Sabadell
Hub Empresa

17 AÑOS PYME LEGAL

Protección de Datos

¿está preparada tu empresa para cumplir con la normativa?

Mayo 2023

ÍNDICE

01 INTRODUCCIÓN

02 ÁMBITO APLICACIÓN/CONTEXTO

03 SANCIONES

04 DEFINICIONES

05 OBLIGACIONES DEL RESPONSABLE

06 LEGITIMACIÓN E INFORMACIÓN

07 TRABAJADORES

08 TRATAMIENTO DE DATOS POR TERCEROS

09 DERECHOS DE LOS INTERESADOS

10 DERECHOS DIGITALES

11 TRANSFERENCIAS INTERNACIONALES DE DATOS

12 BRECHAS DE SEGURIDAD

13 DELEGADO DE PROTECCIÓN DE DATOS

14 MEDIDAS DE SEGURIDAD

15 PÁGINAS WEB

1.
PymeLegal - Introducción

Sabadell Hub Empresa

10 AÑOS PYME LEGAL

HOLA

PymeLegal es una consultora especializada en protección de datos y propiedad intelectual.

En 2013 desarrollamos la plataforma **www.pymelegal.es** para la adaptación a la normativa de **pymes y autónomos**.

Somos un **equipo multidisciplinar integrado por abogados expertos en privacidad e ingenieros**, con una amplia experiencia en este ámbito y formados en despachos de reconocido prestigio.

Finalistas de la primera edición del programa de aceleración de empresas legaltech '**Cuatrecasas Acelera**'.

Certificados como Delegados de Protección de Datos (DPD) según el esquema de la AEPD.

¿QUÉ LE APORTA A TU NEGOCIO CUMPLIR CON LA NORMATIVA?

- Genera confianza y credibilidad
- Evita elevadas sanciones económicas
- Diferenciación frente a competidores
- Protección de los activos del negocio
- Potencia tu marca

Sabadell Hub Empresa

PYME LEGAL

SERVICIOS
ESPECIALIZADOS

Sabadell Hub Empresa

PYME LEGAL

PROTECCIÓN
DE DATOS Y MARCA

Protección de Datos (RGPD-LOPDGDD) y LSSICE

Delegado de Protección de Datos (DPD)

Redacción de textos legales para web, ecommerce y apps

Formación online Academia PymeLegal

Registro de patentes y marcas

Recuperación de dominios online

Regulación legal de campañas de marketing online

Revisión y redacción de contratos de ámbito tecnológico

Sabadell Hub Empresa

PYME LEGAL

OTROS SERVICIOS

Seguro de Protección de Datos y Ciberseguridad

Litigación y defensa jurídica

Gestión del derecho al honor e imagen

Obtención sello de calidad Confianza Online

Canal Denuncias para empresas y entidades

Sabadell Hub Empresa

PYME LEGAL

CÓMO TE AYUDAMOS

PLATAFORMA ONLINE

Servicio autogestionado por el cliente o con acompañamiento.
Modalidad partner para despachos y asesorías.

A DISTANCIA

Servicio a distancia con asesoramiento personalizado.

PRESENCIAL

Consultoría presencial a medida por parte de nuestros consultores.

Sabadell
Hub Empresa

PYME LEGAL

SOMOS...

EXPERIENCIA

Equipo de profesionales con más de **15 años de experiencia en el sector.**

CONFIANZA

Contamos con más de **1.500 clientes finales y 550 partners.**

PROFESIONALES

Somos **colaboradores oficiales** de varios colegios profesionales, como el Colegio Oficial de Gestores de Cataluña (COGAC).

CERTIFICADOS

Los profesionales de **nuestro equipo están certificados como DPD** (Delegado de Protección de Datos).

2.
Ámbito aplicación / Contexto

Sabadell Hub Empresa

PYME LEGAL

Sabadell Hub Empresa

¿Qué es la protección de datos?

La protección de datos es un **derecho fundamental que busca proteger la intimidad y privacidad de las personas físicas** frente a las vulneraciones que puedan producirse por la recogida, almacenamiento y uso indiscriminado de sus datos de carácter personal por parte de las personas jurídicas.

Como derecho fundamental, su protección en España nace de la Constitución Española, que en su artículo 18,4 recoge que **"la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."**

Normativa actual de protección de datos

NORMATIVA

LOPDGDD

Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales 3/2018, de 5 de diciembre de 2018 (LOPDGDD)

Normativa específica dependiendo del sector (sanidad, educación, laboral, etc.)

RGPD

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD)

OBLIGATORIO PARA TODAS LAS EMPRESAS QUE TRATAN DATOS PERSONALES DESDE MAYO DEL 2018

LSSICE

Ley 34/2002 de Servicios de la Sociedad de la Información y Comercio Electrónico

Reglamento e-Privacy

3.
Sanciones

Sabadell Hub Empresa

PYME LEGAL

¿Dónde estamos?

- La normativa establece **obligaciones legales-técnicas-organizativas** a cualquier empresa/autónomo que trate datos.
- **Elevado % de incumplimiento** en toda Europa e **incompatibilidad** con países de fuera de la UE con amplio desarrollo tecnológico (EEUU, China, Rusia).
- En España la **AEPD** (**Agencia Española de Protección de Datos**) es el organismo que vela por el cumplimiento de la normativa. Lleva a cabo **inspecciones** (de oficio o por denuncia) y establece **sanciones** por incumplimiento.
- **23 millones de euros en multas** - Memoria anual AEPD
- **RGPD** – Sanciones mucho más elevadas (hasta 20 millones de euros o 4% facturación de la empresa)
- La Agencia Española de Protección de Datos **está llevando a cabo labor divulgativa** y elaborando guías y herramientas como:
  - Guías para centros educativos
  - Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo
  - Canal prioritario (contenido sexual o violento)
  - Protección del menor en internet
  - RGPD e Inteligencia Artificial
  - Medidas de responsabilidad proactiva en apps para dispositivos móviles
  - Canal Joven
  - Inspecciones remotas (novedad mayo 2023 LOPDGDD)
  - ‘La guía que no viene con el móvil’
  - Directrices para desarrolladores app / IA…
  - ….

Sanciones

GRAVES:

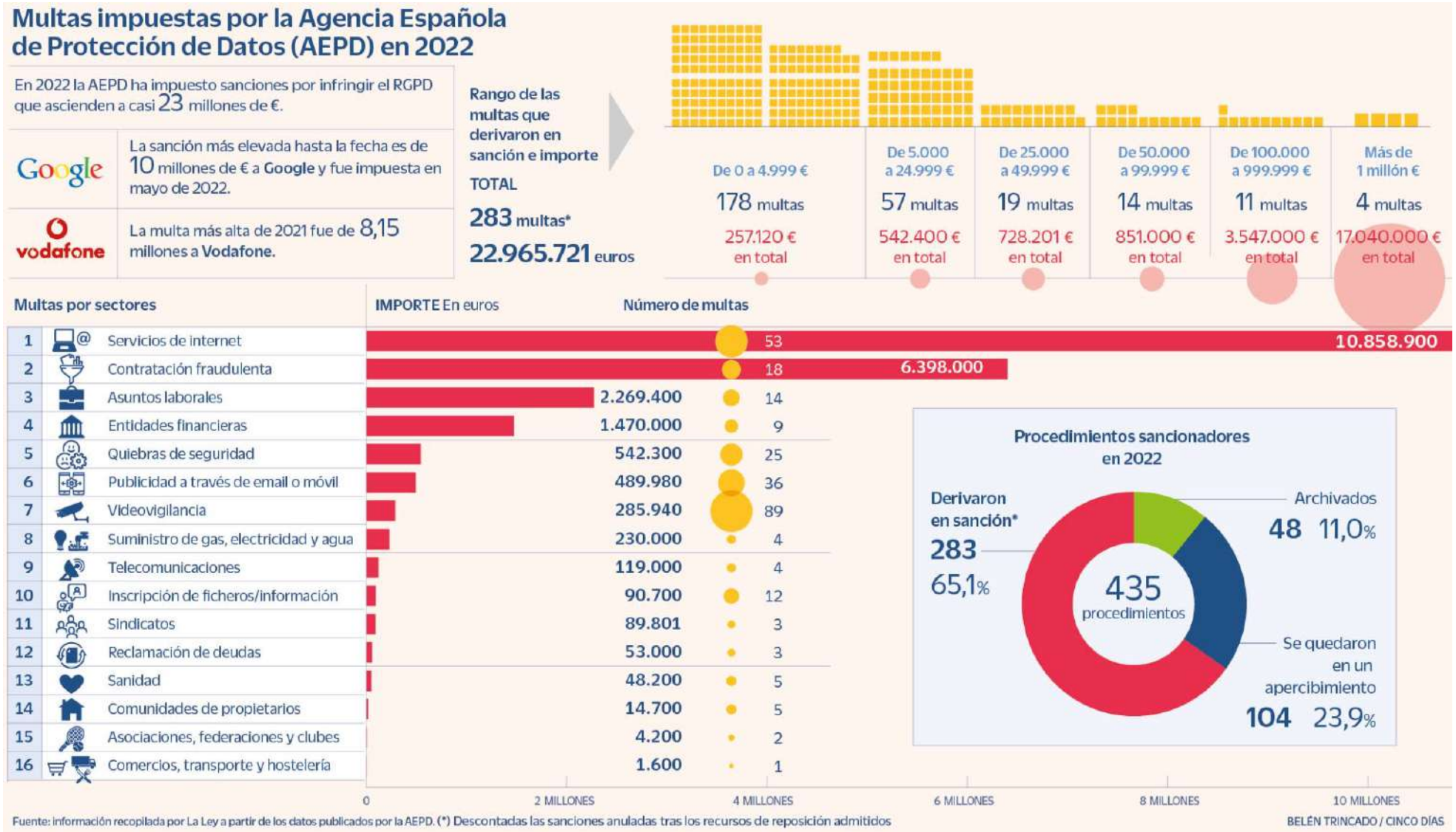
10 MILLONES DE EUROS O 2% DE VOLUMEN ANUAL DE NEGOCIO AÑO ANTERIOR

- Tratar datos de menores sin su consentimiento
- No aplicar medidas técnicas ni organizativas por defecto
- No disponer de Registro de actividades de tratamiento
- No notificar violaciones de seguridad
- No realizar evaluación de impacto
- No designar DPO

MUY GRAVES:

20 MILLONES DE EUROS O 4% DE VOLUMEN ANUAL DE NEGOCIO AÑO ANTERIOR

- No cumplir los principios del RGPD
- No cumplir los derechos de los interesados
- No cumplir requisitos para la transferencia Internacional de datos
- No cumplir con las resoluciones de la Autoridad de Control



Sanciones

LSSI

IKEA ha sido sancionado con 10.000 euros por utilizar cookies incumpliendo la interpretación de la AEPD respecto al art. 22.2 de la Ley 34/2002, de Servicios de la Sociedad de la Información y Comercio Electrónico, tipificada en el artículo 38.4.g) de la LSSI.

aepd agencia española protección datos

PROTECCIÓN DE DATOS

Multa a Vueling.com con 30.000 euros por no dar la posibilidad de oponerse a sus 'cookies'

La Agencia Española de Protección de Datos sanciona a la compañía al comprobar que su sitio web no recaba el consentimiento explícito para instalar 'cookies', sino uno genérico.

