para visitar cualquier página web

Dicho archivo tiene como finalidad identificar al usuario y conocer cuál es la actividad que lleva a cabo a través de su navegador, es decir, rastrear en mayor o menor medida su actividad.

La información que almacenan y comunican a la web, es, por un lado, la IP del usuario, que, conforme a la AEPD, debe ser considerada como un dato personal (Con todas las salvedades que eso puede tener), y junto a ella, la actividad del propio usuario en la web, o incluso, en función del tipo de cookie, en otras webs.

Existen distintos tipos de cookies, desde las meramente identificativas, a aquellas que son de seguridad, de inicio de sesión, o de publicidad, pero a lo que nos afecta nos centraremos en principalmente dos, las de identificación y las de publicidad, y en función de cómo y para que se lleve a cabo ese rastreo, dará lugar a distintos tratamientos, pero los principales que se van a llevar a cabo van a ser siempre dos, el de analítica de la web y el de suministro de publicidad en la web, o publicidad comportamental.

En cualquier caso, y con respecto a ello, se debe identificar en todo momento, el tipo de cookies que se utilizan y su finalidad, es decir, para que se usan, el responsable de su tratamiento, así como recabar el consentimiento para su instalación, o al menos, su información, distinguiendo en función del tipo de tratamiento y su importancia para

ello en caso de que estén exentas del consentimiento por tratarse de cookies técnicas o por corresponder a un servicio expresamente solicitado por la persona interesada.

La AEPD ha actualizado en 2023 su Guía en sobre el uso de cookies con el fin de alinearse con las Directrices 03/2022 sobre patrones engañosos del Comité Europeo de Protección de Datos. Esta actualización, que contó con la colaboración de varios sectores, busca garantizar que las opciones para aceptar o rechazar cookies sean igualmente accesibles y claras, destacando su posición, color y tamaño.

Cambios importantes en la Guía de Cookies 2023 son:

- Se resalta la necesidad de que el usuario puede aceptar, rechazar o modificar las cookies en cualquier momento y de forma clara, sencilla y transparente. Por ello se recomienda la utilización de un

  Gestor de Consentimiento de Cookies (CMP) como primera capa de información en donde el usuario pueda indistintamente acceder a los botones de ACEPTAR – RECHAZAR – MODIFICAR cookies, así como un enlace a una segunda capa de información que configure la Política de Cookies de la web y se informe de manera más extensa.

- El usuario debe tener la opción de modificar las cookies en cualquier momento, no únicamente en el primer acceso a la web, por ello es recomendable la instalación de un botón o acceso que permita realizar los cambios oportunos en todo momento.

- Cookies de Personalización: Si el usuario personaliza estas cookies (como el idioma o la moneda), se consideran técnicas y no requieren consentimiento. Pero si es el editor de la web quien las personaliza basándose en información del usuario, debe informar claramente y ofrecer la opción de aceptarlas o rechazarlas.

- Muros de Cookies: La Guía clarifica que el acceso a servicios web no debe condicionarse a la aceptación de cookies. Si se rechazan las cookies, debe haber una alternativa de acceso al servicio, que no necesariamente tiene que ser gratuita.

Las PYMES y autónomos tienen de plazo hasta el 11 de enero de 2024 para implementar estos requerimientos respecto al uso de cookies[10].

12.10 Tratamientos referidos a la Inteligencia Artificial (IA).

Cuando se utiliza la Inteligencia Artificial (IA) en operaciones de tratamiento de datos personales, es crucial distinguir entre la finalidad del tratamiento y los medios (como los sistemas de IA) utilizados para implementarlo. En este contexto, el responsable del tratamiento de datos decide cómo se emplea la IA:

Decisión Automática o Supervisión Humana: El responsable puede permitir que un sistema de IA tome decisiones automáticamente o puede optar por incluir supervisión humana, donde una persona toma la decisión final basada en la información proporcionada por la IA.

Elección del Responsable: No es inherente a la IA tomar decisiones automatizadas; es una elección hecha por el responsable del tratamiento de datos. La IA es simplemente una herramienta que puede ser utilizada de diferentes maneras.

