GUÍA PARA DESARROLLADORES WEB

Cómo insertar los textos legales en tu web

ADECUACIÓN LEGISLATIVA

BLOG, WEB Y E-COMMERCE

MARINA BROCCA

RGPD · MARKETING · E-COMMERCE

www.marinabrocca.com

GUÍA PARA DESARROLLADORES WEB

Adecuación LSSICE WEB E-COMMERCE

Esta es la guía que he preparado para ayudarte a adecuar tu blog paso y paso y saber cómo insertar los diferentes elementos que he desarrollado para tu web, blog o e-commerce.

Índice:

1. ¿DÓNDE INSERTAS LOS DIFERENTES TEXTOS LEGALES?

Hemos redactado esta guía con el objetivo de ayudar a los desarrolladores web a que puedan implementar todos los mecanismos y elementos informativos que exige la actual legislación española y europea a los sites en internet.

Estos son los textos indispensables, dependiendo de la casuística del proyecto web:

Footer de la web:

- ✔ Aviso legal
- ✔ Política de privacidad
- ✔ Política de cookies
- ✔ Faldón de cookies
- ✔ Condiciones de contratación (si tienes un e-commerce)

Formularios:

- ✔ Leyenda legal pie email
- ✔ Leyenda legal formulario blog
- ✔ Leyenda legal formulario contacto
- ✔ Leyenda legal formulario descarga
- ✔ Leyenda legal formulario servicios
- ✔ Leyenda legal formulario webinar
- ✔ Leyenda legal formulario suscripción
- ✔ Leyenda legal pie boletines

El aviso legal, la política de privacidad, las condiciones de contratación y la política de cookies deben constar separados, para mayor entendimiento y transparencia en las páginas de inicio y en todas las subpáginas. Los tres textos se relacionan entre sí y es necesario introducir los enlaces correspondientes donde proceda (van subrayados).

Footer marinabrocca.com

2. ¿CÓMO CUMPLIR CON LA "LEY DE COOKIES?

Uno de los puntos más importantes a la hora de aplicar la normativa es la necesidad de informar al usuario explícitamente sobre **la utilización de cookies en nuestra página web**, en especial en cuando se utilizan **cookies de terceros** (análiticas, publicitarias, de afiliados, etc.)

Hay dos tipos de cookies: las estrictamente necesarias para la navegación y las que no. Las que no son estrictamente necesarias para la navegación y que suelen ser las estadísticas y otras de seguimiento, requieren el consentimiento del usuario. Es decir, que la web no puede descargar esta cookies hasta que el usuario acepta las mismas. Las que son estrictamente necesarias, como las de autenticación u otras, no requieren el consentimiento y pueden/deben instalarse directamente, independientemente de que se haya informado previamente al usuario sobre su existencia.

Cookies exentas de información y consentimiento

- Cookies de entrada de usuario
- Cookies de seguridad y autentificación o identificación del usuario
- Cookies de sesión del reproductor multimedia
- Cookies de sesión para equilibrar la carga
- Cookies de personalización de la interfaz de usuario
- Cookies de complemento para intercambiar contenidos sociales

Para informar de las cookies, hay varias formas:

Existen varios métodos para informar al usuario:

- Página de bienvenida con información sobre cookies y botón de aceptar (Como las que preguntan si el usuario es mayor de edad).
- Pop-up previo que suspenda la carga completa de la página hasta la aceptación.
- Cabecera o pie de página con información y una caja de aceptación.
- Paso previo de aceptación dentro del cuadro de reproducción de vídeos, juegos y otras aplicaciones web.

Dependiendo del diseño de la web, debes optar por un método u otro. Os recomendamos que este sea lo menos invasivo posible de cara al usuario para evitar abandonos de la página u otros problemas de usabilidad.

Para plataforma de wordpress, este tipo de anuncio se suele llevar a cabo a través de plugins.

RECOMENDACIÓN:

El plugin gratuito WP GDPR Compliance que es ahora mismo seguramente el mejor plugin disponible a estos efectos.