Tecnología

Protección de Datos multa a LaLiga con 250.000 euros por «espiar» a los usuarios a través de su aplicación

- El servicio del campeonato de fútbol incluye una función para acceder al micrófono y la geolocalización de los usuarios con el fin de detectar piratería en bares y restaurantes

Sanciones ⚠

La Comisión de Protección de Datos multa con 5,5 millones de euros a WhatsApp y lo obliga a que sus operaciones de procesamiento de datos cumplan con el RGPD.
Leer más

Sanción de 5.000€ a Servicios Integrales del Hogar Tenerife S.L por notificar el embargo de una nómina por WhatsApp al familiar de un trabajador y vulnerar el RGPD.
Leer más

Sanción 600€ por tener las cámaras de videovigilancia orientadas a la vía publica.
Leer más

Sanción de 300€ a un inquilino de una vivienda propiedad del reclamante, por instalar una cámara de vidoevigilancia orientada a la via publica y al acceso de otra de sus propiedades.
Leer más

Sabadell Hub Empresa

Sanciones

PYME LEGAL

Sanción de 5 millones de euros al BBVA por vulnerar tres artículos del RGPD: la más alta de la historia de la Autoridad
Leer más

Sanción de 10.000 euros por revelar datos personales de un antiguo trabajador
Leer más

Sanción de 10.000€ por dar información errónea en la web, referente al consentimiento de los menores de 13 años como base legitimadora del tratamiento de sus datos para la suscripción a la newsletter.
Leer más

Sanción de 5.000€ por uso ilícito de datos al enviar al padre del afectado una denuncia contra la empresa de éste.
Leer más

Sanción de 3.000€ a página web por no tener el banner de cookies, incumplir con el deber de información en primera y segunda capa y no solicitar el consentimiento al usuario para el uso de cookies de terceros.
Leer más

aepd agencia española protección datos

Multa récord de la AEPD a Vodafone: 8 millones de euros por vulnerar varias normativas
Leer más

Sanción de Apercibimiento a particular por vender un gato sin informar debidamente al comprador
Leer más

Sanción a Air Europa de 600.000 euros por brecha de seguridad que afectó a medio millón de interesados
Leer más

Sanción de 15.000€ a una comunidad de propietarios por publicar las actas de una reunión
Leer más

Sanción de 9.000 por publicar fotografías de un tercero sin su consentimiento
Leer más

Sanción de la APDCAT a un hospital por: no aislar acústicamente la sala de espera / llamar a los pacientes con nombres y apellidos en la sala.
Leer más

Sanción de 6 millones de euros a la Caixa (la más alta impuesta después de la del BBVA) por vulnerar varios artículos del RGPD; **177 páginas de resolución.**
Leer más

Vodafone paga sanción de 54.000€ por vulnerar los principios de exactitud y confidencialidad. El origen viene por un cruce de datos en sus sistemas y realizar las actuaciones solicitadas por un tercero en la cuenta del reclamante.
Leer más

Iberdrola paga sanción de 6.000€ por vulnerar el derecho de oposición de un cliente y recibir éste una llamada informando de una campaña comercial estando inscrito en la lista robinson.
Leer más

Sanciones

economíadigital | La UE multa a Meta con 1.200 millones de euros por

Mark Zuckerberg, consejero delegado de Meta. George Frey EXPANSION

Es la mayor sanción impuesta por violar la normativa de privacidad en la Unión Europea.

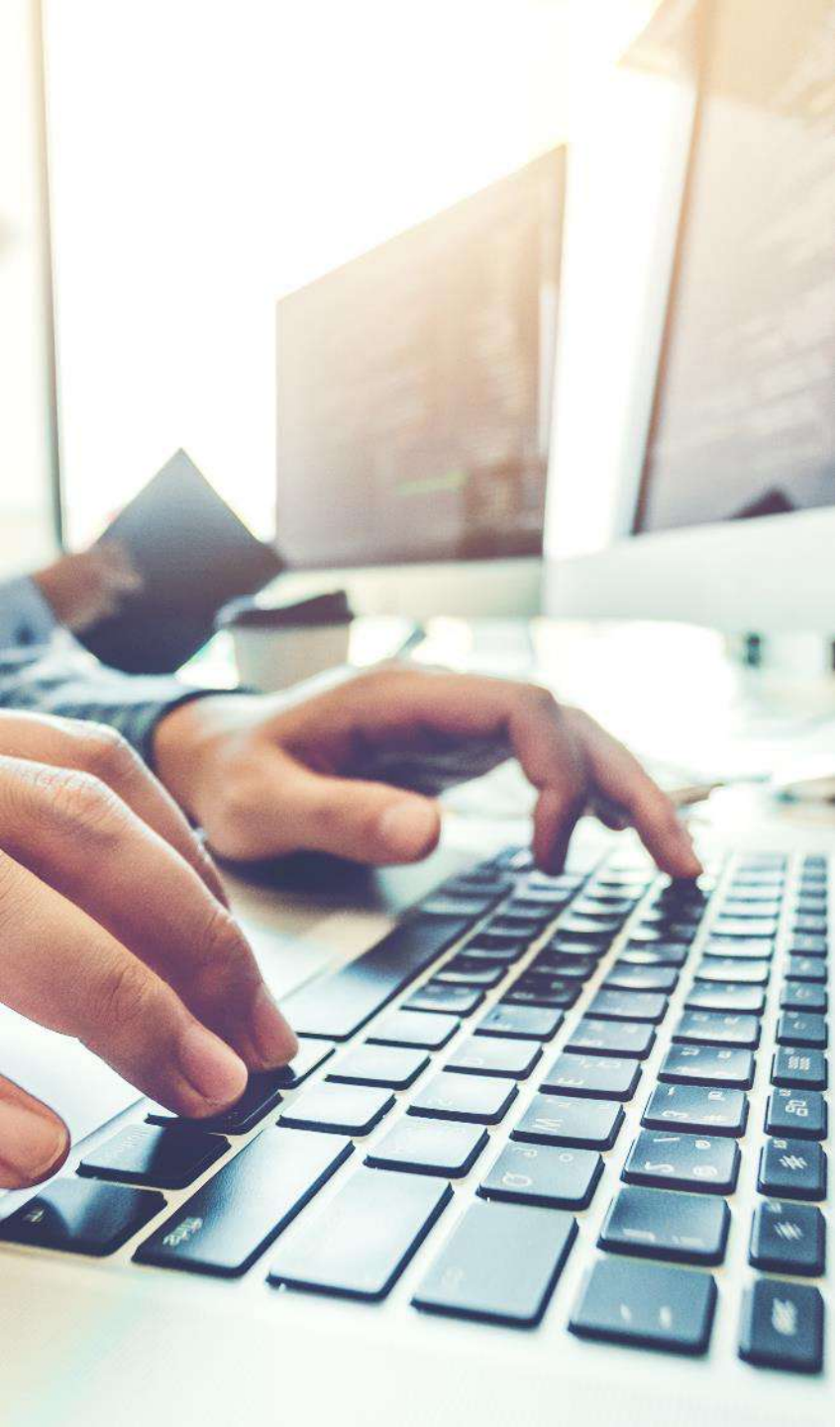
La Unión Europea ha multado a Meta, dueña de Facebook, con una sanción récord de 1.200 millones de euros por vulnerar la legislación comunitaria sobre privacidad al transferir datos de ciudadanos europeos a Estados Unidos. La multa ha sido impuesta por la Comisión de Protección de Datos de Irlanda, país en el que la multinacional estadounidense tiene su sede europea.

El organismo de protección de datos entiende que Facebook ha almacenado ilegalmente durante años datos de ciudadanos europeos en sus servidores de Estados Unidos. La **multa supone un récord en materia de privacidad**, superando a la sanción de 746 millones de euros impuesta contra Amazon en 2021. Además, la Unión Europea da un plazo de cinco meses para que Meta deje de enviar datos de sus usuarios europeos a Estados Unidos y seis meses para borrar cualquier información personal que se haya transferido previamente.

4.
Definiciones

Sabadell Hub Empresa

PYME LEGAL



Datos personales

La normativa de protección de datos define a los **datos de carácter personal** como "**cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a PERSONAS FÍSICAS identificadas o identificables**".

Persona física identificada:
Cuando indica directamente a esa persona sin necesidad de utilizar un conjunto de medios para poder averiguar su identidad.

Persona identificable:
Cuando su identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social.

TIPO DE DATOS:

BÁSICOS

- Cualquier información relativa a una persona física que no sean datos ESPECIALES o PENALES.

ESPECIALMENTE SENSIBLES

- Origen étnico o racial.
- Opiniones políticas.
- Convicciones religiosas o filosóficas.
- Afiliación sindical.
- Datos genéticos o biométricos.
- Datos de salud.
- Datos relativos a la vida y orientación sexual.

ESPECIALES

- Datos relativos a condenas y delitos PENALES o medidas de seguridad afines.
- Datos de colectivos vulnerables (n´ños, ancianos etc)

Datos excluidos

DATOS EXCLUIDOS en la aplicación de la normativa sobre protección de datos

01

Datos que hagan referencia a la identificación de empresas:

De cualquier sociedad de carácter mercantil, sea cual sea su objeto, está exenta de la aplicación de esta normativa, como puedan ser su NIF o razón social.

02

Datos referidos a personas de contacto:

Siempre que se limiten a incorporar los datos de las personas físicas que presten sus servicios en empresas con carácter mercantil, y consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.

03

Datos relativos a empresarios individuales:

Siempre que hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, es decir, dentro de una actividad mercantil.

04

Datos relativos a personas fallecidas:

Sin embargo, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar la defunción, aportando acreditación suficiente del mismo.

05

Datos ámbito doméstico:

Tratamiento de datos efectuado por una persona física en el ejercicio de actividades exclusivamente personales domésticas.

DEFINICIONES

INTERESADO
Persona física cuyos datos son tratados y protegidos por la normativa.

RESPONSABLE TRATAMIENTO (RT)
Persona física o jurídica, de naturaleza pública o privada u órgano administrativo, **que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento**, aunque no lo realizase materialmente.
Es el empresario que obtiene los datos del Interesado.

ENCARGADO TRATAMIENTO (ET)
El encargado de tratamiento es "**la persona física o jurídica, pública o privada, u órgano administrativo externo que solo o conjuntamente con otros trate datos personales por cuenta del responsable del fichero**".

En este caso, es **un tercero que al prestar un servicio al responsable del fichero va a tratar los datos de carácter personal de este**. Dicho tercero no va a tener una dependencia laboral del responsable del fichero, deberá seguir las instrucciones que éste le indique, pero es una entidad independiente.

Ejemplos: gestor que elabora nóminas, empresa informática que nos lleva el mantenimiento, agencia publicidad para las campañas, …

DEFINICIONES

PERSONAL AUTORIZADO (USUARIO)
Personas autorizadas por el Responsable de Tratamiento o Encargados de Tratamiento para realizar un tratamiento de datos.

DELEGADO PROTECCIÓN DE DATOS (DPD – DPO)
Persona o entidad encargada de informar y asesorar al RT, ET y al Personal autorizado de las obligaciones del RGPD y la LOPDGDD.

AUTORIDAD DE CONTROL
Autoridad pública independiente encargada de supervisar la aplicación de las normativas de privacidad; en España son las Agencias de Protección de Datos: **AEPD (española), APDCAT (catalana), AVPD (vasca)**. Las territoriales se encargan de controlar a la Administración Pública.

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS
Organismo de la Unión Europea **responsable de la aplicación del RGPD**. Está en el centro del panorama de la protección de datos en Europa y ayuda a **garantizar que el Reglamento de protección de datos se aplica de forma coherente** en toda la UE y trabajará para garantizar la cooperación efectiva entre las APD.

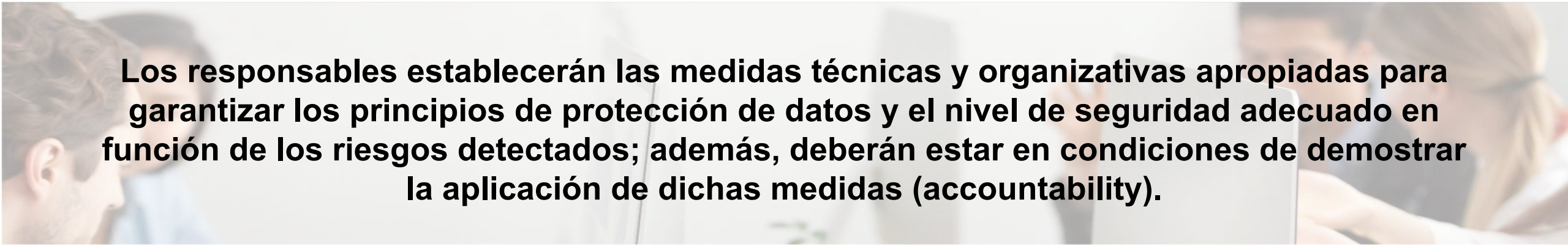
5.
Obligaciones del Responsable

Sabadell Hub Empresa

PYME LEGAL

Responsabilidad proactiva

Privacy by design / default



Los responsables establecerán las medidas técnicas y organizativas apropiadas para garantizar los principios de protección de datos y el nivel de seguridad adecuado en función de los riesgos detectados; además, deberán estar en condiciones de demostrar la aplicación de dichas medidas (accountability).