Es esencial que los responsables del tratamiento de datos personales comprendan y consideren cuidadosamente estas opciones al implementar sistemas de IA. La elección entre decisiones automatizadas o supervisión humana tiene implicaciones significativas en términos de cumplimiento con la normativa, incluyendo los derechos de los interesados y la transparencia del tratamiento.

10 En cualquier caso, se recomienda el estudio de la Guía de Cookies 2023 de la AEPD disponible en https://www.aepd.es/documento/guia-cookies.pdf

13

Manual de autoevaluación en materia de protección de datos.

13 Manual de autoevaluación en materia de protección de datos.

AUTOEVALUACIÓN RGPD PARA PYMES			
	✓	✘	No Procede
REGISTRO DE ACTIVIDADES DE TRATAMIENTO			
1. ¿Están identificados los tratamientos de datos personales?			
2. ¿Están recogidos los tratamientos del apartado anterior en un ***registro de actividades de tratamiento de forma interna y por escrito***, de forma que estén a disposición autoridad de control que pueda requerir esa información?			
3. ¿Dispone el encargado de tratamiento de un registro por escrito de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable?			

PRINCIPIOS DEL RGPD			
4. LICITUD, LEALTAD Y TRANSPARENCIA: ¿Los datos personales son tratados respecto al interesado de manera lícita, leal y transparente?			
5. LIMITACIÓN DE LA FINALIDAD: ¿Los datos personales de cada tratamiento se han recogido con una finalidad determinada, explícita y legítima?			
6. PRINCIPIO DE MINIMIZACIÓN: ¿Los datos personales que se recogen son los datos realmente necesarios adecuados, pertinentes y limitados a la finalidad del tratamiento sin recogerse en ningún caso información excesiva del interesado?			
7. PRINCIPIO DE EXACTITUD: ¿Los datos personales son exactos y están puestos al día y actualizados y además se han adoptado las medidas necesarias para que los que sean inexactos se supriman o se rectifiquen?			
8. LIMITACIÓN DEL PLAZO: ¿Los datos personales se tratan durante un plazo determinado y limitado en el tiempo?			

LEGITIMACIÓN DEL TRATAMIENTO			
9. Cada tratamiento dispone de una base de legitimación (***consentimiento, contrato o precontrato, obligación legal, interés vital, interés público o interés legítimo***).			
10. ¿La empresa verifica que ninguno de sus tratamientos se basa después del 25 de Mayo de 2018 en el consentimiento que no sea expreso?			
DERECHOS DE LOS INTERESADOS			
11. ¿Existe un procedimiento para que las personas interesadas puedan ejercitar los derechos que les reconoce la normativa?			
ENCARGADOS DE TRATAMIENTO			
12. ¿Se dispone de una relación de encargados de tratamiento actualizada y en formato electrónico?			
13. ¿La PYME ha verificado con algún tipo de procedimiento que los encargados de tratamiento que ha contratado cumplen con el RGPD y que disponen de un contrato de encargo de datos firmado con cada uno de ellos?			

14. ¿La PYME o el autónomo dispone a la hora de contratar a un nuevo encargado de tratamiento de un protocolo para verificar que dicho encargado es fiable o de confianza?			
MEDIDAS DE SEGURIDAD			
15. ¿La PYME dispone de un protocolo de notificación de brechas de seguridad en un periodo inferior a 72 horas?			
16. ¿La PYME dispone de medidas técnicas y organizativas que garanticen la confidencialidad, integridad, disponibilidad y resiliencia de los tratamientos?			
17. ¿Sabe la PYME cuando tiene que llevar a cabo una PIA?			
DELEGADO DE PROTECCIÓN DE DATOS (DPD)			
18. ¿Se ha nombrado un DPD?			
19. En caso de que se haya nombrado un DPD, ¿dispone el mismo de práctica verificable en el derecho y en formación en materia de protección de datos?			

20. En caso de que se haya nombrado un DPD, ¿se informa convenientemente del medio para que cualquier interesado pueda contactar con el DPD?			
21. En caso de que se haya nombrado un DPD, ¿se ha notificado a la Agencia Española de Protección de Datos?			
22. En caso de que se haya nombrado un DPD, ¿se ha verificado que su puesto no incurre en conflicto de intereses como puede ocurrir por ejemplo si se nombra como tal al Responsable de Informática?			
INFORMACIÓN			
23. ¿La PYME ha revisado que cada tratamiento dispone de cláusulas de información actualizadas al RGPD?			
24. ¿Se utiliza el sistema de primera y segunda capa para informar a los interesados acerca del tratamiento de sus datos?			
25. ¿En caso de existir cámaras de videovigilancia se informa mediante el cartel preceptivo de la AEPD en un lugar previo a la captación de modo que el mismo sea fácilmente identificable por los afectados?			

