

INFORME LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL (LOPD) Y LEY DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y DE COMERCIO ELECTRÓNICO (LSSI)

La Ley de servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI) regula las situaciones producidas por el avance del comercio electrónico, las nuevas tecnologías e Internet. Establece una serie de obligaciones a los responsables de las páginas Web en las que se realicen actividades comerciales o de promoción.

El objetivo de este informe es dar unas pautas sencillas de asesoramiento, desde un punto de vista jurídico, de aquellos requisitos que en materia de protección de datos y aspectos legales relacionados con la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI) y la Ley de Protección de Datos (LOPD) pueda requerir su proyecto web.

Este informe no sustituye en ningún caso el asesoramiento de una empresa especializada en LOPD y LSSI.

Puntos principales a tener en cuenta:

A) Análisis y Adaptación de la página web referenciada a LSSI:

- Redacción del Aviso Legal de la web.
- Redacción de la Política de Privacidad de la web.
- Inclusión de datos necesarios de identificación relativa a tu empresa en la web o las webs.
- Notificación del nombre de dominio al Registro Mercantil.
- Régimen y asesoramiento mediante informes y redacciones de cláusulas que se deberán implementar en los procedimientos de comunicaciones comerciales.
- Redacción de contratos de colaboración con los enlaces que tengan a terceras páginas.

B) Análisis y Adaptación a la Normativa de Protección de Datos Personales:

En segundo lugar, se procederá a adecuar la Página Web a la normativa de Protección de Datos Personales, únicamente en atención a los procedimientos de recogida de datos personales y la finalidad a la que destinan los datos recogidos, Art. 5 LOPD.

- Notificación de ficheros a la AEPD (Agencia Española de Protección de Datos): clientes, proveedores, personal, etc.

- Contratos de Tratamientos por Cuenta de Terceros con referencia a los alojamientos de los web sites.
- Tratamiento especial en las cláusulas en lo que respecta a imágenes tomadas a los clientes y sobre todo especificar el tratamiento dado a imágenes de personas menores de 14 años.
- Cláusulas Legales de Información de los diferentes formularios de contacto de la página.
- Redacción del documento de seguridad de la empresa.
- Transferencia internacional de datos en el caso de servidores ubicados en otros países.

C) Análisis de la Contratación Electrónica / solicitud de información:

Informe atendiendo a las características de la operativa on-line de la web y relación de las medidas que debe implementar para adecuarse a la normativa vigente en materia de contratación on-line.

Redacción de las Condiciones Generales de Contratación: redacción de las condiciones generales de los productos y servicios del CLIENTE ofertados y comercializados a través de sus páginas Web.

CUESTIONES FORMALES Y PROCEDIMIENTOS

Se entiende **dato de carácter personal** cualquier información concerniente a personas físicas, no jurídicas, identificadas o identificables. Así, el nombre y apellidos de una persona física la identifican y por tanto es un dato de carácter personal; la dirección de correo electrónico, que en principio no parece ser suficiente para identificar a una persona cuando en ésta no aparece el nombre, sí que permite identificarla puesto que podría llegarse hasta ella.

nombre@servidor.com

a.lopez@servidor.es

abgrr45@servidor.com

Las **medidas de seguridad se clasifican en tres niveles**, dependiendo de la sensibilidad de los datos. Por ejemplo, el nivel de sensibilidad de un dato de salud es mayor que el de datos como el nombre o apellidos, pues información como minusvalías o enfermedades puede afectar al honor de una persona en mayor grado que datos como el nombre o teléfono. Por lo tanto, debemos aplicar mayores o menores medidas de seguridad dependiendo del grado de mayor o menor sensibilidad del dato en cuestión. Los niveles de seguridad establecidos por la LOPD son básico, medio y alto.

Datos como el nombre, apellidos y dirección de un usuario son datos de nivel básico.

Son ejemplos de datos de nivel alto los relativos a la salud, ideología, etc. Aunque en un principio pueda no parecerlo, si su empresa realiza el descuento de la cuota sindical en la nómina de sus trabajadores, está manipulando datos de nivel alto. Este simple dato está indicando una ideología. El simple hecho de estar afiliado a un sindicato hace suponer que se tiene su misma ideología, aunque en algún caso esto no sea así exactamente. Otro dato que es de nivel alto es el grado de minusvalía que pueda sufrir un empleado, ese porcentaje, aunque no indique la minusvalía real, proporciona datos sobre la salud del trabajador que hacen que el fichero se considere de nivel alto.

Redactar un documento de seguridad, que deberá recoger, entre otros, aspectos tales como:

- La determinación de los ficheros empleados para almacenar y tratar datos.
- Establecimiento de las medidas normas y procedimientos en materia de seguridad informática.
- El nombramiento de un responsable de seguridad.
- Obligaciones y funciones derivadas del documento de seguridad, tanto para el responsable del fichero como para el responsable de la seguridad, así como para los usuarios que manejan las aplicaciones.
- Etc.