Privacidad desde el DISEÑO (by design)

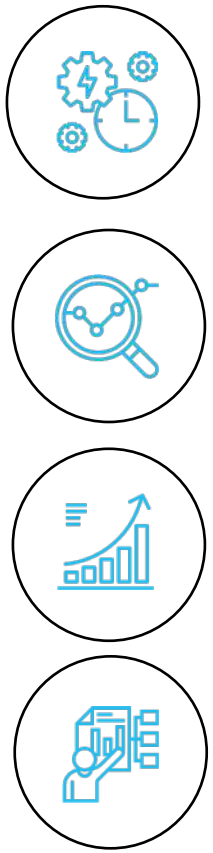
- **Desde el inicio**, aplicar medidas organizativas y técnicas para integrar a los tratamientos garantías que permitan aplicar el RGPD.
- Se aplicarán en el momento que se decida **recoger los datos.**

Privacidad por DEFECTO (by default)

- Los responsables tienen que adoptar medidas que garanticen que **sólo se tratan los datos necesarios** en lo que se refiere a la cantidad de datos, extensión tratamiento, etc. (minimización).

Sabadell
Hub Empresa

Obligaciones del Responsable Tratamiento



- Disponer de un **Registro de Actividades de Tratamiento** (RAT).
- **Cláusulas información** / legitimación
- Regulación **consentimiento**
- **Compromisos confidencialidad trabajadores**
- **Firma con encargados** de tratamiento (ET)
- Garantizar los **derechos de los afectados**.
- **Protocolo brechas** de seguridad.
- Disponer de una **política protección de datos / documento de seguridad**
- Realizar **análisis de riesgos y** aplicar **medidas técnicas**
- Manual usuarios + **formación**
- Cartel **vídeo vigilancia**
- **Avisos legales web**

- Evaluación impacto (PIA)
- Designar **Delegado Protección de Datos** (si procede).
- Regular **transferencias internacionales** de datos (si procede).

6.
Información y Legitimación

Sabadell Hub Empresa

PYME LEGAL

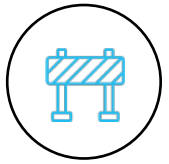
Sabadell Hub Empresa

PYME LEGAL

Principios protección de datos

Principios generales que son la base sobre la que se articula el derecho a la protección de datos, de obligado cumplimiento. Se traducen en garantías para el ciudadano y obligaciones para los RT y ET

LICITUD



LIMITACIÓN DE LA FINALIDAD

MINIMIZACIÓN DE LOS DATOS

EXACTITUD

LIMITACIÓN DEL PLAZO DE CONSERVACIÓN

DISPONIBILIDAD, INTEGRIDAD Y CONFIDENCIALIDAD

RESPONSABILIDAD PROACTIVA

Sabadell
Hub Empresa

PYME LEGAL

INFORMAR: ¿SOBRE QUÉ?

INFORMACIÓN BÁSICA DEL TRATAMIENTO

- Identidad y datos de contacto del RT, del DPD y del representante (si lo tiene)
- Fines del tratamiento
- Legitimación (base jurídica en que se basa el tratamiento)
- Destinatarios de los datos y posibles cesiones de datos a terceros
- Derechos que asisten al interesado:
  - Revocación del consentimiento sin que desvirtúe el previamente otorgado
  - Acceso, rectificación, supresión y portabilidad de datos
  - Limitación u oposición al tratamiento
  - Presentar una reclamación ante la Autoridad de control

Legitimación (bases jurídicas que legitiman el tratamiento)

Todo tratamiento de datos personales por parte de una empresa o profesional exige una base jurídica que lo legitime (artículo 6 RGPD).

Para poder tratar datos, el Responsable de Tratamiento **deberá encontrarse en alguno de los supuestos siguientes**:

Base jurídica
Consentimiento del afectado
Existencia de una **relación contractual**
Cuando resulte una **obligación legal** para el responsable de tratamiento
Justificado en una **necesidad vital** del interesado
Cuando haya un **interés público** o se derive del ejercicio de poderes públicos
Existencia de un **interés legítimo** prevalente del responsable o de terceros a los que se les cedan o comuniquen datos personales

Sabadell
Hub Empresa

Consentimiento del Interesado

El consentimiento debe ser específico para cada finalidad de tratamiento.

Debemos permitir al interesado autorizar de forma independiente las diferentes finalidades.

Cuando no se pueda justificar por ninguno de los otros supuestos,
el Responsable de Tratamiento deberá pedir y poder probar que ha solicitado el consentimiento del afectado.

El consentimiento debe ser:

- **Libre, informado, específico e inequívoco** (art. 4.11 del RGPD).
- Prestarse mediante una acción positiva del interesado, **no será válido el consentimiento tácito.**
- **Verificable**. Se tiene que poder probar que se obtuvo el consentimiento.
- **Prohibido casillas pre-marcadas** en páginas web y formularios.

CONSENTIMIENTO DE MENORES

RGPD mínimo 13 años. Los menores estarán sometidos al consentimiento de sus padres /tutores.

LOPDGDD el limite de edad está en 14 años.

Sabadell Hub Empresa

PYME LEGAL

INFORMAR: ¿CÓMO?

LA PRIMERA CAPA

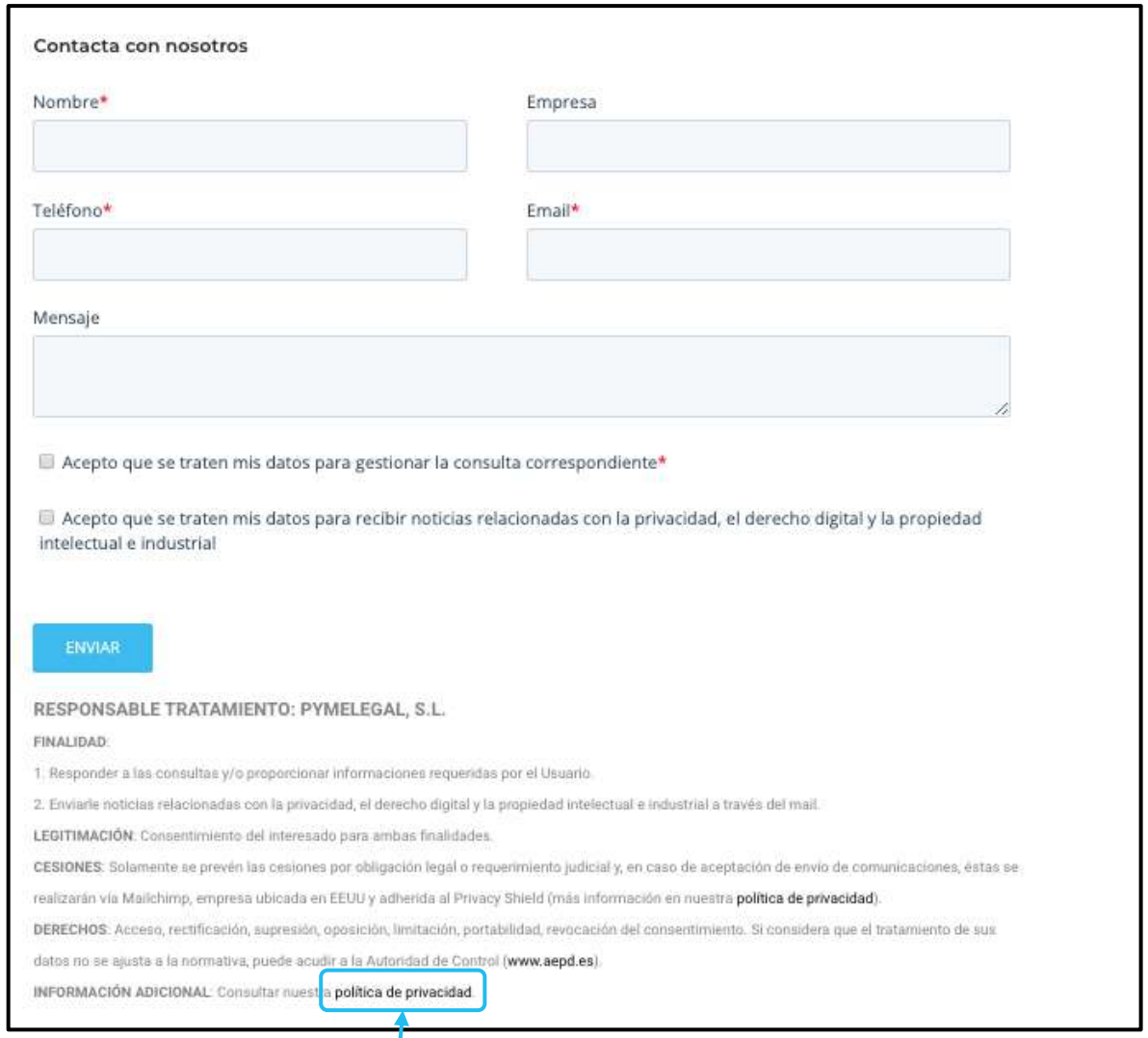
Consiste en la información básica para el interesado, que debe estar de forma resumida, y se debe ofrecer en el mismo momento en que se recopila la información y por el mismo medio por el cual se recojan los datos.

Por ejemplo: contrato que nos firma el cliente, formulario web, …

LA SEGUNDA CAPA

Debe encontrarse la información de forma detallada, en un medio más adecuado para su presentación y compresión por el interesado.

Por ejemplo: Le indicaremos en el contrato que puede consultar más información en la página web (política privacidad)



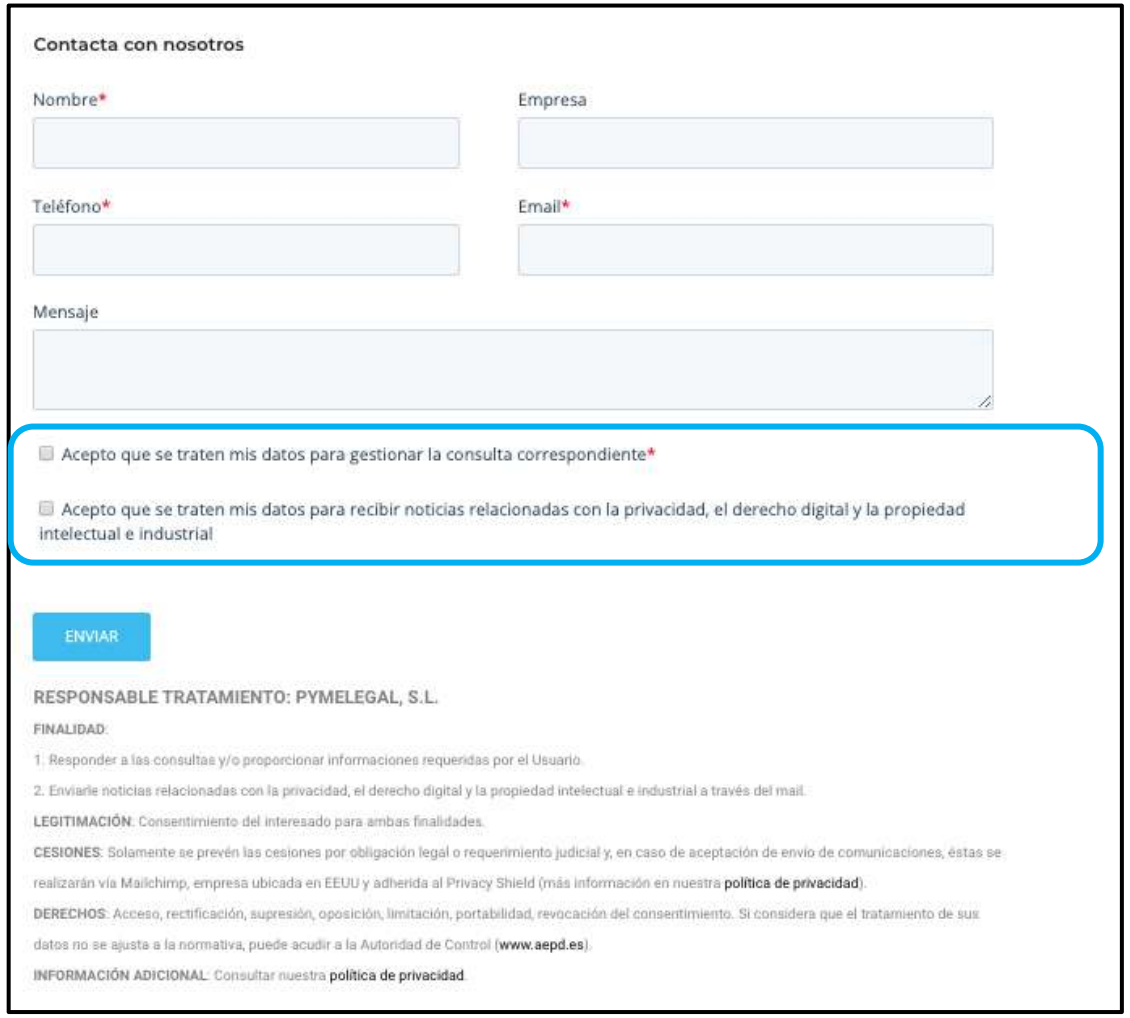
INFORMACIÓN	1ª CAPA	2ª CAPA
Responsable del tratamiento	Identidad del Responsable del Tratamiento	- Datos de contacto del Responsable - Identidad y contacto del representante - Datos de contacto del DPD
Finalidad del Tratamiento	Descripción de los fines del tratamiento	- Descripción ampliada de los fines del tratamiento - Plazos o criterios de conservación de los Datos - Decisiones automatizadas, perfiles y lógica Aplicada
Legitimación del Tratamiento	Base jurídica del tratamiento	- Detalle de la base jurídica del tratamiento - Obligación o no de facilitar datos y consecuencias de no hacerlo
Destinatarios de las cesiones o transferencias	Previsión de cesiones Previsión (o no) de transferencias a terceros países	- Destinatarios o categorías de destinatarios - Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables
Derechos de los interesados	Referencia al ejercicio de derechos	- Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento - Derecho a retirar el consentimiento prestado sin que desvirtúe el previamente otorgado - Derecho a reclamar ante la Autoridad de Control
Procedencia de los datos	Fuente de los datos, cuando no proceden del interesado	- Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público - Categorías de datos que se traten

Ej.: Formulario de contacto

01. DESAGREGAR LA FINALIDAD

- para que el interesado la autorice de forma expresa e independiente

  Ejemplo: *nos autoriza a gestionar los datos personales para tramitar su compra pero no autoriza recibir comunicaciones comerciales.*



Información VIDEOVIGILANCIA

En cuanto al tratamiento de los datos con fines de videovigilancia, el art. 22.4 de la LOPDGDD establece que "***El deber de información previsto en el artículo 12 del Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando****, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679.*

También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información.

¿CUANDO DAR LA INFORMACIÓN?

	OBLIGATORIO	NO OBLIGATORIO
CUANDO LOS DATOS SE OBTIENEN DEL INTERESADO	En el momento de recoger los datos	Cuando el interesado ya disponga de la información
CUANDO LOS DATOS NO SE OBTIENEN DEL INTERESADO	Supuestos: • En un plazo máximo de 1 mes • En el momento de la primera comunicación con el interesado • En el momento que se revelen los datos a un destinatario	• Cuando el interesado ya disponga de la información • Cuando la comunicación sea imposible o suponga un esfuerzo desproporcionado • Cuando el tratamiento esté fundamentado en la legislación vigente

7.
Trabajadores

Sabadell Hub Empresa

PYME LEGAL

Sabadell Hub Empresa

Empleados

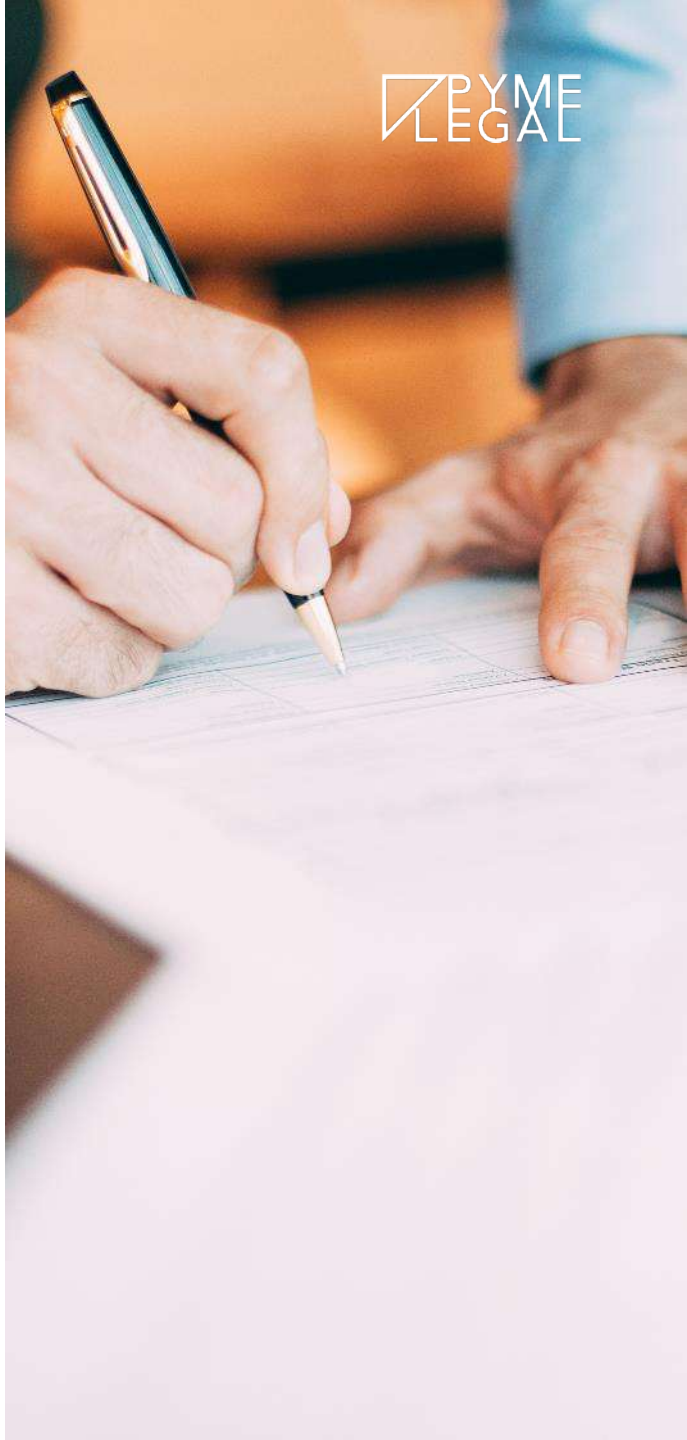
El Responsable de Tratamiento deberá asegurarse de que **sus empleados conocen la normativa de RGPD, velan por la confidencialidad, integridad y disponibilidad** y cumplen en todo caso con las directrices marcadas con la empresa:

Lo que deberá implantar la empresa:

- Hará firmar **COMPROMISO DE CONFIDENCIALIDAD** del trabajador integrado en su contrato de trabajo. Se aplicará a cualquier trabajador que acceda a datos por mínimo que sea el acceso. El nivel de compromiso dependerá de la responsabilidad del empleado y el tipo de datos a los que acceda.

- Se entregará una **NORMATIVA DE USO DE LOS SISTEMAS INFORMÁTICOS Y PAPEL** para que la suscriban. En ella se establecerán normas de uso de los sistemas, de dispositivos, del correo electrónico, de las contraseñas, de las impresoras, normas de archivo electrónico y en papel, etc.

- Se impartirá una **FORMACIÓN PERIÓDICA A EMPLEADOS** para garantizar que conocen la normativa en materia de protección de datos y los protocolos internos de la empresa.



8.
Tratamiento de Datos por terceros

Sabadell Hub Empresa

PYME LEGAL

Encargado de Tratamiento (ET)

Ejemplos de ET:

- ✓ Gestor
- ✓ Asesor
- ✓ Informático
- ✓ Prevención Riesgos
- ✓ Agencia publicidad
- ✓ Colaborador externo
- ✓ Comercial freelance
- ✓ …

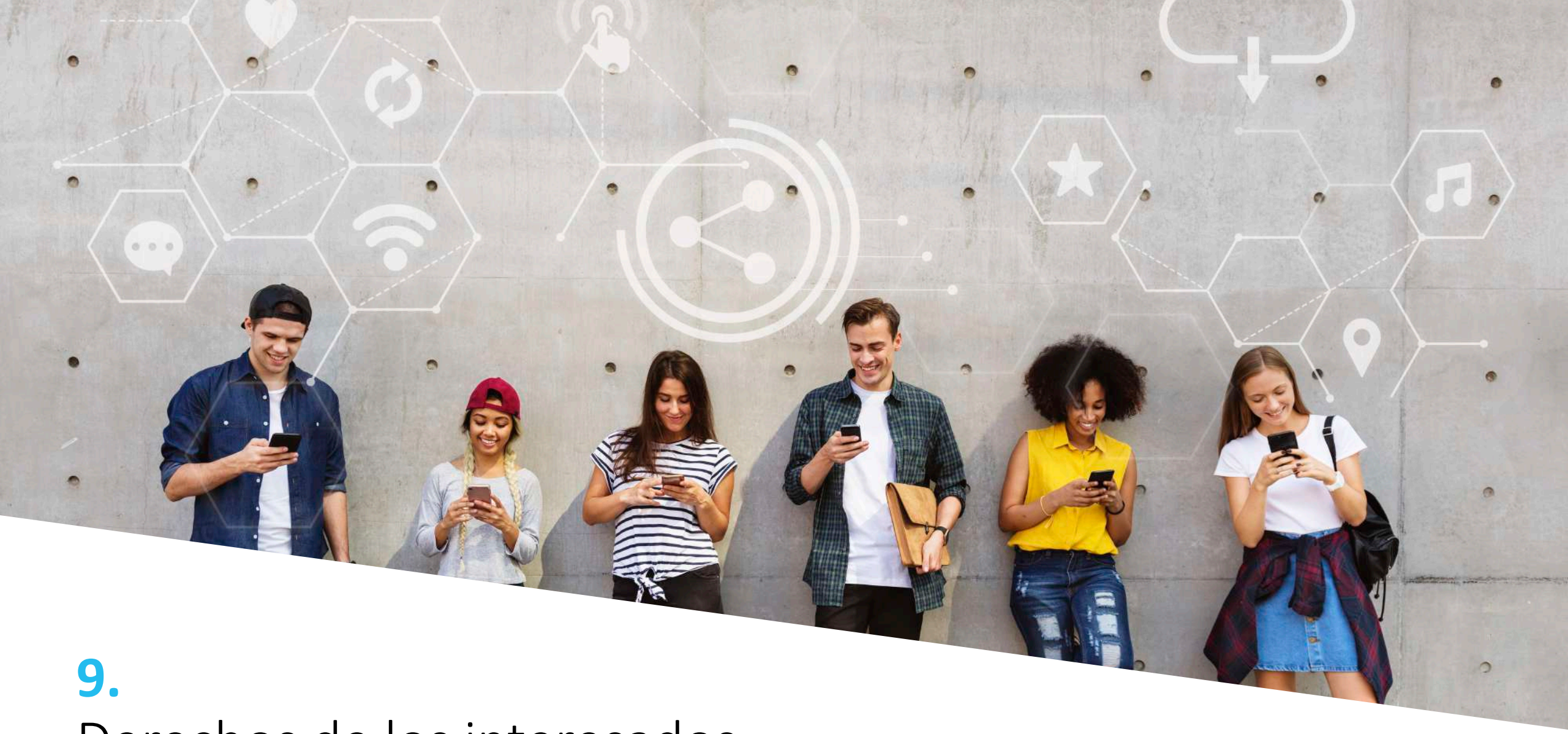
EL ACCESO A LOS DATOS DE CARÁCTER PERSONAL POR PARTE DE TERCEROS DISTINTOS DEL RESPONSABLE DEL TRATAMIENTO COMO CONSECUENCIA DE LA PRESTACIÓN DE UN SERVICIO PROFESIONAL O EMPRESARIAL QUE REALICE DICHO TERCERO A FAVOR DEL RESPONSABLE

(ENCARGADO DE TRATAMIENTO).