FORMACIÓN Y SENSIBILIZACIÓN AL PERSONAL			
26. ¿Se puede demostrar que se ha informado a todo el personal de sus funciones y obligaciones en materia de protección de datos?			
27. ¿Existe un protocolo BYOD por ejemplo en el uso de dispositivos móviles que no pertenezcan a la empresa o al responsable?			
28. Se ha verificado que, en caso de incidencia o brecha de seguridad, ¿el personal tiene conocimiento de como notificar la misma en cuanto tenga conocimiento efectivo?			
29. En caso de que cualquier trabajadora o trabajador de la entidad tenga dudas acerca del cumplimiento en materia de protección de datos, ¿sabe cómo ponerse en contacto con el DPD o con la persona que coordine el cumplimiento de la LOPD?			
30. ¿Se forma y se sensibiliza a todo el personal en cuanto al cumplimiento de la protección de datos de forma periódica y además existen evidencias de dicha formación?			

14

Modelos.

14 Modelos

14.1 Ejemplo de primera capa de información para tratamiento CLIENTES:

Información básica sobre Protección de datos	
Responsable del tratamiento:	PYME o Autónomo
Finalidad:	Gestión de clientes
Legitimación:	Ejecución de un contrato o precontrato.
Destinatarios:	Están previstas cesiones de datos a: Agencia Tributaria; Entidades financieras. No se cederán datos a otros terceros, salvo obligación legal.
Derechos:	Tiene derecho a acceder, rectificar y suprimir los datos, así como otros derechos, indicados en la información adicional, que puede ejercer dirigiéndose a la dirección del responsable del tratamiento
Procedencia:	El propio interesado.
Información adicional:	Política de Privacidad en la web de la Pyme o autónomo

Asimismo, solicitamos su autorización para ofrecerle productos y servicios relacionados con los contratados y fidelizarle como cliente.” (Si marca NO en ningún caso se le puede mandar publicidad.

SI ☐
NO ☐

14.2 Ejemplo de segunda capa o información para CLIENTES:

Información completa sobre Protección de Datos

1. ¿Quién es el responsable del tratamiento de sus datos?

Datos identificativos de la PYME o autónomo

2. ¿Con qué finalidad tratamos sus datos personales?

Tratamos la información que nos facilitan las personas interesadas con el fin de gestionar los servicios contratados por los clientes, así como la gestión administrativa, contable y fiscal de los mismos. No se van a tomar decisiones automatizadas en base de datos proporcionados.

3. ¿Por cuánto tiempo conservaremos sus datos?

Los datos proporcionados se conservarán mientras se mantenga la relación comercial o durante el tiempo necesario para cumplir con las obligaciones legales y atender las posibles responsabilidades que pudieran derivar del cumplimiento de la finalidad para la que los datos fueron recabados.

4. ¿Cuál es la legitimación para el tratamiento de sus datos?

Ejecución de un contrato: Realizar la gestión administrativa, contable y

fiscal de los servicios solicitados.

5. ¿A qué destinatarios se comunicarán sus datos?

Los datos se comunicarán a los siguientes destinatarios:

- Agencia Tributaria, con la finalidad de Cumplir con las obligaciones legales.

- Entidades financieras, con la finalidad de realizar los cargos correspondientes.

6. Transferencias de datos a terceros países.

No están previstas transferencias de datos a terceros países.

7. ¿Cuáles son sus derechos cuando nos facilita sus datos?

Cualquier persona tiene derecho a obtener confirmación sobre si estamos tratando, o no, datos personales que les conciernan.

Las personas interesadas tienen derecho a acceder a sus datos personales, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines que fueron recogidos, así como a la portabilidad de sus datos en los supuestos en los que sea posible.

