¿Cómo hacer que tu web cumpla con la Ley de Protección de Datos?

Georgina Andrés
Abogada – Coordinadora Área Legal Pymelegal – DPD Certificada
✉ gina@pymelegal.es

Jaume Feliu
Ingeniero – CEO Pymelegal – DPD Certificado
✉ jaume@pymelegal.es

PYME LEGAL

nominalia

Índice

M1.

Contexto Normativo:
¿A qué nos obliga la ley?

¿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

Futuro reglamento e-Privacy

Objetivos del RGPD

- Respetar y proteger los derechos de los ciudadanos europeos.
- Dar más garantías y mayor control al ciudadano sobre sus datos.
- Crear un marco normativo único para toda la UE.
- Libre circulación de datos personales en la UE.
- Que las empresas establezcan medidas de seguridad legales, técnicas y organizativas para garantizar que los datos se traten de forma leal, para fines concretos para fines concretos y sobre unas determinadas bases jurídicas (normalmente el consentimiento de la persona).

M2.

Ámbito de aplicación:
¡Cúrate en salud y evita sanciones!

¿Qué son datos personales? (Ámbito objetivo)

DATO DE CARÁCTER PERSONAL: "cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables".

Persona física identificada

Cuando se indica directamente a esa persona sin necesidad de utilizar un conjunto de medios para poder averiguar su identidad.

Persona identificable

Cuando la identidad de una persona puede determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social.

Tipos de datos personales

GENÉRICOS	ESPECIALMENTE SENSIBLES (9 RGPD)	INFRACCIONES Y CONDENAS (10 RGPD)	CONSIDERANDO 75 (RGPD)
Nombre y apellidos	Políticos, filosóficos, religiosos	Penales	Menores y colectivos vulnerables
Teléfono/Mail	Salud, vida u orientación sexual	Administrativas	Rendimiento laboral, situación económica
Fotografías/Vídeos/Imágenes	Genéticos o biométricos		Preferencias o intereses personales
Dirección	Afiliación sindical		Geolocalización
Datos bancarios	Origen étnico o racial		Evaluación de aspectos personales

Datos excluidos

DATOS EXCLUIDOS de protección del RGPD y LOPDGDD

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.

Ámbito de aplicación territorial del RGPD

¿Dónde se aplica el RGPD?

TERRITORIAL

- Establecimiento ubicado en la UE, independientemente de que el tratamiento tenga lugar en la UE o no

- Establecimiento no ubicado en la UE, pero que trate datos de interesados residentes en la UE, cuando las actividades de tratamiento estén relacionadas con
    - O la oferta de bienes o servicios en la UE
    - O el control de su comportamiento, realizado en la UE

Sanciones

GRAVES:

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

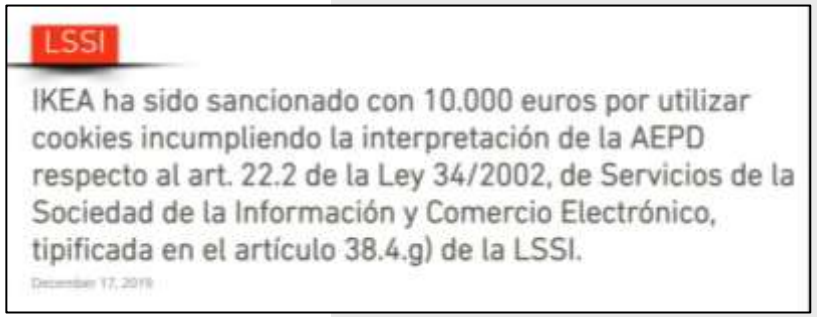
- Tratar datos de menores sin su consentimiento
- No aplicar medidas técnicas ni organizativas por defecto
- No disponer de Registro de actividades de tratamiento
- No notificar violaciones de seguridad
- No realizar evaluación de impacto
- No designar DPO

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 (España hasta 2020)


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.


La Agencia Española de Protección de Datos multa a RTVE por carecer de medidas de seguridad adecuadas en el tratamiento de datos

A finales de noviembre de 2019, la AEPD impuso en su resolución PS/00305/2019 una **multa de 60.000 euros a la empresa Corporación de Radio y Televisión Española S.A.** ("RTVE") **por carecer de medidas de seguridad adecuadas para proteger los datos personales de sus trabajadores.**


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 (Europa)

Primera multa en Europa por incumplimiento del RGPD: 400.000€ de sanción

Medio año después de la entrada en vigor del **Reglamento General de Protección de Datos (RGPD)** de la Unión Europea, la Agencia Portuguesa de Protección de Datos (CNPD por sus siglas en portugués) ha impuesto la **primera multa por incumplimiento de la normativa en toda Europa**.

El "agraciado" ha sido el **Centro Hospitalario Barreiro-Montijo**, situado al sur del país luso, con una sanción que asciende a un total de **400.000 euros** por permitir el **acceso ilícito a datos clínicos**. La autoridad portuguesa inició una investigación tras recibir un aviso por parte del Colegio Oficial de Médicos de Portugal.

Alemania impone una multa de 14,5 millones de euros a una empresa inmobiliaria por infracción del RGPD

Francia multa con 50 millones a Google por infringir las normas de protección de datos

- La sanción se ha impuesto por falta de transparencia, la información insatisfactoria proporcionada y la falta de consentimiento válido para la personalización de publicidad

En el caso de Reino Unido, el regulador ICO ha anunciado las mayores sanciones, por importe de 204 millones de euros a British Airways y 110 millones a Marriot Hoteles, en ambos casos por medidas de seguridad inadecuadas.