En este caso:

- **No se considerará comunicación o cesión de datos,** por lo que **no será necesario el consentimiento previo.**
- La realización de tratamiento por cuenta de terceros debe estar **REGULADA EN UN CONTRATO** que deberá constar por escrito o por cualquier medio que permita acreditar su celebración y contenido.

También se aplicará esta medida **cuando el personal del encargado de tratamiento preste servicios dentro de la organización (*in house*)**. En este caso, el Encargado de Tratamiento deberá tomar medidas para que su personal conozca las medidas de seguridad que deben cumplirse en las instalaciones del Responsable de Tratamiento.



9.
Derechos de los interesados

Sabadell Hub Empresa

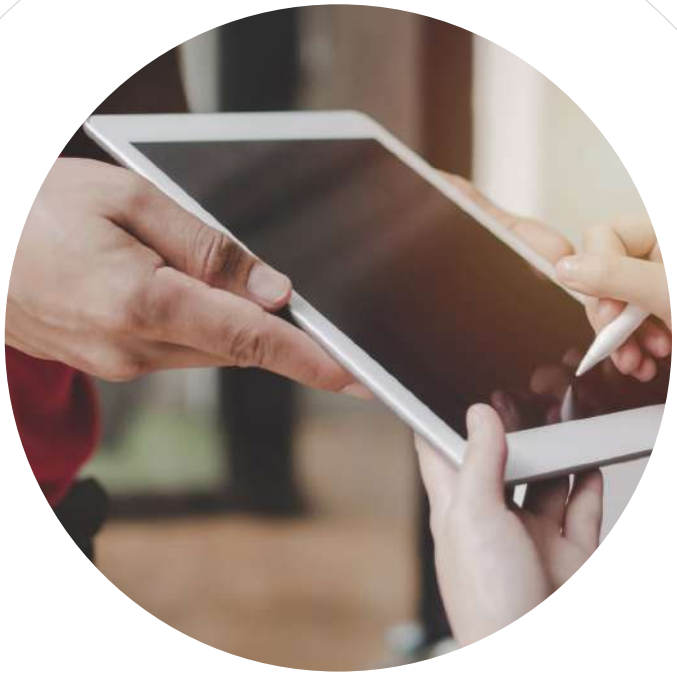
PYME LEGAL

DERECHOS

Gestión de los derechos

- ✓Derecho de Información
- ✓Acceso
- ✓Rectificación
- ✓Supresión
- ✓Oposición
- ✓Portabilidad de los datos
- ✓Limitación al tratamiento
- ✓Derecho al olvido
- ✓Derecho a no ser objeto de decisiones individualizadas

Características comunes para el ejercicio de los derechos



- Los derechos son personalísimos
- Son independientes entre sí
- Se deberá verificar la identidad de quien ejerza el derecho
- Gratuito para el afectado (puede no aplicar en determinados casos)
- Plazo de respuesta: 1mes
- Puede gestionar los derechos un encargado de tratamiento

10.
Derechos Digitales

Sabadell Hub Empresa

PYME LEGAL

Derechos Digitales (Título X LOPDGDD)

- DERECHO A LA NEUTRALIDAD DE INTERNET
- DERECHO DE ACCESO UNIVERSAL A INTERNET
- DERECHO A LA SEGURIDAD DIGITAL
- DERECHO A LA EDUCACIÓN DIGITAL
- PROTECCIÓN DE LOS MENORES EN INTERNET
- DERECHO DE RECTIFICACIÓN EN INTERNET
- DERECHO A LA ACTUALIZACIÓN DE INFORMACIONES EN MEDIOS DE COMUNICACIÓN DIGITALES
- PROTECCIÓN DE DATOS DE LOS MENORES EN INTERNET
- DERECHO AL OLVIDO EN BÚSQUEDAS DE INTERNET
- DERECHO DE PORTABILIDAD EN SERVICIOS DE REDES SOCIALES Y SERVICIOS EQUIVALENTES
- DERECHO AL OLVIDO EN SERVICIOS DE REDES SOCIALES Y SERVICIOS EQUIVALENTES
- DERECHO AL TESTAMENTO DIGITAL

Garantía de los derechos digitales

Artículo 20 bis. Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión

*Los **trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización** en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.*

- **DERECHO A LA INTIMIDAD Y USO DE LOS DISPOSITIVOS DIGITALES EN EL ÁMBITO LABORAL**
- **DERECHO A LA DESCONEXIÓN DIGITAL EN EL ÁMBITO LABORAL**
- **DERECHO A LA INTIMIDAD FRENTE AL USO DE DISPOSITIVOS DE VIDEOVIGILANCIA Y DE GRABACIÓN DE SONIDOS EN EL LUGAR DE TRABAJO**
- **DERECHO A LA INTIMIDAD ANTE LA UTILIZACIÓN DE SISTEMAS DE GEOLOCALIZACIÓN EN EL ÁMBITO LABORAL**
- **DERECHOS DIGITALES EN LA NEGOCIACIÓN COLECTIVA**

11.
Transferencias Internacionales de datos

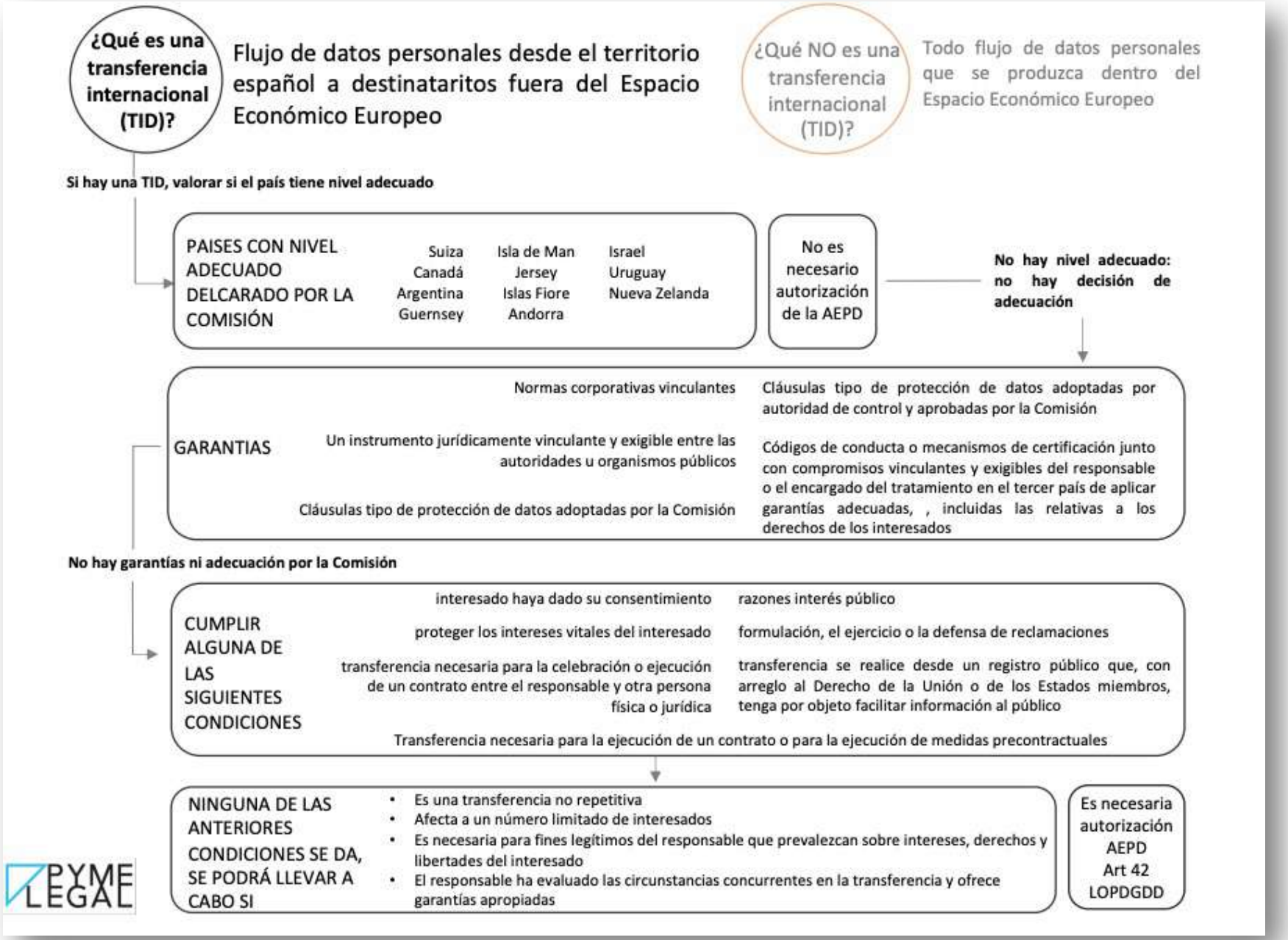
Sabadell Hub Empresa

PYME LEGAL

Sabadell
Hub Empresa

PYME LEGAL

TRANSFERENCIAS INTERNACIONALES DE DATOS



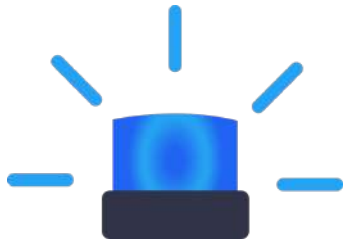
12.
Brechas de Seguridad

Sabadell Hub Empresa

PYME LEGAL

Brechas de seguridad

El RGPD define las violaciones de seguridad de los datos, más comúnmente conocidas como '**quiebras o brechas de seguridad**', de una forma muy amplia, que incluye **todo incidente 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 a dichos datos.**



Sabadell Hub Empresa

VIOLACIONES SEGURIDAD

Ejemplos

ACCESO A DATOS NO AUTORIZADO

- Acceso por terceros a documentación en fotocopiadoras, impresoras
- Acceso no autorizado a información confidencial
- Acceso no autorizado a los sistemas informáticos

COMUNICACIÓN DE DATOS NO AUTORIZADA

- Transmisión ilícita de datos a un destinatario
- Vulneración del secreto profesional
- Publicación de imágenes sin autorización del interesado
- Envío masivo de email sin ocultar los destinatarios (copia oculta)

ALTERACIÓN DE DATOS

- Modificación de datos malintencionado
- Falsificación de datos

PÉRDIDA DE INFORMACIÓN

- Perdida de documentación con información sensible
- Fuga de información por ataque red corporativa / web
- Robo o sustracción de información
- Borrado accidental de ficheros con datos personales
- No usar destructora de papel o de soportes digitales
- Incendio, inundación u otras causas ajenas a la empresa

Gestión

PREPARACIÓN	• Elaborar un **protocolo interno** para la gestión de estos sucesos y mantener un registro. • Este protocolo incluirá: identificación de los agentes implicados, análisis de riesgos o evaluaciones de impacto (si son necesarias) y definición de los planes de respuesta.
DETECCION E IDENTIFICACION	• Fase que debe funcionar de manera continua dentro de la operativa habitual. • Se debe poder concretar si la situación se considera violación de la seguridad y las herramientas o mecanismos con los que se cuenta. • La detección de estas brechas puede proceder de fuentes internas o externas.

PLAN DE ACTUACIÓN	• Si el incidente se clasifica como brecha de seguridad se deberá iniciar el proceso de notificación.
	• Figuras implicadas:
	  ◦ Responsable Tratamiento
	  ◦ Expertos en materia de seguridad
	  ◦ Delegado protección de datos
	  ◦ Autoridad de control competente

NOTIFICACIÓN AEPD

Si la violación de seguridad **supone un riesgo para los derechos y libertades de los afectados** el responsable de tratamiento, deberá **notificar la incidencia a la autoridad de control competente en un plazo máximo de 72 horas.**

Ciberseguridad

La ciberseguridad es el conjunto de **medidas de seguridad que se implantan para proteger los sistemas de información en el entorno tecnológico.** Nuestra información es un activo que tiene un valor y debe ser protegido frente a terceros o frente a incidentes internos.