Los interesados podrán solicitar la limitación del tratamiento de sus datos cuando sea posible, en cuyo caso únicamente los conservaremos para el ejercicio o la defensa de reclamaciones.
En determinadas circunstancias de tratar los datos, salvo por motivos legítimos imperiosos, o el ejercicio o la defensa de posibles reclamaciones.

Cuando se realice el envío de comunicaciones comerciales utilizando como base jurídica el interés legítimo del responsable, el interesado podrá oponerse al tratamiento de sus datos con ese fin.

Igualmente tiene derecho a retirar el consentimiento otorgado para cualquier finalidad concreta en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.

Puede presentar una reclamación ante la Agencia Española de Protección de Datos competente a través de su sitio web: www.agpd.es.

14.3 Ejemplo de segunda capa o información para CONTACTOS:

Por medio de la presente, y con motivo de la entrada en vigor del Reglamento General de Protección de Datos, te informamos de nuestra nueva política de privacidad:

¿Quién es el responsable del tratamiento de sus datos?

Datos de contacto de la PYME o autónomo
protecciondedatos@pyme.es

¿Con que finalidades vamos a tratar tus datos personales?

Gestionar la recepción y tramitación de las consultas y comunicaciones recibidas y poder dar respuesta a las mismas.

¿Cuál es la legitimación para el tratamiento de tus datos?

La base legal principal para el tratamiento de sus datos es el consentimiento.

¿Durante cuánto tiempo vamos a mantener los datos personales?

El tiempo necesario para dar respuesta a su consulta.

¿A qué destinatarios se comunicarán tus datos?

Los datos no serán cedidos a terceros salvo administraciones o jueces y tribunales con competencia en la materia.

¿Cuáles son tus derechos en relación con el tratamiento de datos?

Cualquier persona tiene derecho a obtener confirmación sobre si en Empresa X estamos tratando, o no, datos personales que les conciernan.

Las personas interesadas tienen derecho a acceder a sus datos personales, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines que fueron recogidos, así como a la portabilidad de sus datos en los supuestos en los que sea posible.

Los interesados podrán solicitar la limitación del tratamiento de sus datos cuando sea posible, en cuyo caso únicamente los conservaremos para el ejercicio o la defensa de reclamaciones.

En determinadas circunstancias de tratar los datos, salvo por motivos legítimos imperiosos, o el ejercicio o la defensa de posibles reclamaciones.

Cuando se realice el envío de comunicaciones comerciales utilizando como base jurídica el interés legítimo del responsable, el interesado podrá oponerse al tratamiento de sus datos con ese fin.

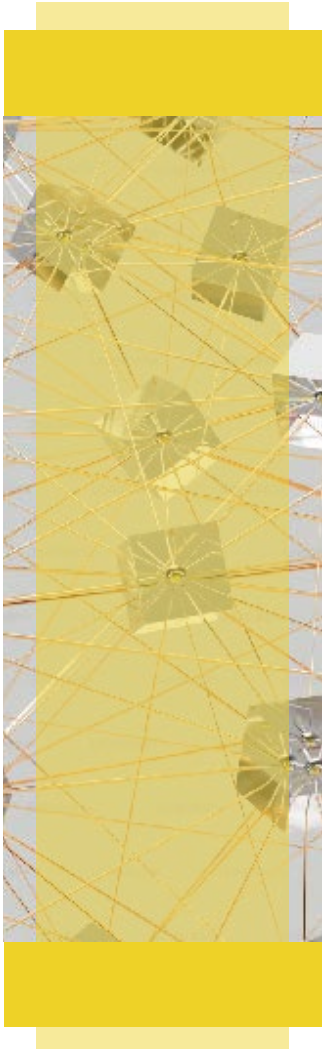
Igualmente tiene derecho a retirar el consentimiento otorgado para cualquier finalidad concreta en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.

Puede presentar una reclamación ante la Agencia Española de Protección de Datos competente a través de su sitio web: www.agpd.es.

14.4 Modelo de Registro de Actividades de Tratamiento.

La herramienta "Facilita RGPD" de la Agencia Española de Protección de Datos (AEPD) es un recurso inicial para ayudar a responsables como PYMES o autónomos que sean responsables de tratamientos de bajo riesgo a comprender y abordar las obligaciones del RGPD y la LOPDGDD. Sin embargo, la mera obtención de documentos a través de esta herramienta no garantiza el cumplimiento automático de estas normativas. Es esencial que cada responsable y encargado del tratamiento de datos personales realice adaptaciones específicas, considerando los riesgos que dichos tratamientos puedan implicar para los derechos y libertades de las personas.