M3.

Principios:
¿Cuándo y cómo podemos tratar los datos?

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

Art. 5 RGPD: *Los datos personales deben ser tratados de acuerdo con el principio de* ***licitud, lealtad y ser transparentes*** *en relación con el interesado*.

Un tratamiento de datos, para ser considerado lícito, leal y transparente, deberá ajustarse a alguna de las circunstancias previstas por el RGPD, que veremos más adelante.

La información debe ser **facilitada de forma accesible** a los interesados e **indicando toda la información** necesaria para que el tratamiento sea transparente, y no dé lugar a dudas.

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

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.

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

LIMITACIÓN DE LOS FINES

Para iniciar un tratamiento de datos es necesario haber informado previamente de todas las **finalidades determinadas, explícitas y legítimas** para las que van a tratarse, y si ello no fuera posible y se añadieran una vez ya se esta realizando dicho tratamiento, se informará inmediatamente antes de la realización del mismo, siempre basándose en alguna de las legitimaciones para que el tratamiento sea lícito.

Las distintas finalidades añadidas posteriormente **nunca podrán ser incompatibles** con las finalidades iniciales.

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

MINIMIZACIÓN DE LOS DATOS

Los datos deberán ser objeto de tratamiento de forma **adecuada a la finalidad, pertinente y limitada** a lo necesario en relación con los fines para los que son tratados.

EXACTITUD

Los datos siempre **deberán estar actualizados y ser veraces** con respecto a los fines para los que se tratan.

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

LIMITACIÓN DEL PLAZO DE CONSERVACIÓN

Los datos sólo podrán mantenerse durante el tiempo necesario para cumplir los fines por los que se recopilaron.

Deberá haber una lista con todos los plazos de conservación o criterios para valorarlo según la normativa vigente.

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

DISPONIBILIDAD, INTEGRIDAD Y CONFIDENCIALIDAD

Deberán implementarse las medidas técnicas y organizativas adecuadas para proteger los datos contra tratamientos no autorizados o ilícitos y su pérdida, destrucción o daño accidentales, y sobretodo garantizar los **tres pilares de la seguridad de la información**:

LA **CONFIDENCIALIDAD**: que requiere que la **información sea accesible de forma única** a las personas que se encuentran autorizadas.

LA **INTEGRIDAD**: supone que **la información se mantenga inalterada** ante accidentes o intentos maliciosos. Sólo se podrá modificar la información mediante autorización. El objetivo de la integridad es **prevenir modificaciones no autorizadas de la información**.

LA **DISPONIBILIDAD**: supone que **el sistema informático se mantenga trabajando sin sufrir ninguna degradación en cuanto a accesos**. Es necesario que se ofrezcan los recursos que requieran los usuarios autorizados cuando se necesiten. La información deberá permanecer accesible a elementos autorizados.

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

INFORMAR: ¿CÓMO?

LA PRIMERA CAPA

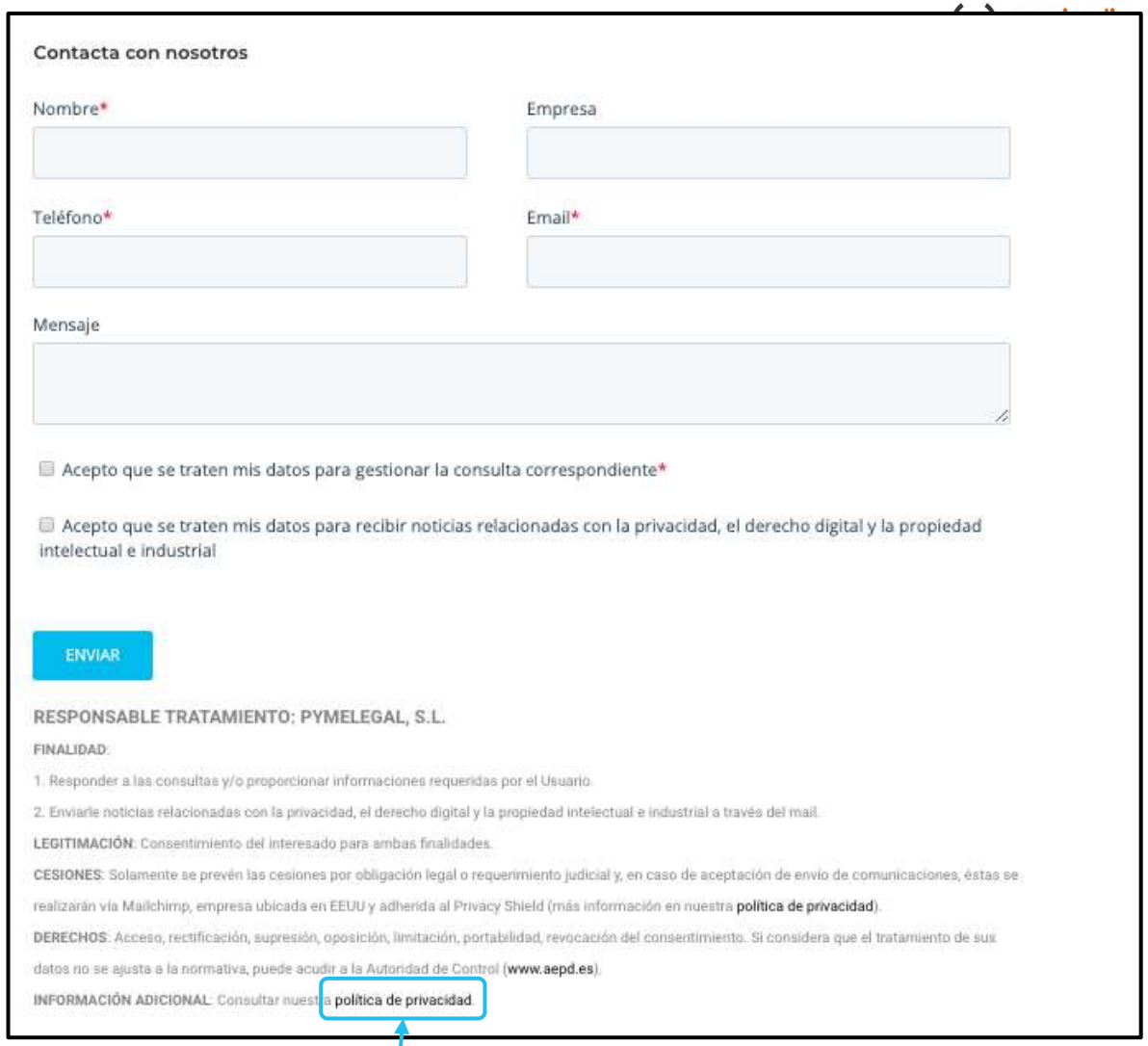
Consiste en la información básica para el interesado, que debe estar de forma resumida, y se debe ofrecer en el mismo momento en que se recopila la información y por el mismo medio por el cual se recojan los datos.