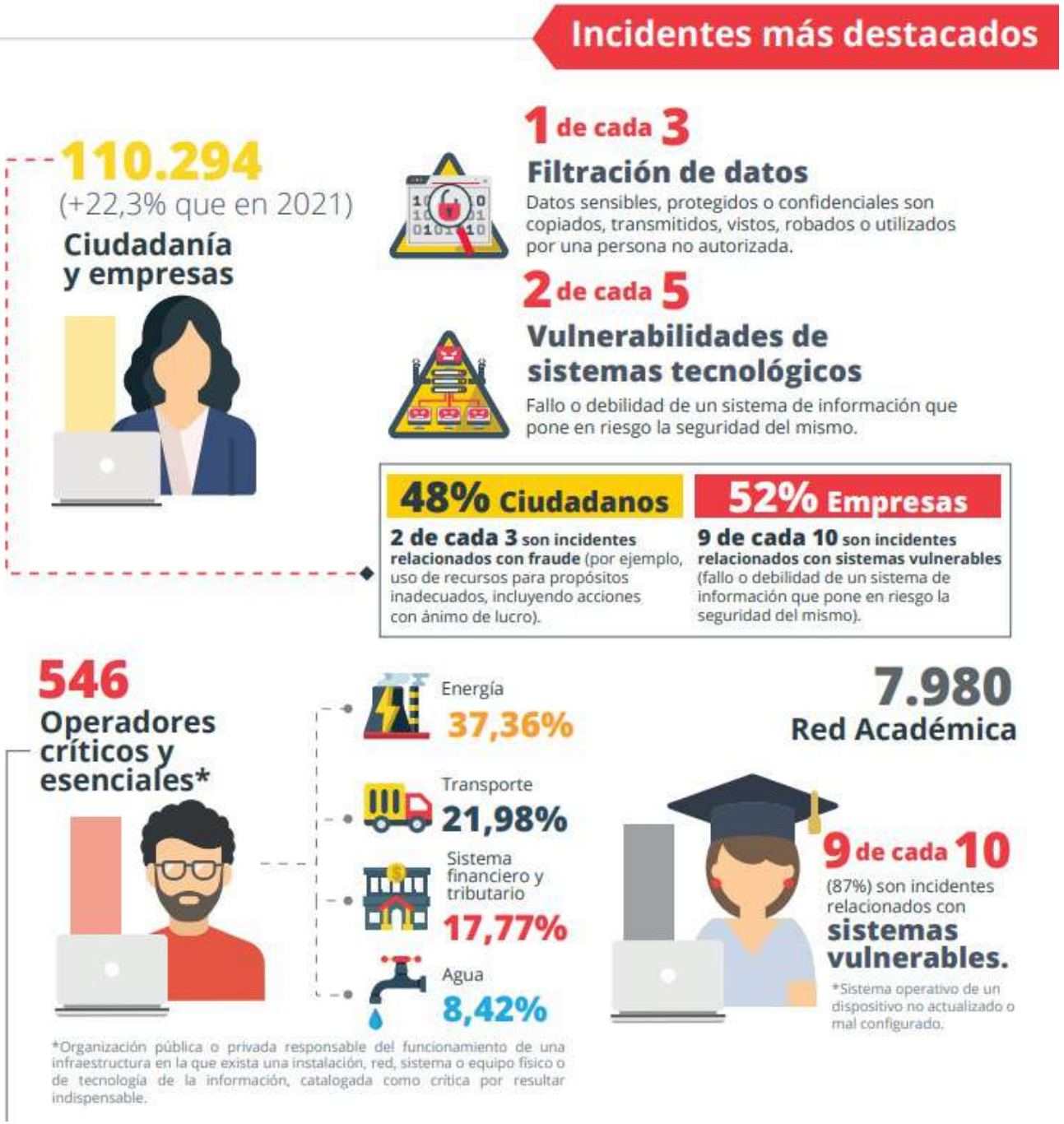
El **incremento del teletrabajo** han dejado al descubierto lo **vulnerables que son las empresas y usuarios ante la ciberdelincuencia**. Cada día nos llegan noticias sobre nuevos fraudes que pretenden apropiarse de datos personales e información confidencial. La dependencia de los sistemas informáticos, el teletrabajo, el auge de las herramientas para videoconferencias y el incremento de los ecommerce, entre otros aspectos, han convertido a la **ciberseguridad y la protección de datos en el gran reto de los próximos años para pymes y autónomos**.

La **mayoría de los incidentes de seguridad** que afectan a las empresas tienen en común dos factores: el **correo electrónico y comunicaciones que utilizan técnicas de ingeniería social**. La ingeniería social consiste en utilizar diferentes técnicas de manipulación psicológica con el objetivo de conseguir que las potenciales víctimas revelen información confidencial o realicen alguna acción como instalar software malicioso. Según un informe de INCIBE, les **principales ciber amenazas y fraudes** que pueden afectar a empresas y autónomos son:

- **Fugas de información**
- **Ataques tipo *phishing***
- **Fraude del CEO**
- **Fraude de RRHH**
- **Sextorsión**
- **Ataques contra la web corporativa**
- **Ransomware**
- **Fraude del falso soporte de Microsoft**
- **Campañas de correos electrónicos con *malware***
- **Ataques de denegación de servicios.**
- **Etc.**

Sabadell Hub Empresa

Ciberseguridad



Ciberseguridad

13.
Delegado protección de datos

Sabadell Hub Empresa

PYME LEGAL

Delegado de protección de datos

¿QUÉ ES EL DELEGADO DE PROTECCIÓN DE DATOS?

Esta figura, conocida popularmente como **DPO (en inglés, *Data Protection Officer*),** constituye uno de los elementos claves del RGPD, y un **garante del cumplimiento de la normativa de la protección de datos en las organizaciones.**

El Delegado de Protección de Datos deberá contar con conocimientos especializados en Derecho y en protección de datos, y actuará de forma independiente; **se le atribuyen una serie de funciones reguladas en el artículo 39 del RGPD** y **artículo 34 de la LOPDGDD.**

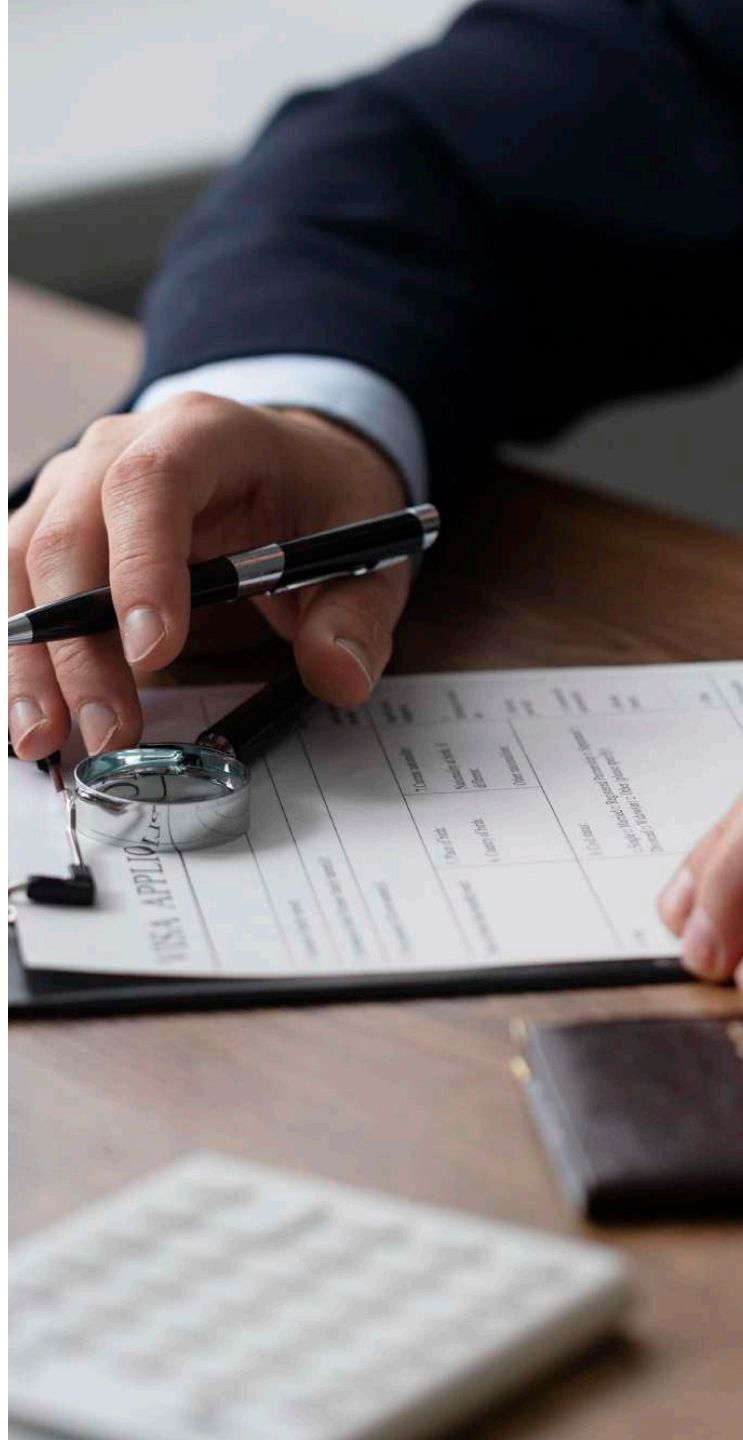
OBLIGACIONES Y RESPONSABILIDADES DEL DPD

- Informar y asesorar al responsable o encargado de tratamiento y a los empleados que se ocupen del tratamiento sobre las obligaciones que les incumben en materia de protección de datos.
- Supervisar el cumplimiento de lo dispuesto en el RGPD y otras disposiciones de protección de datos.
- Asignación de responsabilidades, concienciación, y formación del personal que participa en las operaciones de tratamiento.
- Realización de auditorías.
- Ofrecer asesoramiento respecto de la evaluación de impacto (art.35)
- Cooperar con la autoridad de control.
- Prestar la debida atención a los riesgos asociados a las operaciones de tratamiento.
- Rendir cuentas directamente al más alto nivel jerárquico del responsable/encargado.
- Atender a los interesados que se pongan en contacto con el DPD.

Sabadell
Hub Empresa

Delegado de protección de datos

- ✓ Esta figura **NO es obligatoria para todas las empresas**. El RGPD establece algunos supuestos y la LOPDGDD amplía los supuestos.
- ✓ Aunque las empresas no encajen en los supuestos designados, **pueden designar de forma voluntaria un DPD.**
- ✓ Un **grupo empresarial podrá nombrar un único DPD.**
- ✓ Será designado atendiendo a sus cualidades profesionales, y en particular, a sus **conocimientos en derecho y protección de datos**.
- ✓ El **DPD podrá formar parte de la plantilla o ser externo** (regular mediante contrato).
- ✓ Se comunicarán los datos del **DPD a la Autoridad de Control**.
- ✓ El responsable garantizará que el **DPD no reciba instrucciones respecto sus funciones y no se produzca un conflicto de intereses**.
- ✓ Los profesionales se podrán **certificar como DPD** (esquema de certificación AEPD).