Facilita RGPD, gratuita y fácil de usar, es adecuada para tratamientos de datos personales de bajo riesgo, como los de clientes, proveedores o recursos humanos. No es aplicable para tratamientos de alto riesgo, como puedan ser los datos de salud, de menores o datos biométricos como los referidos al control laboral con reconocimiento facial o huella dactilar. La herramienta ayuda a evaluar si se cumple con los requisitos del RGPD y proporciona documentos útiles como cláusulas informativas y contractuales, registros de actividades de tratamiento y medidas de seguridad mínimas.



Es importante recordar que los documentos generados por Facilita RGPD deben personalizarse y actualizarse según las circunstancias específicas de cada tratamiento de datos, y su uso es solo un punto de partida hacia el cumplimiento del RGPD. Es por ello por lo que añadimos aquí el modelo de registro de tratamientos que proporciona la Herramienta Facilita LOPD de la AEPD.

Cualquier PYME o autónomo puede dirigirse a la web de la AEPD en el apartado de la herramienta FACILITA RGPD para poder elaborar su propio registro de tratamientos siempre y cuando los mismos sean tratamientos de bajo riesgo[11].

Tratamiento: **Gestión de Clientes**

a) Responsable del tratamiento	Datos identificativos de la Pyme o autónomo
b) Finalidad del tratamiento	Gestión de la relación con los clientes
c) Categorías de interesados	Clientes: Personas con las que se mantiene una relación comercial como clientes
d) Categorías de datos	Los necesarios para el mantenimiento de la relación comercial. Facturar, enviar publicidad postal o por correo electrónico De identificación: nombre y apellidos, NIF, dirección postal, teléfonos, e-mail Características personales: estado civil, fecha y lugar de nacimiento, edad, sexo, nacionalidad Datos académicos Datos bancarios: para la domiciliación de pagos
e) Categorías de destinatarios	Agencia Estatal de Administración Tributaria Bancos y entidades financieras
f) Transferencias internacionales	No está previsto realizar transferencias internacionales

11 Disponible en https://www.aepd.es/guias-y-herramientas/herramientas/facilita-rgpd

g) Plazo de supresión	Los previstos por la legislación fiscal respecto a la prescripción de responsabilidades
h) Medidas de seguridad	Las reflejadas en el ANEXO MEDIDAS DE SEGURIDAD (a definir por la PYME o el autónomo)

Tratamiento: **Potenciales Clientes y/o contactos**

a) Responsable del tratamiento	Datos identificativos de la Pyme o autónomo
b) Finalidad del tratamiento	Gestión de la relación con los potenciales clientes
c) Categorías de interesados	Potenciales clientes: Personas con las que se busca mantener una relación comercial como clientes
d) Categorías de datos	Los necesarios para la promoción comercial de la empresa De identificación: nombre y apellidos y dirección postal, teléfonos, e-mail
e) Categorías de destinatarios	No se contempla
f) Transferencias internacionales	No está previsto realizar transferencias internacionales.
g) Plazo de supresión	Un año desde el primer contacto
h) Medidas de seguridad	Las reflejadas en el ANEXO MEDIDAS DE SEGURIDAD (a definir por la PYME o el autónomo)

Tratamiento: **Gestión de Personal**

a) Responsable del tratamiento	Datos de la Pyme o autónomo
b) Finalidad del tratamiento	Gestión de la relación laboral con los empleados
c) Categorías de interesados	Empleados: Personas que trabajan para el responsable del tratamiento
d) Categorías de datos	Los necesarios para el mantenimiento de la relación comercial. Gestionar la nómina De identificación: nombre, apellidos, número de Seguridad Social, dirección postal, teléfonos, e-mail Características personales: estado civil, fecha y lugar de nacimiento, edad, sexo, nacionalidad y porcentaje de minusvalía Datos académicos Datos profesionales Datos bancarios, para la domiciliación del pago de las nóminas
e) Categorías de destinatarios	Agencia Estatal de Administración Tributaria Instituto Nacional de la Seguridad Social Bancos y entidades financieras [Otros posibles destinatarios]
f) Transferencias internacionales	No está previsto realizar transferencias internacionales
g) Plazo de supresión	Los previstos por la legislación fiscal y laboral respecto a la prescripción de responsabilidades
h) Medidas de seguridad	Las reflejadas en el ANEXO MEDIDAS DE SEGURIDAD (a definir por la PYME o el autónomo)

Tratamiento: **Selección de Personal**

a) Responsable del tratamiento	Datos de la Pyme o autónomo
b) Finalidad del tratamiento	Gestión de la relación con las personas candidatas a una oferta de empleo
c) Categorías de interesados	Candidatos: Personas que desean trabajar para el responsable del tratamiento
d) Categorías de datos	Los necesarios para gestionar los currículums de posibles futuros empleados De identificación: nombre, apellidos, dirección postal, teléfonos, e-mail Características personales: estado civil, fecha y lugar de nacimiento, edad, sexo, nacionalidad y otros excluyendo datos de raza, salud o afiliación sindical Datos académicos Datos profesionales
e) Categorías de destinatarios	No se contempla el envío de datos de carácter personal a ningún destinatario
f) Transferencias internacionales	No está previsto realizar transferencias internacionales
g) Plazo de supresión	Un año desde la presentación de la candidatura
h) Medidas de seguridad	Las reflejadas en el ANEXO MEDIDAS DE SEGURIDAD (a definir por la PYME o el autónomo)

Tratamiento: **Proveedores**

a) Responsable del tratamiento	Datos de la Pyme o autónomo.
b) Finalidad del tratamiento	Gestión de la relación con los proveedores
c) Categorías de interesados	Proveedores: Personas con las que se mantiene una relación comercial como proveedores de productos y/o servicios
d) Categorías de datos	Los necesarios para el mantenimiento de la relación laboral De identificación: nombre, NIF, dirección postal, teléfonos, e-mail Datos bancarios: para la domiciliación de pagos
e) Categorías de destinatarios	Agencia Estatal de Administración Tributaria Bancos y entidades financieras [Otros posibles destinatarios]
f) Transferencias internacionales	No está previsto realizar transferencias internacionales
g) Plazo de supresión	Los previstos por la legislación fiscal respecto a la prescripción de responsabilidades
h) Medidas de seguridad	Las reflejadas en el ANEXO MEDIDAS DE SEGURIDAD (a definir por la PYME o el autónomo)

Tratamiento: **Videovigilancia**

a) Responsable del tratamiento	Datos de la Pyme o autónomo
b) Finalidad del tratamiento	Seguridad de las personas y bienes
c) Categorías de interesados	Personas que accedan o intenten acceder a las instalaciones
d) Categorías de datos	Imágenes
e) Categorías de destinatarios	Fuerzas y Cuerpos de Seguridad
f) Transferencias internacionales	No está previsto realizar transferencias internacionales
g) Plazo de supresión	Un mes desde su grabación
h) Medidas de seguridad	Las reflejadas en el ANEXO MEDIDAS DE SEGURIDAD (a definir por la PYME o el autónomo)

CEA
Confederación de Empresarios de Andalucía

FINANCIADO POR

Andalucía TRADE

Junta de Andalucía
Consejería de Presidencia, Interior, Diálogo Social y Simplificación Administrativa
Consejería de Economía, Hacienda y Fondos Europeos

+CEA mpresas

COLABORAN

CEC CONFEDERACIÓN EMPRESAS PROVINCIA DE CÁDIZ

CES CONFEDERACIÓN DE EMPRESARIOS DE SEVILLA

CEGE CONFEDERACION GRANADINA DE EMPRESARIOS

Asempal CONFEDERACIÓN EMPRESARIAL DE LA PROVINCIA DE ALMERÍA

CEJ CONFEDERACION DE EMPRESARIOS DE JAEN

CECO CENTRO DE FORMACIÓN, INICIATIVA Y APOYO A LA ACTIVIDAD EMPRESARIAL

FOE Federación Onubense de Empresarios

CEM CONFEDERACIÓN DE EMPRESARIOS DE MÁLAGA