Con este plugin puedes adecuar el pop up de cookies, obtener registros de consentimientos y de información, los enlaces a la política de cookies, etc.

Este plugin es completamente compatible con la última versión de Contact Form 7, Gravity Forms, WooCommerce y los comentarios de WordPress para que puedas configurar las opciones de consentimiento, así como también la integración de una pestaña de ajustes.

Texto pop-ups advertencia cookies publicitarias:

Utilizamos cookies propias y de terceros para mejorar nuestros servicios y mostrarle publicidad relacionada con sus preferencias mediante el análisis de sus hábitos de navegación. Si continúa navegando, consideramos que acepta su uso. Puede cambiar la configuración u obtener más información 'aquí (poner enlace política de cookies)'.

Texto pop-ups advertencia cookies analíticas:

Utilizamos cookies propias y de terceros para realizar el análisis de la navegación de los usuarios y mejorar nuestros servicios. Si continúa navegando, consideramos que acepta su uso. Puede cambiar la configuración u obtener más información 'aquí (poner enlace política de cookies)'.

3. ¿CÓMO ADECUAR LOS FORMULARIOS?

Requiere siempre la confirmación de lectura o el consentimiento, según el caso:

En el Reglamento Europeo de Protección de Datos (RGPD), se dota de especial relevancia a la obligatoriedad de requerir el consentimiento expreso en muchos casos.

Como cada formulario persigue una finalidad diferente, **es preciso informar de manera específica** en cada uno de esos formularios sobre la finalidad, destinatarios, etc. La aplicación te permite obtener los diferentes textos legales para los diferentes tipos de formularios que tienes en la web.

Cuando un usuario facilita voluntariamente sus datos de carácter personal a través de Internet, debe ser informado y/u otorgar su consentimiento para el tratamiento de los mismos en los términos de los que ha sido convenientemente informado en el momento de la recogida.

Cómo adecuarlos técnicamente:

- **Mediante código:** si sabes programar y conoces el código, lo puedes hacer manualmente.

- **Mediante plugins:** En este caso, puedes utilizar:

  - WP Forms Lite
  - Gravity Forms
  - Contact Form 7

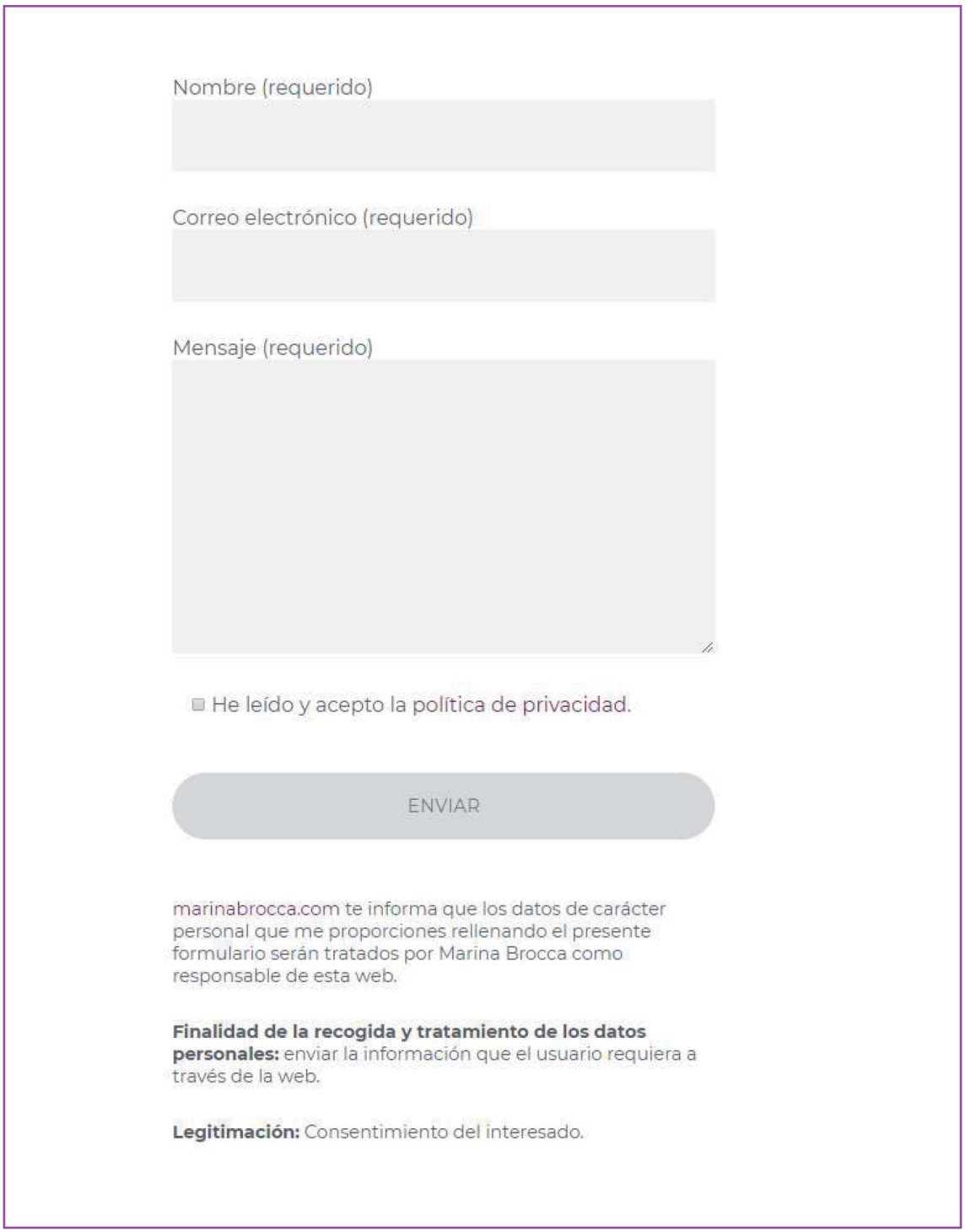
Todo formulario debe:

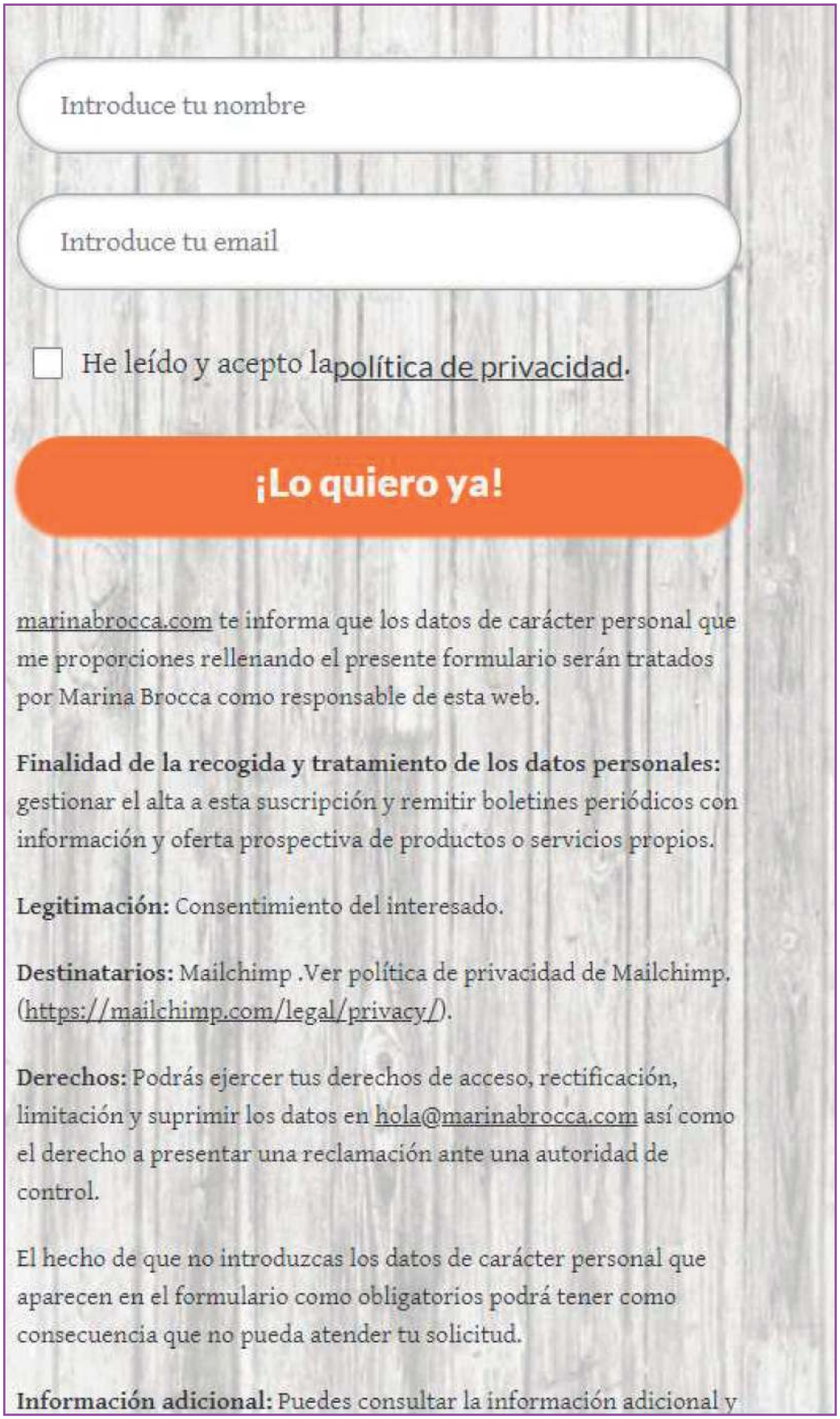
1) Incluir una casilla de aceptación

2) Incluir un enlace hacia la política de privacidad.

3) Incluir una primera capa informativa con la coletilla legal del formulario según su tipología.

Es indispensable recoger la conformidad del usuario con la política de privacidad antes de validar sus datos en cualquier formulario mediante una casilla de "acepto", tal como se expone en los formularios siguientes:




Introduce tu nombre
Introduce tu email
He leído y acepto la política de privacidad.
¡Lo quiero ya!
marinabrocca.com te informa que los datos de carácter personal que me proporciones rellenando el presente formulario serán tratados por Marina Brocca como responsable de esta web.
Finalidad de la recogida y tratamiento de los datos personales: gestionar el alta a esta suscripción y remitir boletines periódicos con información y oferta prospectiva de productos o servicios propios.
Legitimación: Consentimiento del interesado.
Destinatarios: Mailchimp .Ver política de privacidad de Mailchimp. (https://mailchimp.com/legal/privacy/).
Derechos: Podrás ejercer tus derechos de acceso, rectificación, limitación y suprimir los datos en hola@marinabrocca.com así como el derecho a presentar una reclamación ante una autoridad de control.
El hecho de que no introduzcas los datos de carácter personal que aparecen en el formulario como obligatorios podrá tener como consecuencia que no pueda atender tu solicitud.
Información adicional: Puedes consultar la información adicional y

El **"Texto legal pie de formulario web"** es importante que **esté visible en el formulario** para garantizar la información correcta a cada usuario.

Según el tipo de formulario (Venta, contacto, suscripción) **deberás utilizar la cláusula informativa correspondiente que hemos redactado para caso.**

Consentimientos específicos:

Hay tratamientos que requieren consentimiento específico, concretamente en estos casos:

- ✔ Cuando se realiza transferencia internacional de datos (TDI) a un país considerado no seguro y no exista amparo legal para ello (ej: Adhesión de la empresa destinataria al Escudo de Privacidad, existencia de cláusulas tipo, etc.).
- ✔ Cuando existan decisiones automatizadas, incluida la elaboración de perfiles.
- ✔ Cuando se prevea ceder datos a un tercero que requiera el consentimiento del afectado.
- ✔ Cuando se traten datos especialmente protegidos sin que la empresa esté legitimada para ello por cualquier base legal que no sea el consentimiento.