Delegado de protección de datos

Art. 37 RGPD:

- **Autoridades u organismos públicos.**
- Actividades que requieran una **observación habitual y sistemática de interesados a gran escala**.
- Tratamientos a **gran escala de categorías especiales de datos.**

Art. 34 LOPDGDD:

- Los **colegios profesionales** y sus consejos generales.
- Los **centros docentes**, 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 la **información** cuando **elaboren a gran escala perfiles de los usuarios** 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 servicios de inversión, reguladas por la legislación del Mercado de Valores.
- Los distribuidores y comercializadores de **energía eléctrica** y los distribuidores y comercializadores de **gas natural**.
- Las **entidades responsables** de **ficheros** comunes para la **evaluación de la solvencia patrimonial y crédito** o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los **responsables** de los ficheros regulados por la legislación de **prevención del blanqueo de capitales y de la financiación del terrorismo** como **notarios y registradores, abogados y procuradores, casinos, joyeros, entidades de pago, agencias inmobiliarias, entre otros**.
- 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 los afectados o realicen actividades que impliquen la elaboración de perfiles.
- Los centros **sanitarios**. 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**.
- Los **operadores** 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**.

14.
Medidas de Seguridad

Sabadell Hub Empresa

PYME LEGAL

Medidas de Seguridad

MEDIDAS

ORGANIZATIVAS

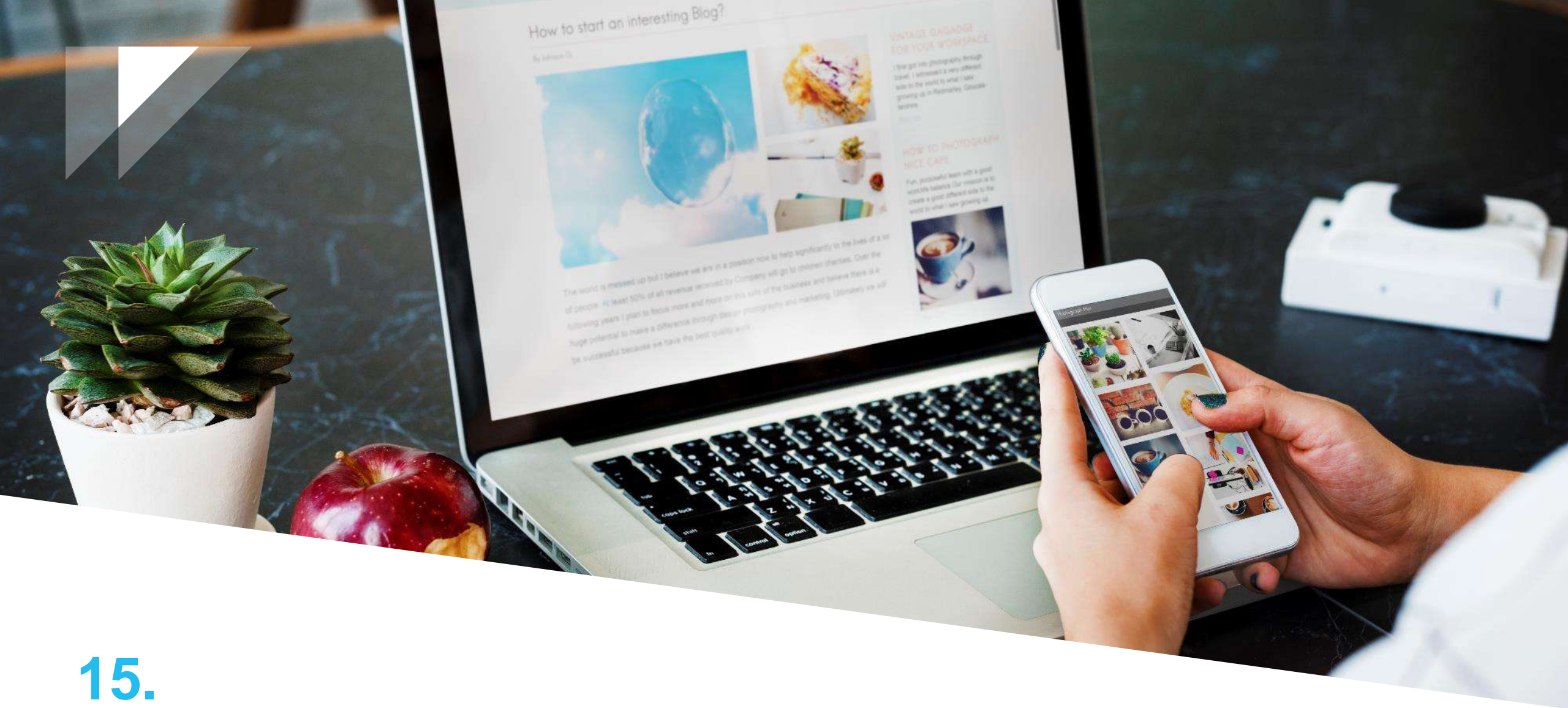
Accesos a instalaciones
Colocación de dispositivos de impresión
Destructoras de papel
Archivo documentación
Protocolos para empleados
Protocolo brechas de seguridad
…

TÉCNICAS

Claves de acceso para cada usuario
Perfiles de usuario
Uso de contraseñas seguras
Copias de Seguridad
Sistema actualizados
Inventario de dispositivos
Control acceso físico servidores
Ficheros en servidor
Antivirus
Antimalware
Firewall
Auditorías
Cifrado de dispositivos
Registro de accesos
…

FORMATIVAS

Formación a usuarios con acceso a datos por los canales que estime oportuno la empresa



15.
Páginas Web

Sabadell Hub Empresa

PYME LEGAL

Páginas web

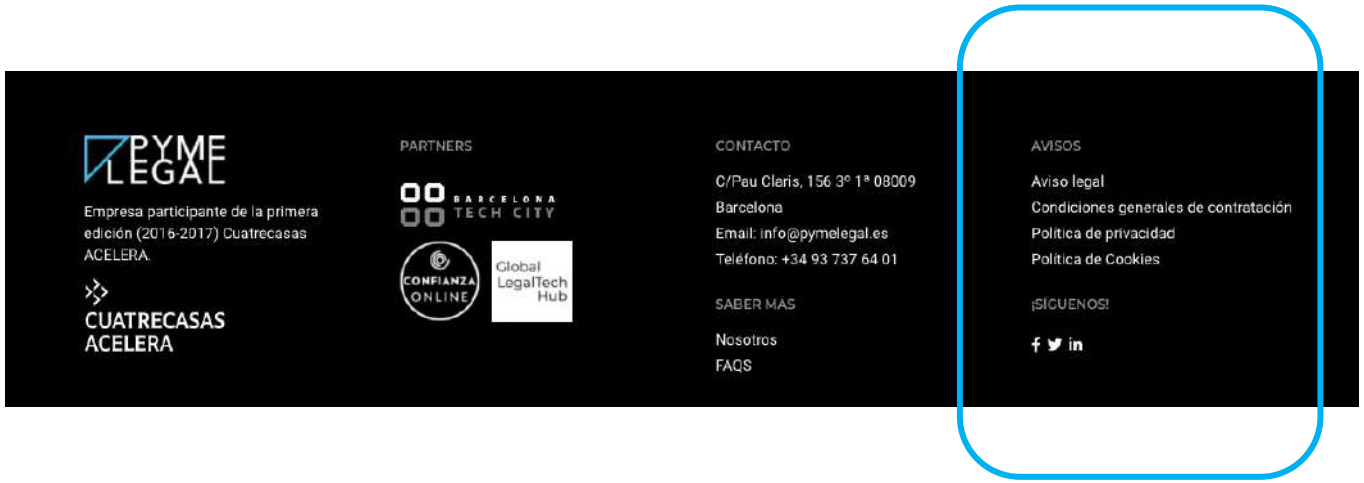
La LSSICE (Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico) establece obligaciones a actividades como: comercio electrónico, información y publicidad online, contratación en línea, servicios de intermediación.

Debe incluir:

- **Aviso Legal (art. 10 LSSICE)**
- **Política de Privacidad (RGPD-LOPDGDD)**
- **Política de Cookies (LSSICE)**
- **Condiciones generales de contratación (ecommerce)**
- **Cláusula para comunicaciones comerciales (newsletters)**

Otros:

- **Formulario de contacto web**
- **Sección envío CV**
- **Términos y condiciones de uso (apps)**
- **Formulario para chat**
- **Formulario para cita previa**



Sabadell Hub Empresa

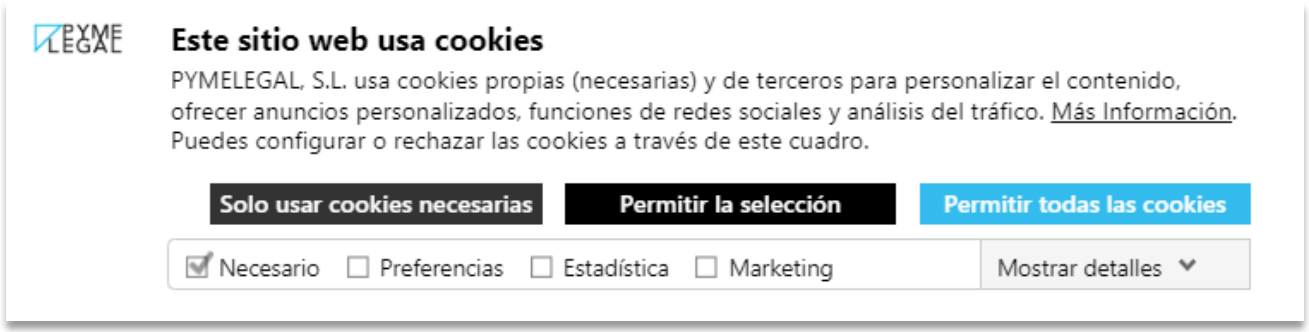
PYME LEGAL

Páginas web

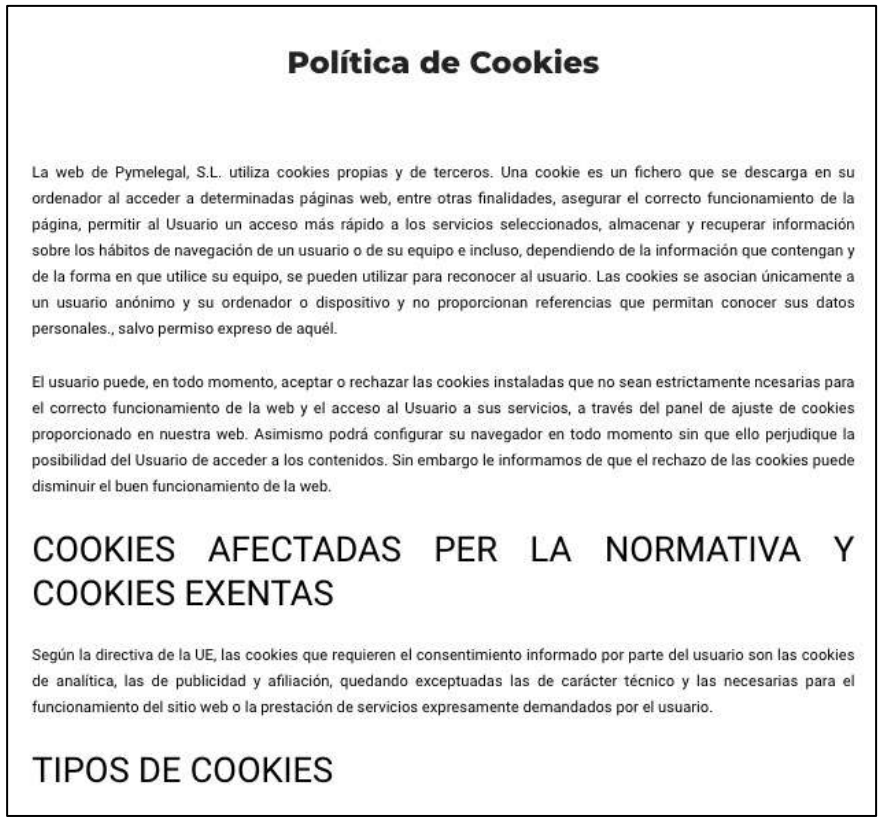
POLITICA DE COOKIES

- Mostrar una 'política de cookies' clara y visible que incluya: finalidad, quién las instala y cómo se pueden desinstalar.
- Información por capas.
- Información en la política:
  - Definición y función genérica de las cookies
  - Información sobre el tipo de cookies que se utilizan y su finalidad
  - Identificación de quien utiliza las cookies.
  - La finalidad de uso de las mismas
  - Información sobre la forma de aceptar, denegar, revocar el consentimiento o eliminar las cookies.
  - Información relacionada con el tratamiento de datos personales prevista en el artículo 13 RGPD

Banner cookies



Política cookies



Política de Cookies

La web de Pymelegal, S.L. utiliza cookies propias y de terceros. Una cookie es un fichero que se descarga en su ordenador al acceder a determinadas páginas web, entre otras finalidades, asegurar el correcto funcionamiento de la página, permitir al Usuario un acceso más rápido a los servicios seleccionados, almacenar y recuperar información sobre los hábitos de navegación de un usuario o de su equipo e incluso, dependiendo de la información que contengan y de la forma en que utilice su equipo, se pueden utilizar para reconocer al usuario. Las cookies se asocian únicamente a un usuario anónimo y su ordenador o dispositivo y no proporcionan referencias que permitan conocer sus datos personales., salvo permiso expreso de aquél.