Declaración de los ficheros al Registro General de Protección de Datos (RGPD)

Conforme a lo dispuesto en el artículo 25 de la LOPD, una de las obligaciones fundamentales del responsable del fichero (persona física o jurídica que dispone del tratamiento de los datos personales) es la declaración al RGPD de los diferentes ficheros lógicos que agrupan homogéneamente a los diferentes colectivos o grupos de datos personales tratados en la empresa.

Están obligados a notificar la creación de ficheros para su inscripción en el RGPD, de acuerdo con lo dispuesto en la Ley Orgánica 15/99, aquellas personas físicas o jurídicas, de naturaleza pública o privada, u órgano administrativo, que procedan a la creación de ficheros que contengan datos de carácter personal.

La notificación puede hacerse por Internet, mediante la descarga de un programa informático que se halla en la siguiente dirección https://www.agpd.es/portaIweb/canalresponsable/inscripcion_ficheros/ind_ex-ides-idphp.php

Cumplimiento del deber de información: obtención del consentimiento de los afectados

Uno de los derechos fundamentales de los afectados-personas físicas cuyos datos son objeto de tratamiento por parte del responsable del fichero está relacionado con la obligación de este último de informarle cuando se recaben sus datos personales, de forma **previa, expresa, precisa e inequívoca**, de la existencia de un fichero y su tratamiento, de la finalidad de la recogida y de los destinatarios de la información; de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; así como de la identidad y dirección del responsable, entre otros extremos definidos en el artículo 5 de la LOPD.

El referido derecho a la información previa responde a que el tratamiento de los datos personales **requiere el consentimiento inequívoco** del afectado, salvo que la Ley disponga otra cosa.

De acuerdo con todo lo anterior, habrá que revisar las cláusulas LOPD incluidas en los diferentes contratos y/o formularios utilizados por la empresa para recabar datos personales, al objeto de verificar que con las referidas cláusulas LOPD se da correcto cumplimiento a los correlativos derechos y obligaciones de información y obtención del consentimiento del afectado.

Conservación de los datos de carácter personal

Deberá revisarse la política de conservación de datos personales en la compañía, teniendo en cuenta que la LOPD dispone que los datos personales incluidos en los ficheros y aplicaciones de la misma deberán ser **exactos y actualizados**, por lo que habría que determinar si, superados los plazos de prescripción legal correspondiente, procede o no conservar datos de personas con las que ya no existe ninguna relación jurídica o laboral.

Calidad de los datos objeto de tratamiento

Considerando que los datos personales tratados por el responsable del fichero han de ser **adecuados, pertinentes y no excesivos** para las finalidades **determinadas, explícitas y legítimas** para las que se obtuvieron, habría que revisar la naturaleza de los datos personales tratados en la compañía, al objeto de comprobar que no se incumplen los principios de calidad exigidos en el artículo 4 de la LOPD.

Procedimiento de ejercicio de los derechos de acceso, rectificación, cancelación u oposición

El ejercicio de los derechos de acceso, rectificación, cancelación u oposición por parte de los afectados cuyos datos personales son objeto de tratamiento en sede del responsable del fichero supone necesariamente **disponer de un procedimiento** que permita una rápida y eficaz respuesta para la satisfacción de los mencionados derechos, teniendo en cuenta el riesgo de sanción que gravita ante el eventual incumplimiento de los mismos.

Comunicación de datos de carácter personal

Debe destacarse que, salvo determinadas excepciones dispuestas en el artículo 11 de la LOPD, toda cesión o revelación de datos personales a persona distinta del interesado o del responsable del fichero, requiere el consentimiento previo del afectado.

A tal efecto, el responsable del fichero deberá verificar que ha informado y obtenido previamente de los afectados el consentimiento para la cesión de sus datos (relaciones matriz-filial, etc.), toda vez que su incumplimiento puede suponer una infracción grave o muy grave.

Régimen jurídico aplicable al encargado del tratamiento

Como excepción al estricto régimen previsto para la comunicación de datos, existe la posibilidad de justificar el acceso de un tercero a determinados datos personales tratados por el responsable del fichero cuando dicho acceso sea necesario para la prestación de un servicio. La citada figura sería el **encargado del tratamiento**, que exigirá, en todo caso, la documentación contractual de la referida

prestación de servicios y la inclusión en el contrato de determinadas cláusulas legales, previstas en el artículo 12 de la LOPD.

Deber de secreto

Una obligación que no debe ser descuidada por las empresas como responsables de ficheros es la necesaria formación de su personal en la normativa de aplicación en materia de protección de datos personales. Así mismo, deberá obtenerse el deber de secreto y confidencialidad de los referidos trabajadores en cuanto a su acceso a determinados datos personales.