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

LA SEGUNDA CAPA

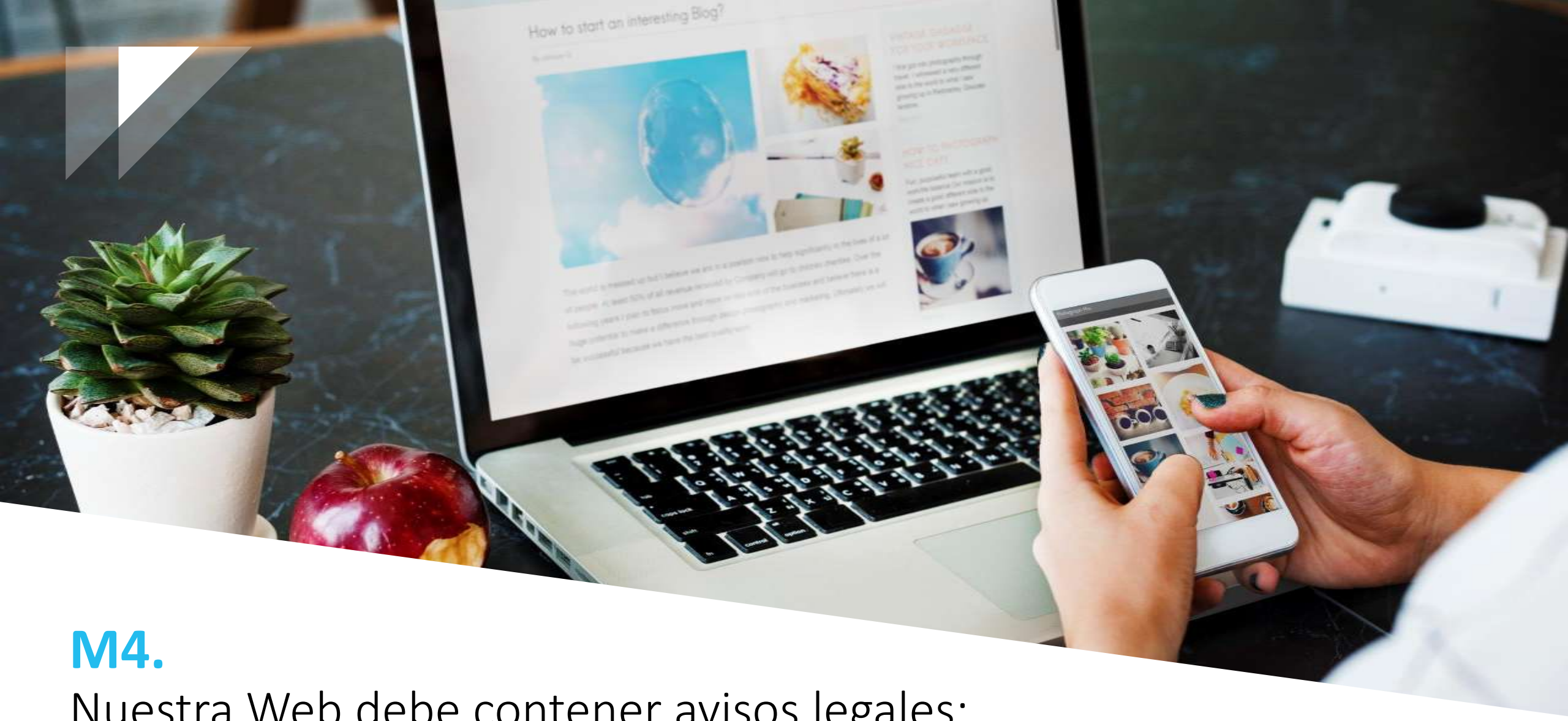
Debe encontrarse la información de forma detallada, en un medio más adecuado para su presentación y compresión por el interesado.

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



¿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



M4.

Nuestra Web debe contener avisos legales: ¿cuáles?

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.