El usuario puede, en todo momento, aceptar o rechazar las cookies instaladas que no sean estrictamente ncesarias para el correcto funcionamiento de la web y el acceso al Usuario a sus servicios, a través del panel de ajuste de cookies proporcionado en nuestra web. Asimismo podrá configurar su navegador en todo momento sin que ello perjudique la posibilidad del Usuario de acceder a los contenidos. Sin embargo le informamos de que el rechazo de las cookies puede disminuir el buen funcionamiento de la web.

COOKIES AFECTADAS PER LA NORMATIVA Y COOKIES EXENTAS

Según la directiva de la UE, las cookies que requieren el consentimiento informado por parte del usuario son las cookies de analítica, las de publicidad y afiliación, quedando exceptuadas las de carácter técnico y las necesarias para el funcionamiento del sitio web o la prestación de servicios expresamente demandados por el usuario.

TIPOS DE COOKIES

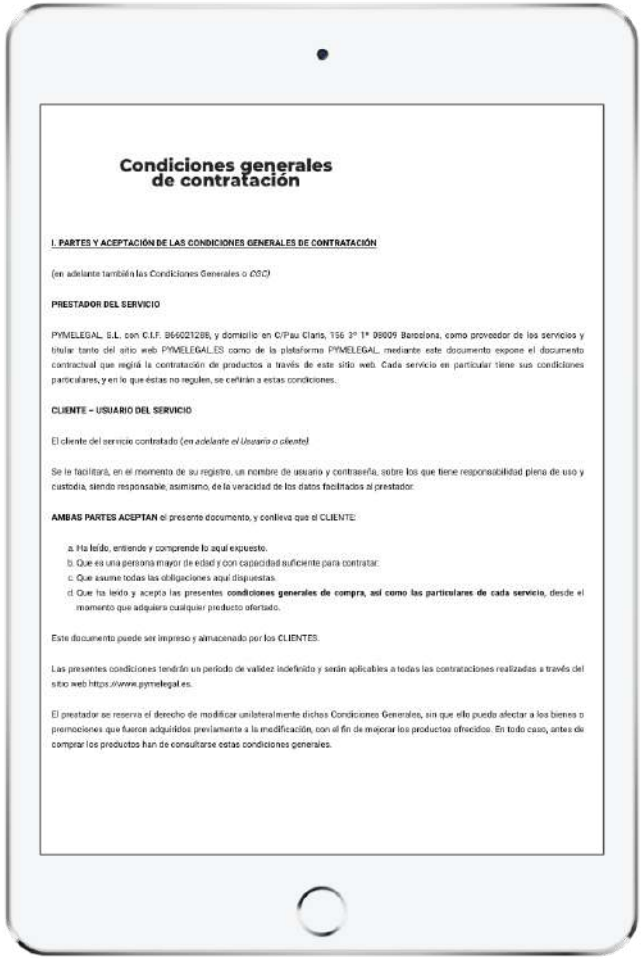
Páginas web

CONDICIONES GENERALES DE CONTRATACIÓN (ecommerce)

Condiciones de uso y contratación que abarcan el conjunto de **disposiciones que regulan el ecommerce, definidas** por el vendedor y dirigidas al comprador, el cual las debe aceptar (sino, no se puede realizar la compra online).

ANTES DE LA CONTRATACIÓN, informar de:
- Características de los bienes o servicios
- Identidad del empresario
- El precio total (con impuestos y tasas)
- Gastos adicionales de transporte, entrega o postales y cualquier otro gasto.
- Los procedimientos de pago y entrega o ejecución
- Garantía legal de los productos y servicios postventa.
- La duración del contrato
- La lengua o lenguas de formalización del contrato
- La existencia del derecho de desistimiento o indicación expresa de las excepciones
- La Funcionalidad de los contenidos digitales
- El Procedimiento para atender las reclamaciones de los consumidores y usuarios

DESPUÉS DE LA CONTRATACIÓN:
Con posterioridad, obligación de confirmar la aceptación del contrato. El prestador lo suele realizar mediante el envío de un correo de confirmación del pedido.


Condiciones generales de contratación

I. PARTES Y ACEPTACIÓN DE LAS CONDICIONES GENERALES DE CONTRATACIÓN

(en adelante también las Condiciones Generales o *CGC*)

PRESTADOR DEL SERVICIO

PYMELEGAL, S.L. con C.I.F. B66021286, y domicilio en C/Pau Claris, 156 3º 1ª 08009 Barcelona, como proveedor de los servicios y titular tanto del sitio web PYMELEGAL.ES como de la plataforma PYMELEGAL, mediante este documento expone el documento contractual que regirá la contratación de productos a través de este sitio web. Cada servicio en particular tiene sus condiciones particulares, y en lo que éstas no regulen, se ceñirán a estas condiciones.

CLIENTE – USUARIO DEL SERVICIO

El cliente del servicio contratado (*en adelante el Usuario o cliente*)

Se le facilitará, en el momento de su registro, un nombre de usuario y contraseña, sobre los que tiene responsabilidad plena de uso y custodia, siendo responsable, asimismo, de la veracidad de los datos facilitados al prestador.

AMBAS PARTES ACEPTAN el presente documento, y conlleva que el CLIENTE:

a. Ha leído, entiende y comprende lo aquí expuesto.
b. Que es una persona mayor de edad y con capacidad suficiente para contratar.
c. Que asume todas las obligaciones aquí dispuestas.
d. Que ha leído y acepta las presentes **condiciones generales de compra, así como las particulares de cada servicio**, desde el momento que adquiera cualquier producto ofertado.

Este documento puede ser impreso y almacenado por los CLIENTES.

Las presentes condiciones tendrán un período de validez indefinido y serán aplicables a todas las contrataciones realizadas a través del sitio web https://www.pymelegal.es.

El prestador se reserva el derecho de modificar unilateralmente dichas Condiciones Generales, sin que ello pueda afectar a los bienes o promociones que fueron adquiridos previamente a la modificación, con el fin de mejorar los productos ofrecidos. En todo caso, antes de comprar los productos han de consultarse estas condiciones generales.

Páginas web

Comunicaciones comerciales - newsletters

El régimen jurídico de este tipo de comunicaciones se regula en los artículos del 19 a 22 de la LSSICE.

El artículo 21.1 LSSICE **prohíbe el envío de comunicaciones comerciales por correo electrónico sin el consentimiento previo y expreso del afectado**.

Además del consentimiento previo, se deberá informar en las comunicaciones sobre la finalidad del tratamiento y derecho al denegar o retirar el consentimiento; inclusión de una dirección.

No es necesario el consentimiento previo si ha existido una relación contractual previa, siempre y cuando se hayan obtenido los datos de forma lícita y se trate de publicidad de productos/servicios similares a los contratados.

VALIDACIÓN MAIL USUARIOS

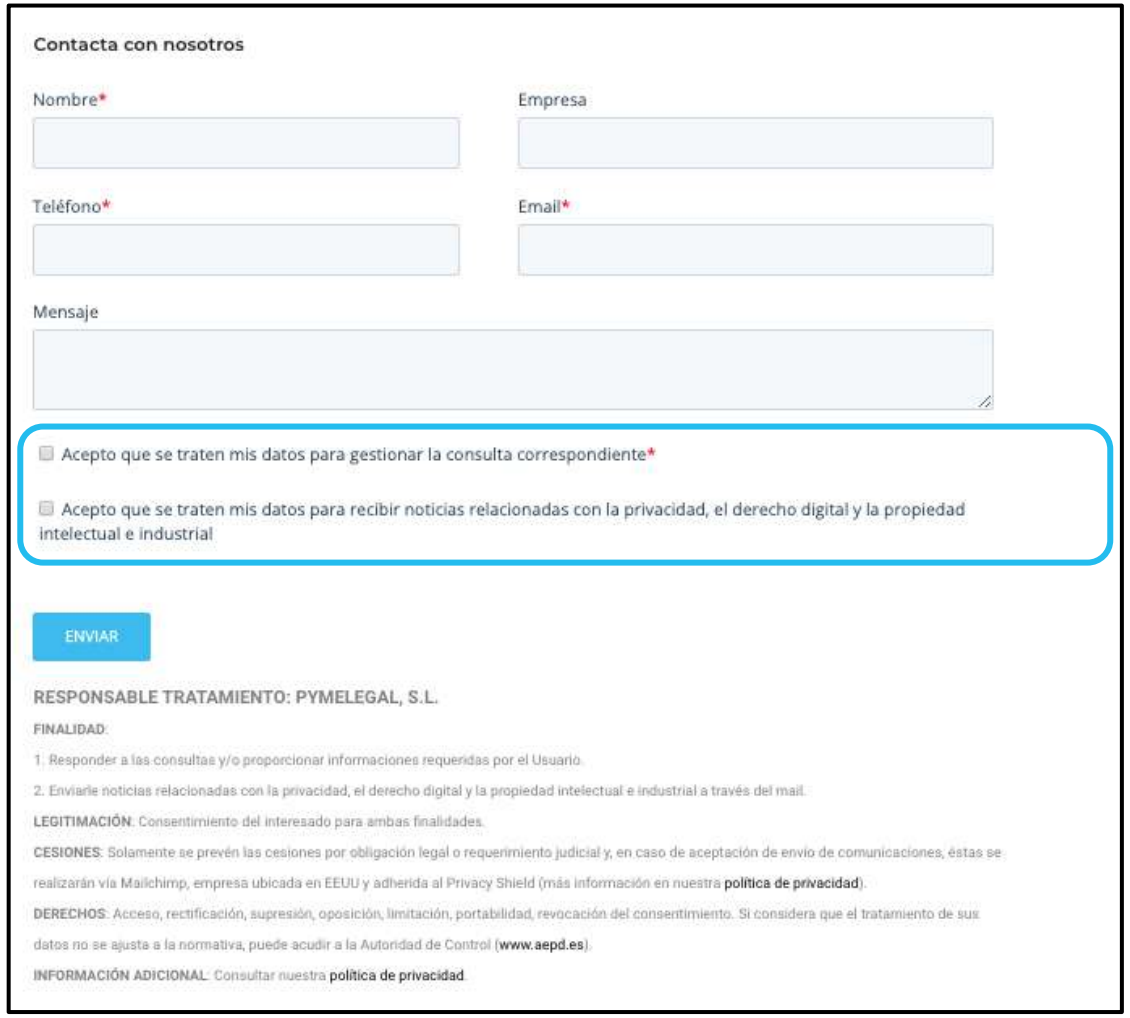
01. DESAGREGAR LAS FINALIDADES

- para que el interesado la autorice de forma expresa e independiente

  Ejemplo: *nos autoriza a gestionar los datos personales para tramitar su compra pero no autoriza recibir comunicaciones comerciales.*

02. ACTIVAR EL DOBLE OPT IN *

- En el doble opt in **se envía un email de confirmación, en el cual la persona ratifica el deseo de recibir publicidad** de los temas de interés de la empresa ofertante. Esto permite validar que el correo electrónico es correcto y veraz.



Sabadell
Hub Empresa

PYME LEGAL
17 AÑOS
acompañándote

WWW.PYMELEGAL.ES
info@pymelegal.es

Consultoria especializada en
protección de datos y registro de marcas.

PymeLegal, S.L.

Diagonal, 363, 2o 1a
08037 Barcelona
T: 93 737 64 01