En estos casos, deberás incluir un check box específico para cada caso según la siguiente tabla:

TRATAMIENTO	TEXTO CHECK BOX
Cuando se realiza transferencia internacional de datos (TDI)	Autorizo la transferencia internacional de mis datos a un país fuera de la UE + **información**
Cuando existan decisiones automatizadas, incluida la elaboración de perfiles.	Autorizo que se tomen decisiones automatizadas y la elaboración de perfiles + **información**
Cuando se prevea ceder datos a un tercero.	Autorizo la cesión de mis datos a (indicar razón social) para (indicar finalidad) + **información**
Cuando se traten datos especialmente protegidos.	Autorizo el tratamiento de datos especialmente protegidos para (finalidad) + **información**

Es imprescindible la creación de un **sistema de verificación doble opt-in** para acreditar la identidad y voluntad de los suscriptores y requerir confirmación a su suscripción, también obligatorio. Ten en cuenta que, además, debes asegurarte de la procedencia legítima de esa dirección y esos datos personales y para eso se recurre al envío de un mensaje que, mediante una acción explícita, como el opt in, exige confirmar el deseo de suscripción, por ejemplo.

Finalmente, debes saber que la LSSI prohíbe el envío de comunicaciones comerciales no solicitadas o autorizadas realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes, que no hayan sido autorizadas o expresamente autorizadas y la única manera de acreditar esa autorización es el doble opt-in.

No deberías nunca mandar un correo o un boletín sin informar sobre tu identidad, como has obtenido esos datos, cuál es su finalidad y cómo pueden los destinatarios ejercitar su derecho a acceder, rectificar, cancelar u oponerse al tratamiento de sus datos.

Esta información es obligatoria y debe estar presente en cada nueva comunicación. También es obligatorio darle la posibilidad al usuario de desistir de nuevas comunicaciones en cualquier momento, por eso, debes ofrecer siempre esta posibilidad habilitando un mecanismo para gestionar las bajas.

4. ¿CÓMO REGULARIZAR LOS REGISTROS DE SUSCRIPTORES PREVIOS AL RGPD?

El RGPD, a diferencia del Reglamento de Desarrollo de la LOPD (RDLOPD), no admite formas de consentimiento tácito o por omisión, ya que se basan en la inacción del usuario y no se consideran legítimos desde el punto de vista del RGPD.

Por tanto, los tratamientos iniciados con anterioridad a la aplicación del RGPD sobre la base del consentimiento seguirán siendo legítimos siempre que ese consentimiento se hubiera prestado mediante una manifestación o acción afirmativa, es decir,.en los términos que exige el RGPD, es decir, que sea expreso, inequívoco, específico e informado (Art. 7 RGPD).

En caso de que tu lista no cumpla con ese requisito, es imprescindible que mandes un boletín con el texto indicado en el documento: **Autorización para el tratamiento de datos** (tú lo redactas luego a tu estilo) y vuelvas a pedirles a tus suscriptores que confirmen su voluntad de seguir a tu lado de forma expresa, eso implica la necesidad de hacerlos pasar por el check box y aceptar tus nuevas condiciones de privacidad.

Registros verificables:

El RGPD exige que tus consentimientos sean verificables, es decir, que puedas acreditar los consentimientos. En este sentido, habrá que recabar pruebas de que los consentimientos han sido otorgados mediante un **acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada e inequívoca** del interesado respecto al tratamiento de los datos que le conciernen.

El consentimiento verificable requiere necesariamente de **un registro escrito de cuándo y cómo alguien decidió permitirte procesar sus datos personales.**

La forma correcta sería recabar el consentimiento conforme exige el RGPD y dejar constancia de que todas las personas de nuestra lista, han prestado este consentimiento **mediante un registro.**

¿Cómo llevar un registro de esos consentimientos?

Te recomendamos que obtengas el consentimiento por escrito o **de manera archivable para cada suscriptor**. Este registro por tanto, deberá contener una serie de datos que confirmen la validez de los consentimientos recabados, por ejemplo, deberá contener la fecha en la que se otorgó, la IP, el email y la URL implicados, el nombre del usuario.

Tus formularios y la plataforma de email marketing con la que trabajes, deben permitirte por tanto, recopilar la dirección de correo electrónico, la dirección IP y la marca de tiempo asociada a todos los que envían el formulario.

PARA E-COMMERCE O WEBS CON VENTAS ONLINE

Términos comerciales:

Antes de iniciar la contratación, debes informar al usuario, pudiendo hacerlo a través de su web, de forma «clara, comprensible e inequívoca» sobre:

1. **Los trámites o pasos a seguir para celebrar el contrato.**

2. Si el documento generado, el contrato, va a ser almacenado por el prestador.

3. **Los medios técnicos** que pondrás a disposición del usuario/consumidor para identificar y corregir errores en los datos, la lengua o lenguas en que se podrá formalizar el contrato.

4. **La lengua o lenguas en que se podrá formalizar el contrato.**

5. **El derecho de desistimiento:** Es imprescindible incluir este apartado. Tienes 14 días naturales (incluidos festivos) para que el usuario pueda ejercer su derecho al desistimiento de la compra. **De no existir información expresa sobre este derecho**, el usuario no tendrá que hacer frente a los gastos asociados a la devolución de su compra **y será la empresa la responsable**. Por tanto, si la tienda online no informa correctamente sobre el plazo de desistimiento, la Ley le castiga poniéndoselo más difícil: **el plazo se amplía a 12 meses. ¡Cuidado con no informar!** Un e-commerce legal debe explicar al usuario **cómo ejercitar el derecho a desistimiento** y puede ofrecer la opción de cumplimentar y enviar electrónicamente **el modelo de formulario de desistimiento. Existen excepciones a la aplicación de este derecho. Si la venta de tu servicio o producto está exento de aplicarlo, debes indicarlo en las condiciones de venta y justificarlo.**

6. Son nulas de pleno derecho las cláusulas que impongan a la persona consumidora **una penalización** o renuncia al ejercicio del derecho de desistimiento.

7. También debes informar sobre si el **coste de la devolución** corre por cuenta del comprador o por tu cuenta Si no informas, lo pagarás tú.

8. **El vendedor tiene un plazo de 14 días** para reintegrar al comprador el importe de la compra y los gastos de envío originales (si también los pagó el comprador), pudiendo exigirse el doble si se retrasa. Como vendedor, estás obligado a devolverle al comprador los **gastos de envío iniciales**, pero puedes hacerle pagar al comprador lo que cuesta enviar el producto desde su casa hasta la sede de la tienda (costes de devolución).

9. **La garantía legal de la compra dura dos años en productos físicos nuevos.** Ten en cuenta que hay algunos productos que no están totalmente sujetos a esta norma: es el caso de productos personalizados, precintados (un CD, una crema), que no se puedan devolver por motivos de salud o higiene...

Confirmación de compra:

El e-commerce debe facilitar de forma gratuita al consumidor la confirmación del pedido, sus características esenciales y las condiciones generales del contrato en un soporte duradero (papel, memorias USB, DVD, tarjetas de memoria, correos electrónicos, SMS...).

Si la venta se efectúa por vía telefónica, el vendedor está obligado a tener una confirmación por escrito.

El botón de pago:

El consumidor debe tener claro que si confirma la compra tiene la obligación de efectuar el pago, esto se exige en también en la Ley General para la Defensa de los Derechos de los Consumidores y Usuarios.

Si el pedido online implica una obligación de pago, un e-commerce legal debe establecer un botón o función similar que contenga solo la expresión "pedido con obligación de pago" o una expresión similar que deje claro que la realización del pedido implica la obligación de pagar.

Puedes utilizar expresiones como **"pagar ahora", "comprar ahora" o "confirmar compra",** pero no los términos "confirmar", "registrar" o "pedir ahora".

Importante: Si no figuran las expresiones correctas, el consumidor no estará obligado a pagar.

Hay que generar también una confirmación de compra en el momento que el cliente completa el proceso de pago.

Nueva Orden de IVA APLICADO: Obligaciones del comerciante

Se aplica a todas las compras online y solo afecta a consumidores, no a empresas.

Obliga a que el IVA que se aplica en las compras sea el del país del consumidor y no como sucedía antes, que correspondía al país de origen del vendedor.

Además, desde el 15 de enero las empresas dedicadas al comercio electrónico tienen la obligación de emitir una factura electrónica a todo aquel usuario que lo solicite. Una medida que está incluida dentro del Plan de Impulso a la Factura Electrónica.

Las nuevas normas exigen que los comerciantes **identifiquen el país en el que se encuentra su cliente final** mediante la recopilación de varias pruebas de obligado cumplimiento. Las tiendas de comercio electrónico deberán:

- ✔ Comunicar los ingresos obtenidos por IVA
- ✔ Almacenar durante diez años de la información relativa a las transacciones de IVA
- ✔ Certificar el país de residencia del comprador
- ✔ Garantizar el cumplimiento de los diversos regímenes de IVA existentes en la Unión Europea

Los proveedores que no cumplan con estas reglas podrían ser sancionados en la normativa que marque el estado miembro en el que se ha infringido esta ley fiscal.

¿Cómo gestionar todas las ventas?

Para facilitar la labor de reconocer el IVA apropiado en cada transacción, se ha creado en todos los países un organismo llamado Mini-One-Stop-Shop o MOSS, con el que el usuario a través de un registro inicial, puede hacer las declaraciones del IVA de manera trimestral. Todas ellas podrán gestionarse desde un único portal web.

SEGURIDAD DE LA PLATAFORMA

La seguridad en un e-Commerce es fundamental para garantizar la confianza de los usuarios así como para evitar ataques informáticos y el fraude electrónico. Esto es fundamental para el éxito de un negocio con presencia digital.

El principal peligro para el comercio electrónico, de hecho, es la ignorancia. Hay un montón de maneras de hacer que tu seguridad pueda hacer frente a las amenazas.

El responsable de un e-commerce deberá adoptar medidas para que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

Por tanto, cuando los usuarios registrados en una web tengan acceso on-line a los datos de que dispone el responsable del e-commerce respecto a su persona (sistema de registro de usuario), deberán establecerse procedimientos de identificación, autenticación y control de accesos.

Capas de seguridad recomendadas para una web

1. Utilizar conexiones seguras: Se recomienda utilizar protocolos de seguridad como Secure Sockets Layer (SSL) para la autenticación web y la protección de datos. Esto protege tanto a la empresa como a los clientes y evita que personas ajenas puedan obtener información financiera o importante. Mejor aún, integrar EV SSL (Extended Validation Secure Sockets Layer), para que los clientes sepan que se trata de un sitio web seguro.

En términos generales, los certificados SSL deben incluir y mostrar (todos o al menos uno) su nombre de dominio, nombre del titular, dirección, ciudad, estado y país. También siempre muestra la fecha de expiración del certificado y por supuesto, los detalles de la autoridad certificadora que expide el certificado.

2. No almacenar datos sensibles o desactualizados: No hay necesidad de almacenar miles de registros de los clientes, particularmente números de tarjeta de crédito, fechas de caducidad o códigos CW2 (Card Verification Value). Se recomienda eliminar los registros antiguos de la base de datos y mantener una cantidad mínima de información, suficiente para cargos al usuarios y reembolsos.

3. Usar un sistema de verificación de direcciones: Utilizar un sistema de verificación de direcciones (AVS) y la verificación del valor de la tarjeta (CVV) para las transacciones hechas con tarjetas de crédito y reducir con ello los cargos fraudulentos.

Más Recomendaciones:

1. Debes mantener tu seguridad: Debes tener un software de seguridad que se actualice automáticamente con regularidad.

2. Actualización de tus sistemas operativos con los últimos parches: Esto es absolutamente esencial.