Los “must” de toda página web:

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

Otros:

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

Páginas web

AVISO LEGAL

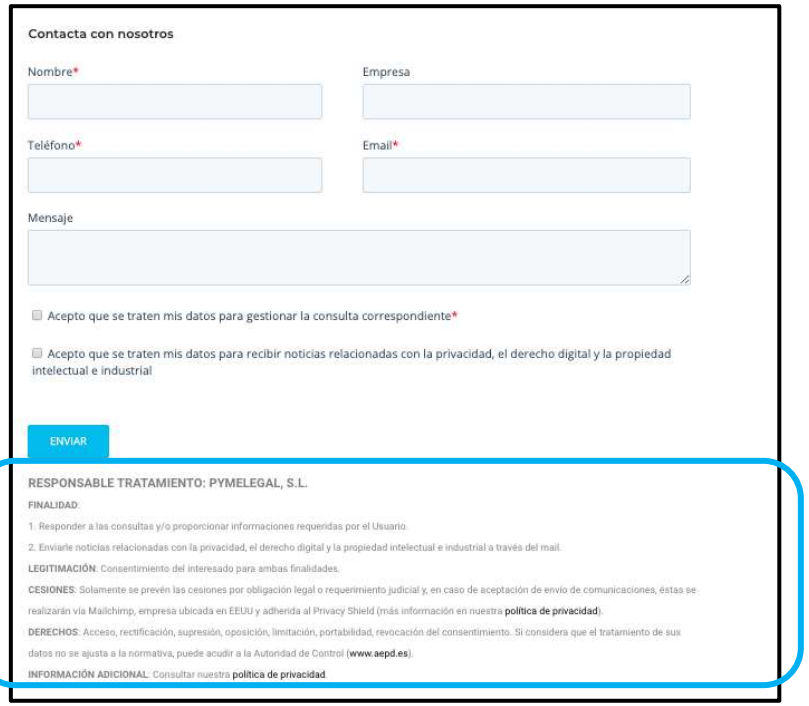
- Objetivo fundamental:
  - Indicar responsable del la web
  - Indicar Términos y condiciones de uso de la misma
- Información obligatoria LSSICE (art. 10)
- Garantías y responsabilidades por parte del Responsable
- Condiciones de los hiperenlaces,
- Propiedad intelectual e industrial de la página y
- Legislación aplicable

Páginas web

POLITICA DE PRIVACIDAD

- Información por capas
- Información sobre el tratamiento de datos
- Información de interés para el usuario
- Datos del responsable de tratamiento
- Envío comunicaciones electrónicas
- Política redes sociales
- Cesiones y transferencias
- Datos DPD (si tienen)
- Periodo de conservación e los datos
- …

Primera capa



Segunda Capa

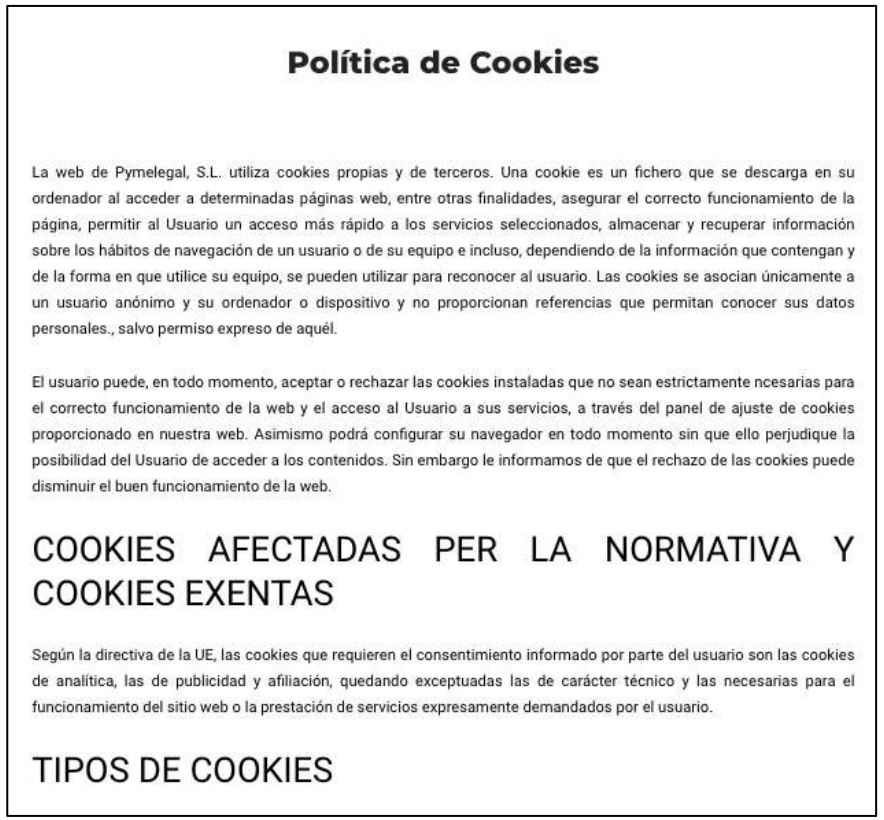
Páginas web

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.

RESUMEN

¿Cuándo una web debe cumplir el RGPD?

- ❑ Cuando tienes en tu web un formulario de contacto.
- ❑ Cuando tienes en tu web un formulario de suscripción.
- ❑ Cuando los visitantes de tu web pueden registrarse.
- ❑ Cuando tu web tiene un formulario de alta como afiliado o participa de programas de afiliados de terceros.
- ❑ Cuando vendes productos, servicios o infoproductos.
- ❑ Cuando se realizan promociones en redes sociales.
- ❑ Cuando en la web hay un formulario de inscripción para Webinars.
- ❑ Cuando se está utilizando Google Analytics u otro similar de análisis y/o métrica.
- ❑ Cuando se realizan campañas de email-marketing.

M5.

Campañas de marketing: ¿Hasta dónde podemos llegar?

Campañas de marqueting

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

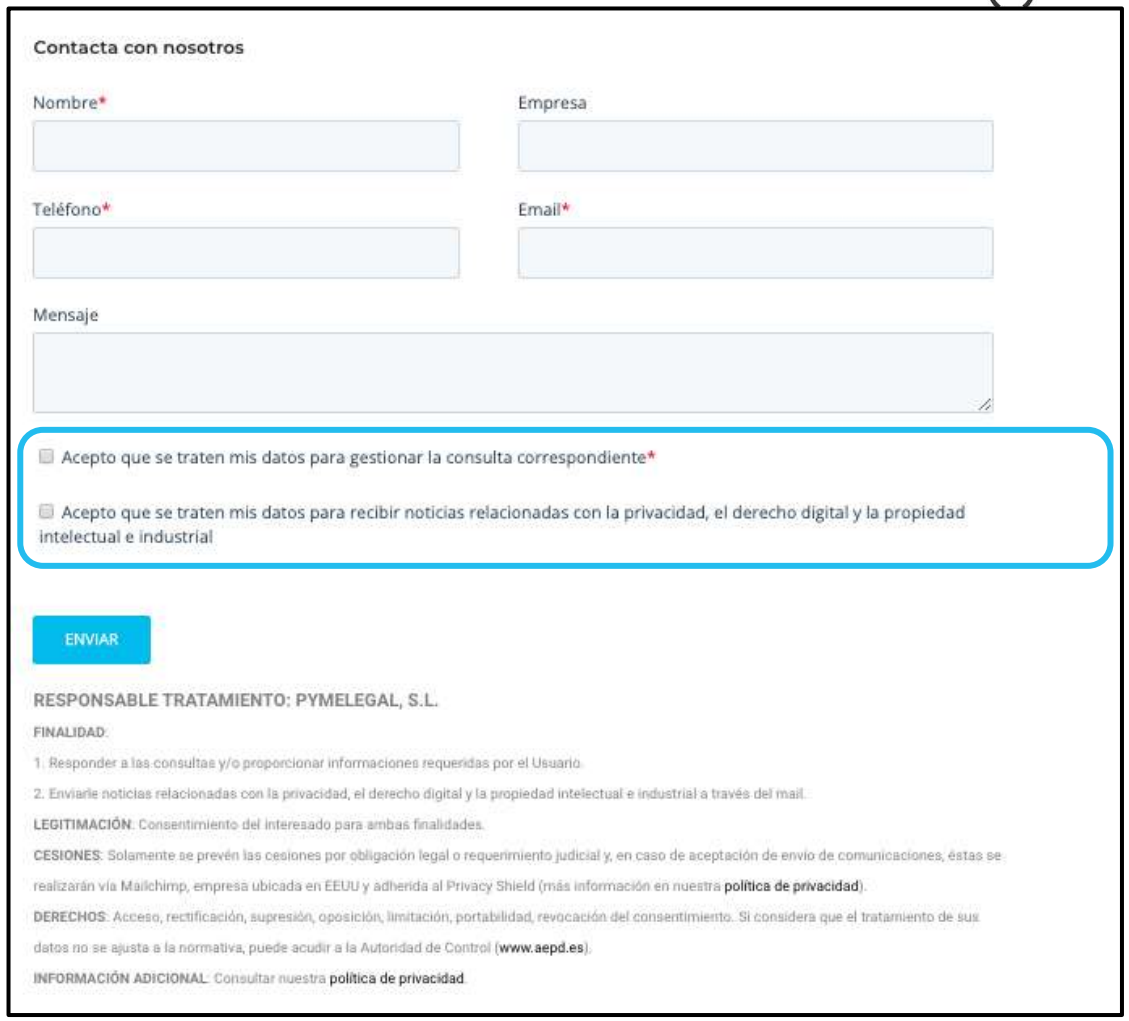
01. DESAGREGAR LAS FINALIDADES

- 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.



RECUERDA ….

- **No se pueden realizar campañas de email marketing si no se tiene un consentimiento válido de los usuarios** que se tengan en las listas.
- Se deberá informar en cada campaña de los aspectos esenciales del tratamiento y habilitar un mecanismo automático para revocar el consentimiento previo.
- Si se utilizan además herramientas de segmentación, se tiene un esquema de afiliados o se comparten datos con otras herramientas, éstas deberán garantizarnos que cumplen con el RGPD.
- Informar con la máxima transparencia al recoger los datos y requerir el consentimiento expreso, informado, inequívoco y libre.
- Todas las comunicaciones comerciales que se emitan deberán cumplir rigurosamente con los principios del RGPD y permitir al usuario el ejercicio de sus derechos en cualquier momento.
- Implementar medidas de seguridad adecuadas a las bases de datos de usuarios, suscriptores y clientes.
- Poder acreditar todas esas medidas en cualquier momento, incluyendo el haber guardado los consentimientos obtenidos hasta que el usuario se dé de baja.

CHECKLIST

¿Cumple mi web?

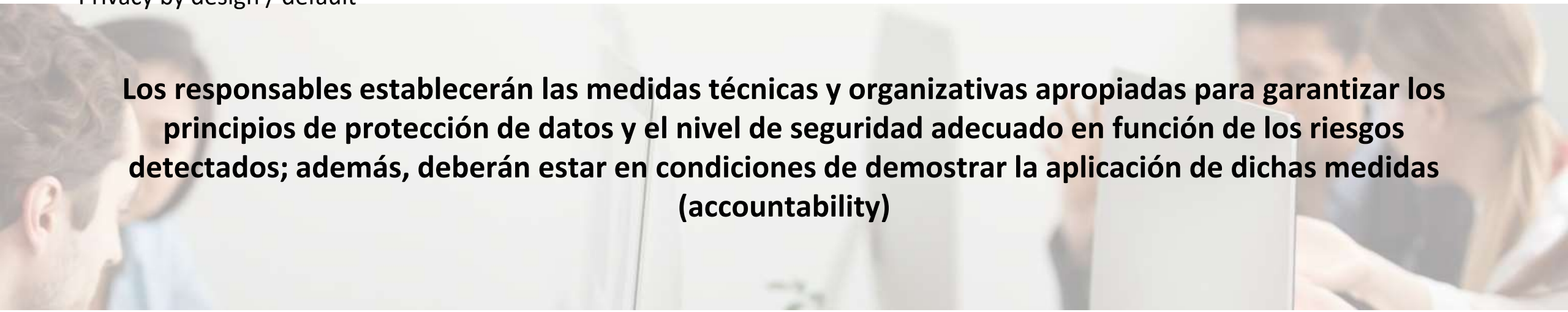
- ¿Tienes los textos legales de Aviso legal, Política de privacidad y Pol. De cookies visible en todas las páginas de la web?
- ¿Los textos legales están adaptados a las exigencias del RGPD y de la LOPDGDD así como de la LSSICE?
- Cuando se entra a la web, ¿salta el banner de aceptación/rechazo de cookies?
- En los formularios, ¿se recogen los datos mediante el doble – opt in?
- ¿se recoge el consentimiento de forma expresa?
- Todos los formularios de la web disponen de la primera capa informativa que redirija a la segunda capa?

M6.

Obligaciones del Responsable del tratamiento: ¿Qué se debe tener en cuenta?

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)

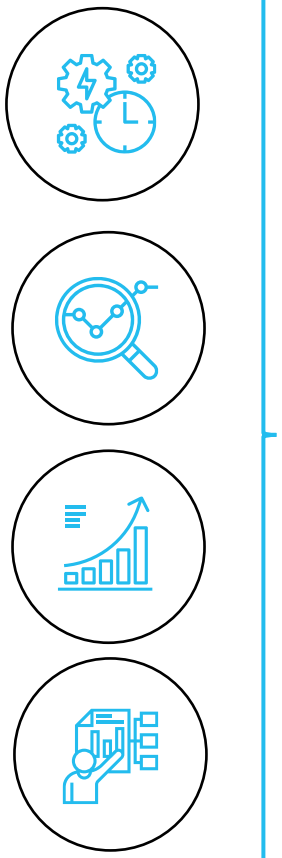
Privacidad desde el DISEÑO (by design)

- **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** (ej.: seudonimización).

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).

Obligaciones del Responsable Tratamiento



- Garantizar los **principios de la protección de datos**.
- **Informar debidamente** a los usuarios
- Disponer del **Registro de Actividades de Tratamiento** (RAT).
- Realizar un **análisis de riesgos** y/o **evaluación de impacto** (si procede).
- Garantizar los **derechos de los afectados**.
- Designar **Delegado Protección de Datos** (si procede).
- Regular **transferencias internacionales** de datos (si procede).
- Regular relación con **encargados de tratamiento**.
- **Protocolo trabajadores**.
- **Aplicar medidas técnicas y organizativas**.
- **Protocolo brechas** de seguridad.

Gestión de los derechos

DERECHOS

La protección de los datos personales es un derecho fundamental de la persona y para su defensa la Ley y el RGPD reconocen y amparan los derechos de los ciudadanos al control y disponibilidad de sus datos ante los terceros que los tratan.

PROTOCOLO INTERNO

Se deberá **desarrollar un protocolo interno** para facilitar a los interesados el ejercicio de estos derechos. Todos los usuarios autorizados para tratamiento de datos deberán conocer este protocolo.

GESTION DERECHOS

El ejercicio de estos derechos se debe llevar a cabo mediante **medios sencillos, visibles y accesibles** puestos a disposición por el responsable del tratamiento a los afectados.

TUTELA DE DERECHOS

Si la persona reclamante cree que sus derechos no han sido atendidos en forma y plazo según la normativa legal vigente, puede **acudir a la tutela de la Autoridad de control pertinente (en España** la Agencia Española de Protección de Datos (AEPD)).

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

DERECHOS DIGITALES (TÍTULO X LOPDGDD)

DERECHO DE RECTIFICACIÓN EN INTERNET

DERECHO AL OLVIDO EN BÚSQUEDAS DE INTERNET

DERECHO A LA NEUTRALIDAD DE INTERNET y ACCESO UNIVERSAL A INTERNET

PROTECCIÓN DE LOS MENORES EN INTERNET

POLÍTICAS DE IMPULSO

DERECHO AL OLVIDO EN SERVICIOS DE REDES SOCIALES Y SERVICIOS EQUIVALENTES

USO DE DISPOSITIVOS EN EL ÁMBITO LABORAL

VIDEOVIGILANCIA EN EL LUGAR DE TRABAJO

DERECHO A LA ACTUALIZACIÓN DE INFORMACIONES EN MEDIOS DE COMUNICACIÓN DIGITALES

PROTECCIÓN DE DATOS DE LOS MENORES EN INTERNET

DERECHO A LA SEGURIDAD DIGITAL

DERECHO A LA EDUCACIÓN DIGITAL

DERECHO DE PORTABILIDAD EN SERVICIOS DE REDES SOCIALES Y SERVICIOS EQUIVALENTES

DERECHO AL TESTAMENTO DIGITAL

DERECHO DESCONEXIÓN DIGITAL

SISTEMAS DE GEOLOCALIZACIÓN

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**, sin sustituir las funciones que desarrollan las Autoridades de Control (en este caso, la Agencia de Protección de Datos).

Al Delegado de Protección de Datos, que deberá contar con conocimientos especializados del Derecho y en protección de datos, y que actuará de forma independiente, **se le atribuyen una serie de funciones reguladas en el artículo 39 del RGPD** y **artículo 34 de la LOPDGDD**, entre las que destacan informar y asesorar, así como supervisar el cumplimiento del citado RGPD por parte de la empresa o el profesional que trata datos de carácter personal.

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.

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**.

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.

EMPLEADOS

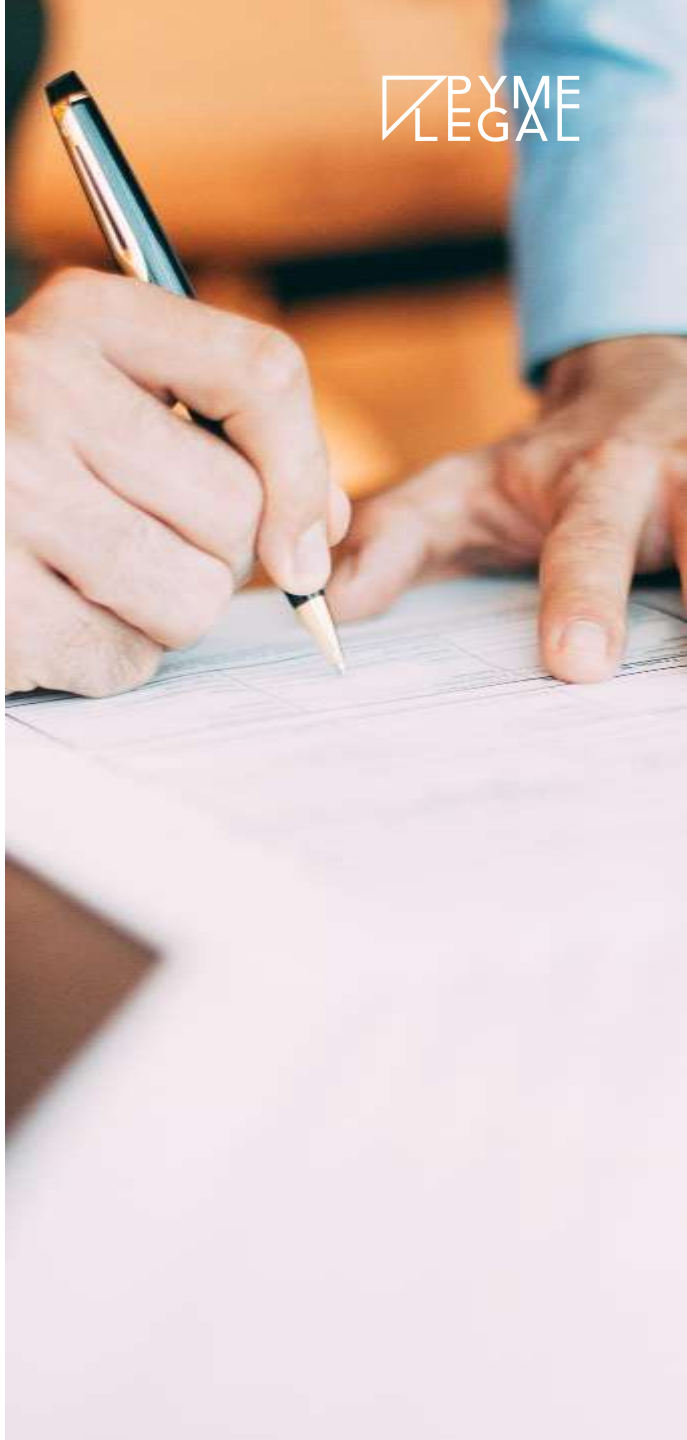
El Responsable de Tratamiento deberá asegurarse de que **sus empleados conocen la normativa de RGPD, velan por la confidencialidad, integridad y disponibilidad** y cumplen en todo caso con las directrices marcadas con la empresa:

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.



MEDIDAS DE SEGURIDAD

Los datos que el empresario ya ha obtenido de forma legítima deben tratarse **aplicando una serie de medidas de seguridad diseñadas para garantizar que los datos no van a ser accesibles a terceros, van a mantenerse íntegros y seguros y estarán protegidos de amenazas**.

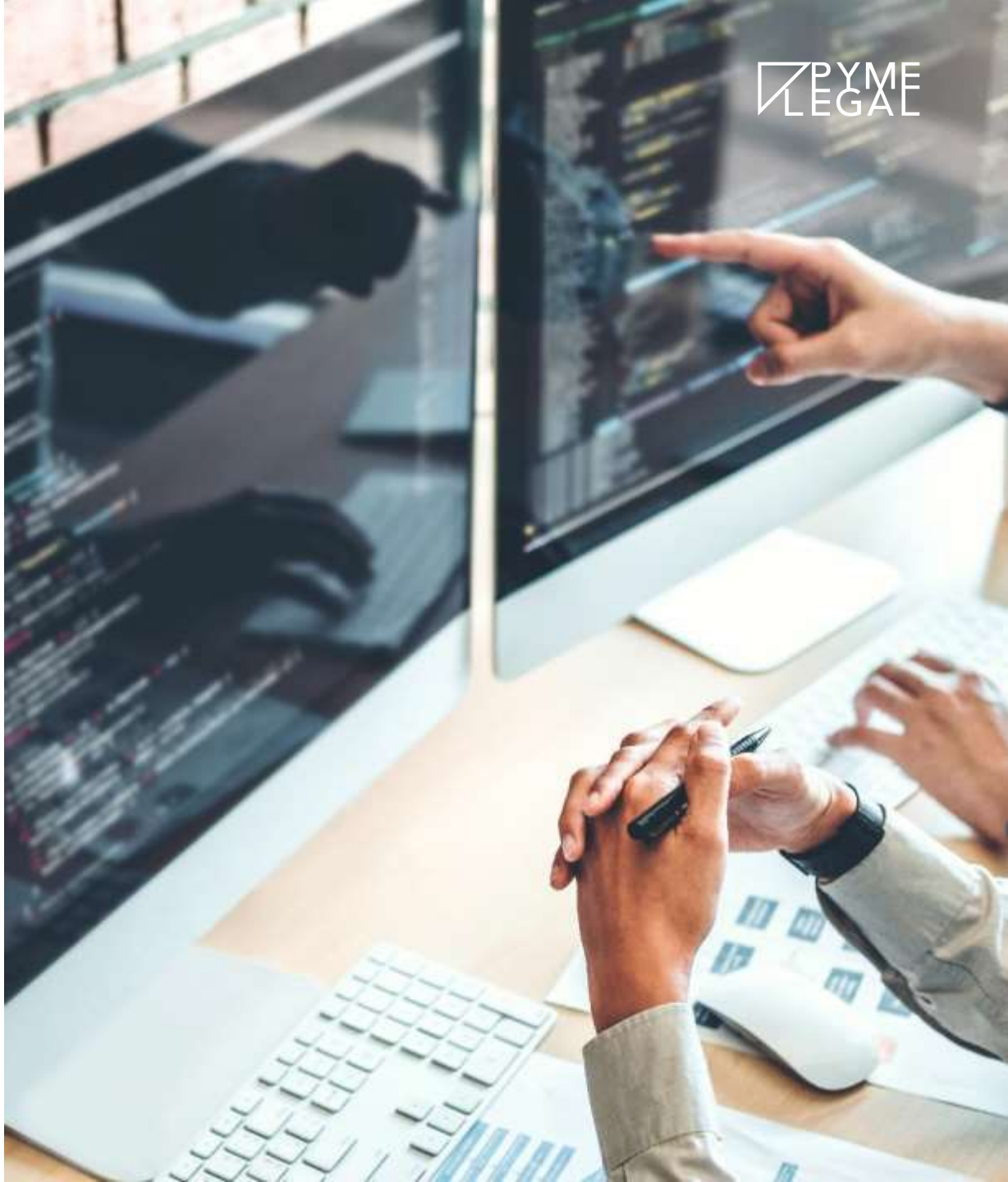
*'Los responsables y **encargados establecerán las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos detectados en un análisis previo**; además, **deberán estar en condiciones de demostrar la aplicación de dichas medidas** (responsabilidad activa).'*

ESTAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS SE DEBERÁN ESTABLECER TENIENDO EN CUENTA:

- El coste de la técnica
- Los costes de aplicación
- La naturaleza, alcance, contexto y las finalidades del tratamiento
- Los riesgos para los derechos y libertades

ALGUNAS MEDIDAS MÍNIMAS (ART.32):

- Seudonimización y cifrado
- Capacidad de restauración
- Capacidad de garantizar:
  - Confidencialidad
  - Integridad
  - Disponibilidad



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

M7.

Cómo resolver las Brechas de Seguridad: para empezar, ¡no entrar en pánico!

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.**

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


DELITOS EN LA RED

Los ciberdelitos se disparan y multiplican hoy por cinco las cifras de hace nueve años

Las infracciones penales por los fraudes informáticos experimentan la mayor curva de crecimiento exponencial, junto a los asuntos sexuales

La **pandemia y el 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 2021 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:** La página web de la empresa es un **activo importante**, los ciberdelincuentes buscarán atacarla por diversos motivos, como hacerse con información confidencial, utilizarla para perpetrar nuevos ataques o para dañar la imagen de la organización.
- **Ransomware**
- **Fraude del falso soporte de Microsoft**
- **Campañas de correos electrónicos con *malware***
- **Ataques de denegación de servicios.**
- **…**

Anexo

Errores Habituales

Errores

- No antender los derechos de un usuario (baja newsletter)
- Controlar el correo electrónico del trabajador sin informar
- Pensar: '*yo no trato datos; no me afecta…*'
- Copiar el aviso legal de otra página web
- Realizar la adaptación a la normativa a 'coste cero' (Fundae)
- No tener implantadas medidas de seguridad
- No atender las brechas de seguridad ni comunicarlas
- No hacer copias de seguridad

nominalia

PYME LEGAL

WWW.PYMELEGAL.ES

info@pymelegal.es

Consultoría especializada en
protección de datos y registro de marcas.

PymeLegal, S.L.

c/Pau Claris, 156 3-1 08009 Barcelona
T: 93 737 64 01