Asimismo debe velar por que los datos no sean accesibles por terceras personas no autorizadas, mediante la adopción de medidas de seguridad tanto físicas como informáticas.

Medidas de seguridad

Otro deber significativo que debe mencionarse es la obligación que atañe a todas las empresas de implementar las medidas de seguridad que salvaguarden los datos de carácter personal registrados en ficheros automatizados.

Dichas medidas han sido desarrolladas reglamentariamente por el Real Decreto 994/1999, de 11 de junio. Las más importantes son:

- Existencia de un Responsable de Seguridad.
- Existencia de un Documento de Seguridad actualizado.
- Realización de una auditoría interna o externa cada dos años.

Ubicación del servidor

El problema es ubicar el lugar dónde se realiza el tratamiento, importante a los efectos de la sujeción a la norma. Si los servidores se encuentran en España o la UE no habrá problema, pero si los mismos se encuentran, por ejemplo, en Estados Unidos, la solución no es tan sencilla. El problema radica en que "físicamente" los datos están alojados en el servidor, pero las órdenes al sistema se transmiten desde España. La seguridad obliga a establecer que el tratamiento se efectúa en el lugar en que se toman las decisiones, en este caso España, y por lo tanto con sometimiento a la norma.

Resumen de la LOPD

1 Debes Notificar el fichero a la Agencia Española de Protección de Datos para inscribirlo en el Registro General de Protección de Datos.

2 Debes recoger los datos respetando el principio de calidad de los datos (art 4), informando debidamente al titular de los datos (art 5) y obteniendo su consentimiento en los casos en que sea necesario (art 6).

3 Debes redactar un documento de seguridad e implantar las medidas de seguridad necesarias (art 9).

4 Debes cumplir y hacer cumplir el deber de secreto (art 10).

5 Si vas a entregar los datos a terceros debes hacerlo aplicando lo dispuesto en el art 11.

6 Si vas a permitir que alguien acceda a los datos debes hacerlo aplicando lo dispuesto en el art 12.

7 Si vas a enviar los datos fuera de España debes hacerlo aplicando lo dispuesto en el art 33 y 34.

8 Debes facilitar a las personas el ejercicio de sus derechos ARCO (acceso, rectificación, cancelación y oposición) contestándoles dentro de los plazos establecidos.

IMÁGENES

Las imágenes (fotografías, vídeos u otro elemento gráfico) donde aparezcan personas que participen en las actividades de tu empresa son también datos de carácter personal.

Para las imágenes de clientes que almacenes en los equipos de tu empresa deberás especificarlo en las cláusulas ya que también requiere tratamiento de datos, tanto si las publicas en web como si no lo haces.

Es decir, en los contratos a firmar por los clientes (tanto en formato papel como electrónico) deberás explicar que en el desarrollo de las actividades se realizarán fotografías o vídeos que luego se podrán ver en alguna plataforma:

- Indicar si el acceso a esas imágenes es público o restringido, solo las pueden ver los registrados en la web.

- Indicar la finalidad de esas imágenes dentro de tu actividad (condiciones de servicio). Especificar por ello el tratamiento exacto de las mismas.

- Indicar la no transferencia de estas imágenes a terceros ya que tú eres el responsable del fichero sin la previa autorización del usuario del servicio.

- El cliente decide qué uso se debe dar a sus fotos.
- Una vez finalizada la relación con el cliente, eliminar los datos de contacto de los equipos y sistemas de información.

Respecto a aquellas imágenes de menores de catorce años de edad, será requisito imprescindible que se haya obtenido previamente el consentimiento paterno, del tutor o del representante legal para que los datos de carácter personal puedan ser objeto de tratamiento por parte de tu empresa. Por ello deberás especificarlo en las cláusulas.

GLOSARIO DE TÉRMINOS

A los efectos de la LOPD se entenderá por:

- a. **Datos de carácter personal:** cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.
- b. **Fichero:** todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
- c. **Tratamiento de datos:** operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
- d. **Responsable del fichero o tratamiento:** persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.
- e. **Afectado o interesado:** persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.
- f. **Procedimiento de disociación:** todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.
- g. **Encargado del tratamiento:** la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.
- h. **Consentimiento del interesado:** toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
- i. **Cesión o comunicación de datos:** toda revelación de datos realizada a una persona distinta del interesado.
- j. **Fuentes accesibles al público:** aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

DOCUMENTOS DE APOYO

En este enlace encontrarás manuales referentes a diferentes partes de la implementación la LOPD a las empresas.

<https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/index-ides-idphp.php>

TODA LA LEGISLACIÓN AL RESPECTO

<https://www.agpd.es/portalweb/canaldocumentacion/legislacion/estatal/index-ides-idphp.php>

Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI).