

# LOPDGDD y RGPD

## 1. Introducción

En la constitución española aprobada en 1978 se dispone en su artículo 18:

*«Artículo 18 – Derecho a la intimidad de domicilio*

*Se garantizará el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*

*El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.*

*Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.*

*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».*

Hay multitud de directivas nacionales e internacionales, sentencias judiciales, ..., que han resaltado el derecho de toda persona a tener un control sobre sus datos personales, sobre su uso y destino, para impedir su tráfico ilícito y lesivo para su dignidad y derecho. En España, estos principios se han concretado en la **Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)** y en el **Reglamento General de Protección de Datos (RGPD)** que la desarrolla.

Anteriormente la protección sobre los datos personales se regulaba con:

- Ley Orgánica 5/92 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal de 26 de Octubre (**LORTAD**) y el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal (RMS).
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (**LOPD**) y el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal (**RDLOPD**).

## 2. La protección de datos en España

La legislación española establece una serie de obligaciones que cualquier empresa o institución que tenga, mantenga, utilice o trate datos de carácter personal, en soporte informático o en papel, debe cumplir<sup>1</sup>. La normativa no contempla excepciones por tamaño, facturación o sector de actividad, de forma que cualquier empresa está incluida en el ámbito de aplicación de la legislación, siempre que trabaje con ficheros con datos personales.

El nivel de exigencia en cuanto al cumplimiento de la LOPDGDD es el mismo para todas las empresas, sin que se establezcan criterios distintos dependiendo de si es una gran empresa o una microempresa. La LOPDGDD establece un marco general para todos y debe ser cumplida por todos.

Estas obligaciones se aplican a cada una de las fases que conlleva la utilización de los datos:

1. Con carácter previo a la recogida de los datos.
2. Durante el tratamiento de los datos.
3. Una vez finalizado el tratamiento.

El reglamento establece las normas, medidas, procedimientos y mecanismos que se han de adoptar obligatoriamente para garantizar la seguridad respecto a los ficheros automatizados y no

<sup>1</sup> Esto se traduce a que la totalidad de empresas e instituciones están obligadas a proteger los datos de carácter personal que usen.

automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de los datos de carácter personal.

En España, la **Agencia Española de Protección de Datos (AEPD)** es el ente encargado de velar por el control y cumplimiento de la normativa sobre Protección de Datos. Depende del Ministerio de Justicia y entre sus funciones están:



- Controlar la aplicación de la legislación sobre protección de datos.
- Dictar Instrucciones sobre determinados aspectos de la protección de datos de carácter personal. Por ejemplo, instrucciones sobre el tratamiento de los datos personales con fines de vigilancia a través de sistemas de cámaras.
- Atender a las peticiones, reclamaciones y consultas que formulen los titulares de los datos personales
- Ejercer la potestad inspectora y sancionadora .
- Etc.

### 3. Conceptos

Se van a definir una serie de conceptos básicos asociados a la LOPD:

- **Persona identificable:**
  - Toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social.
  - Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.
- **Datos de carácter personal:**
  - Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier tipo concerniente a personas físicas identificadas o identificables.
  - Nombre, DNI, dirección, datos de contacto, currículum vitae, salario, historia clínica, ...
  - Los datos de carácter personal se clasifican en niveles según su seguridad:
    - Datos personales ordinarios
    - Datos protegidos de carácter especial
    - Datos relativos a condenas e infracciones penales
    - Datos que no requieren identificación

Datos personales ordinarios	Datos protegidos de carácter especial	Datos relativos a condenas e infracciones penales
<ul style="list-style-type: none"> <li>■ Nombre y dirección</li> <li>■ Fecha nacimiento</li> <li>■ Características personales</li> <li>■ Circunstancias laborales</li> <li>■ Circunstancias personales</li> <li>■ Académicos y profesionales.</li> <li>■ Empleo y puestos de trabajo</li> <li>■ Información comercial.</li> <li>■ Económico-financieros.</li> <li>■ Transacciones.</li> </ul>	<ul style="list-style-type: none"> <li>■ Origen étnico o racial</li> <li>■ Opiniones políticas</li> <li>■ Convicciones religiosas y filosóficas</li> <li>■ Afiliación sindical</li> <li>■ Datos genéticos</li> <li>■ Datos biométricos</li> <li>■ Relativos a la salud</li> <li>■ Vida u orientación sexual</li> </ul>	<ul style="list-style-type: none"> <li>■ Solo se tratarán cuando estén bajo la supervisión de autoridades públicas jurídicas o lo autorice el el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados.</li> </ul>

■ Dirección IP		
■ ...		

### ■ **Dato disociado:**

- Aquel que no permite la identificación de un afectado o interesado.
- Por ejemplo, los datos estadísticos no permiten identificar a las personas.

### ■ **Fichero:**

- Conjunto organizado de datos de carácter personal, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso.
- Un fichero es tanto el conjunto de fichas en papel de los pacientes que un dentista guarda por orden alfabético, como la más sofisticada base de datos de clientes de una multinacional en forma automatizada.

### ■ **Fichero automatizado:**

- Los datos se encuentran almacenados en dispositivos informáticos (discos duros, ordenadores, DVD...) que requieren de herramientas capaces de descifrar la información que contienen para su tratamiento.

### ■ **Fichero no automatizado o manual:**

- Los datos están almacenados en soportes que no requieren de herramientas para su tratamiento, como el papel, (siempre y cuando el fichero esté estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales).
- Archivo físico de historias clínicas de pacientes de un hospital, archivo de nóminas en formato papel de una empresa, currículum vitae de candidatos a un puesto de trabajo, facturas de proveedores, albaranes de clientes, tarjeteros con contactos, ...

### ■ **Fichero mixto:**

- Los datos están distribuidos entre soportes automatizados y no automatizados.

### ■ **Tratamiento de datos:**

- Cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
- Confección de nóminas, elaboración de listas de asistentes a un congreso, listas de pacientes, envío de mailing, ...

### ■ **Cesión o comunicación de datos:**

- Modalidad de tratamiento de datos que supone su revelación a una persona distinta del propio interesado.

### ■ **Niveles de seguridad:**

- La ley identifica tres niveles de medidas de seguridad aplicables a los ficheros que contengan datos de carácter personal: básico, medio y alto.
- El establecimiento de uno u otro nivel de seguridad se adopta en función de la diferente sensibilidad de los datos personales incluidos en los archivos, considerándose de nivel básico los ficheros con información menos sensible y de nivel alto aquéllos que recogen información de naturaleza especialmente sensible.

En relación a las personas:

### ■ **Afectado o interesado:**

- Persona física titular de los datos que sean objeto de tratamiento.

- El cliente, empleado, proveedor, candidato a formar parte de la empresa, paciente, etc., cuyos datos estén siendo tratados por la empresa.

■ **Responsable del fichero o responsable de tratamiento:**

- Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decide sobre la finalidad, contenido y uso del tratamiento.
- Es decir, la propia empresa será la responsable de los ficheros que contienen datos relativos a sus empleados, proveedores, clientes, etc.

■ **Encargado de tratamiento:**

- Persona física o jurídica, de naturaleza pública o privada, u organismo administrativo, que trate datos personales por cuenta del responsable del fichero o responsable de tratamiento.
- El encargado no decide sobre la finalidad, contenido y tratamiento. El responsable sí.
- Por ejemplo, una gestoría que elabora nóminas.

#### 4. Legitimación de datos

En esta fase hay que respetar una serie de principios y obligaciones tanto en la recogida como en el posterior tratamiento de los datos. Un aspecto que se debe respetar en todo momento es el de la calidad de los datos:

- Sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.
- No podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. Cualquier desviación de su utilización original constituye una falta.<sup>2</sup>
- Serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. En el caso de ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados.
- Serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. En caso de finalización del tratamiento para el que fueron recabados, deberán ser cancelados y por tanto finalizar su utilización. No se pueden conservar una vez superado el tiempo necesario para los fines originales.
- Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

Además del principio de calidad de los datos la empresa tiene que cumplir lo siguiente:

■ **Solicitar el consentimiento del interesado:**

- La empresa debe solicitar el consentimiento del interesado para poder usar sus datos<sup>3</sup> o cederlos a otras empresas.
- El consentimiento debe ser:
  - **Libre:** salvo que la ley disponga otra cosa, no nos pueden obligar a facilitar nuestros datos. En caso de que así fuera nos deben informar del carácter obligatorio de las preguntas que realicen y de las consecuencias que se derivan si nos negamos a facilitar datos.
  - **Específico:** para un uso concreto.
  - **Previo e Informado:** el afectado debe conocer con anterioridad al tratamiento la existencia del mismo y sus finalidades.

<sup>2</sup> No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

<sup>3</sup> La LOPD contempla ciertas excepciones, recogidas en el artículo 6.

- **Revocable:** Excepto cuando sea obligatorio facilitar los datos, si se puede consentir libremente se puede retirar el consentimiento. El procedimiento de revocación debe ser sencillo y gratuito.
- El **responsable** debe poder **probar** en todo momento **que ha obtenido el consentimiento**.

#### ■ Gestionar los derechos:

- Hay que atender las solicitudes de acceso, rectificación, oposición, supresión (“derecho al olvido”), limitación del tratamiento, portabilidad y de no ser objeto de decisiones automatizadas.
- **ACCESO:**
  - Saber si nuestros datos están siendo tratados, la finalidad del tratamiento, origen de los datos y comunicaciones realizadas o previstas.
- **RECTIFICACIÓN:**
  - Solicitar la modificación de los datos erróneos o incompletos.
- **OPOSICIÓN:**
  - Requerir al responsable del fichero para que no se lleve a cabo el tratamiento de sus datos de carácter personal cuando se están tratando sus datos personales en una misión de interés público o en el interés legítimo y cuando el tratamiento de sus datos se realice con fines de publicidad o de prospección comercial.
- **SUPRESIÓN (derecho al olvido):**
  - Solicitar la supresión de los datos de carácter personal si ya no son necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo, si te has opuesto al tratamiento, si han sido tratados ilícitamente, ...
- **LIMITACIÓN DEL TRATAMIENTO**
  - Un interesado puede limitar la forma en que una organización utiliza los datos sobre él. Esta es una alternativa a solicitar el borrado de datos.
- **PORTABILIDAD**
  - El individuo puede solicitar los datos personales que haya facilitado a un responsable del tratamiento y transmitirlos a otros responsables sin que el anterior lo pueda impedir. Los datos le han de ser facilitados al individuo en un formato estructurado, de uso común y lectura mecánica.
- **NO SER OBJETO DE DECISIONES INDIVIDUALES AUTOMATIZADAS**
  - Garantizar que no seas objeto de una decisión basada únicamente en el tratamiento de tus datos, incluida la elaboración de perfiles, que produzca efectos jurídicos sobre ti o te afecte significativamente de forma similar

## 5. Protección de datos e implantación de medidas de seguridad

Las empresas deben adoptar las medidas de carácter técnico, organizativo y/o jurídico que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado. Estas medidas se fijan en función del nivel de seguridad correspondiente al fichero y del soporte del mismo (automatizado o no automatizado).

Existen tres niveles de seguridad en función de la mayor o menor sensibilidad de los datos recogidos en ellos:

- **Nivel Básico.**
- **Nivel Medio.**
- **Nivel Alto.**

Las medidas incluidas en cada uno de estos niveles tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero. Además, los niveles de seguridad son acumulativos; es decir, los ficheros de nivel alto deben cumplir las medidas previstas para los ficheros de nivel alto, medio y básico, y los ficheros de nivel medio deben hacer lo propio con respecto a los niveles medio y básico.

	Nivel Básico	Nivel Medio	Nivel Alto
<b>Responsable seguridad</b>		<ul style="list-style-type: none"> <li>• El responsable del fichero tiene que designar a uno o varios responsables de seguridad (no es una delegación de responsabilidad).</li> <li>• El responsable de seguridad es el encargado de coordinar y controlar las medidas del documento.</li> </ul>	
<b>Personal</b>	<ul style="list-style-type: none"> <li>• Funciones y obligaciones de los diferentes usuarios o de los perfiles de usuarios claramente definidas y documentadas.</li> <li>• Definición de las funciones de control y las autorizaciones delegadas por el responsable.</li> <li>• Difusión entre el personal, de las normas que les afecten y de las consecuencias por su incumplimiento.</li> </ul>		
<b>Incidencias</b>	<ul style="list-style-type: none"> <li>• Registro de incidencias: tipo, momento de su detección, persona que la notifica, efectos y medidas correctoras.</li> <li>• Procedimiento de notificación y gestión de las incidencias.</li> </ul>	<b>SOLO AUTOMATIZADOS</b> <ul style="list-style-type: none"> <li>• Anotar los procedimientos de recuperación, persona que lo ejecuta, datos restaurados, y en su caso, datos grabados manualmente.</li> <li>• Autorización del responsable del fichero para la recuperación de datos.</li> </ul>	
<b>Control de acceso</b>	<ul style="list-style-type: none"> <li>• Relación actualizada de usuarios y accesos autorizados.</li> <li>• Control de accesos permitidos a cada usuario según las funciones asignadas.</li> <li>• Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados.</li> <li>• Concesión de permisos de acceso sólo por personal autorizado.</li> <li>• Mismas condiciones para personal ajeno con acceso a los recursos de datos.</li> </ul>	<b>SOLO AUTOMATIZADOS</b> <ul style="list-style-type: none"> <li>• Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información.</li> </ul>	<b>SOLO AUTOMATIZADOS<sup>4</sup></b> <ul style="list-style-type: none"> <li>• Registro de accesos: <ul style="list-style-type: none"> <li>• usuario</li> <li>• hora</li> <li>• fichero</li> <li>• tipo de acceso</li> <li>• autorizado o denegado</li> </ul> </li> <li>• Revisión mensual del registro por el responsable de seguridad.</li> <li>• Conservación 2 años.</li> </ul> <b>SOLO NO AUTOMATIZADOS</b> <ul style="list-style-type: none"> <li>• Control de accesos autorizados.</li> <li>• Identificación accesos para documentos accesibles por múltiples usuarios.</li> </ul>

<sup>4</sup> No es necesario este registro si el responsable del fichero es una persona física y es el único usuario que tiene acceso y trata los datos

<b>Identificación y autenticación</b>	<ul style="list-style-type: none"> <li>• SOLO AUTOMATIZADOS</li> <li>• Identificación y autenticación personalizada de los usuarios.</li> <li>• Procedimiento de asignación y distribución de contraseñas.</li> <li>• Almacenamiento ininteligible de las contraseñas.</li> <li>• Periodicidad del cambio de contraseñas (&lt;1 año).</li> </ul>	SOLO AUTOMATIZADOS <ul style="list-style-type: none"> <li>• Limite de intentos reiterados de acceso no autorizado.</li> </ul>	
<b>Gestión de soportes</b>	<ul style="list-style-type: none"> <li>• Inventario de soportes.</li> <li>• Identificación del tipo de información que contienen, o sistema de etiquetado.</li> <li>• Acceso restringido al lugar de almacenamiento.</li> <li>• Autorización de las salidas de soportes (incluidas a través de email)</li> <li>• Medidas para el transporte y el desecho de soportes.</li> </ul>	SOLO AUTOMATIZADOS <ul style="list-style-type: none"> <li>• Registro de entrada y salida de soportes: documento o soporte, fecha, emisor/destinatario, número, tipo de información, forma de envío, responsable autorizado para recepción/entrega.</li> </ul>	SOLO AUTOMATIZADOS <ul style="list-style-type: none"> <li>• Sistema de etiquetado confidencial.</li> <li>• Cifrado de datos en la distribución de soportes.</li> <li>• Cifrado de información en dispositivos portátiles fuera de las instalaciones (evitar el uso de dispositivos que no permitan cifrado, o adoptar medidas alternativas).</li> </ul>
<b>Copias de respaldo</b>	<ul style="list-style-type: none"> <li>• SOLO AUTOMATIZADOS</li> <li>• Copia de respaldo semanal.</li> <li>• Procedimientos de generación de copias de respaldo y recuperación de datos.</li> <li>• Verificación semestral de los procedimientos.</li> <li>• Reconstrucción de los datos a partir de la última copia o Grabación manual en su caso, si existe documentación que lo permita.</li> <li>• Pruebas con datos reales. Copia de seguridad y aplicación del nivel de seguridad correspondiente.</li> </ul>		SOLO AUTOMATIZADOS <ul style="list-style-type: none"> <li>• Copia de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos.</li> </ul>
<b>Criterios de archivo</b>	SOLO NO AUTOMATIZADOS <ul style="list-style-type: none"> <li>• El archivo de los documentos debe realizarse según criterios que faciliten su consulta y localización para garantizar el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO)</li> </ul>		
<b>Almacenamiento</b>	SOLO NO AUTOMATIZADOS <ul style="list-style-type: none"> <li>• Dispositivos de almacenamiento dotados de mecanismos que obstaculicen su apertura.</li> </ul>		SOLO NO AUTOMATIZADOS <ul style="list-style-type: none"> <li>• Armarios, archivadores de documentos en áreas con acceso protegido mediante puertas con llave.</li> </ul>
<b>Custodia soportes</b>	SOLO NO AUTOMATIZADOS <ul style="list-style-type: none"> <li>• Durante la revisión o tramitación de los documentos, la persona a cargo de los mismos debe ser diligente y custodiarla para evitar accesos</li> </ul>		

	no autorizados.		
<b>Copia o reproducción</b>			<b>SOLO NO AUTOMATIZADOS</b> <ul style="list-style-type: none"> <li>• Sólo puede realizarse por los usuarios autorizados.</li> <li>• Destrucción de copias desechadas.</li> </ul>
<b>Auditoría</b>		<ul style="list-style-type: none"> <li>• Al menos cada dos años, interna o externa.</li> <li>• Debe realizarse ante modificaciones sustanciales en los sistemas de información con repercusiones en seguridad.</li> <li>• Verificación y control de la adecuación de las medidas.</li> <li>• Informe de detección de deficiencias y propuestas correctoras.</li> <li>• Análisis del responsable de seguridad y conclusiones elevadas al responsable del fichero.</li> </ul>	
<b>Telecomunicaciones</b>			<b>SOLO AUTOMATIZADOS</b> <ul style="list-style-type: none"> <li>• Transmisión de datos a través de redes electrónicas cifradas.</li> </ul>
<b>Traslado de documentación</b>			<b>SOLO NO AUTOMATIZADOS</b> <ul style="list-style-type: none"> <li>• Medidas que impidan el acceso o manipulación.</li> </ul>

## 6. Sanciones

La LOPD contempla tres tipos de infracciones:

- **Leves:** sancionadas con multa de hasta 40.000 €.
- **Graves:** sancionadas con multa de 40.001 € a 300.000 €.
- **Muy Graves:** sancionadas con multa entre 300.001 € a 20.000.000 € (o el 4% de la facturación anual).

La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, el volumen de los tratamientos efectuados, los beneficios obtenidos, el grado de intencionalidad, la reincidencia, los daños y perjuicios causados a las personas interesadas y a terceras personas, etc. También hay que tener en cuenta que habitualmente en un procedimiento Sancionador se recogen varias infracciones, por lo que las sanciones son acumulativas,

## Ley Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE).

### 1. Definiciones

#### Servicio de la Sociedad de la Información:

- Servicios prestados normalmente a título **oneroso** (para obtener algún beneficio a cambio) a **distancia**, por **vía electrónica** y a **petición individual**.



- También se incluyen servicios no remunerados por sus destinatarios en la medida que si lo sean para el prestador de servicios.
- Ejemplos: compra de entradas por vía electrónica, reserva de alojamiento por vía electrónica, envío de comunicaciones comerciales, suministro de información por vía telemática....

### **Prestador de Servicios de la Información:**

- Tanto empresas como particulares, que realicen un servicio por Internet a petición del usuario, incluidos los no remunerados, pero que supongan un beneficio económico para la empresa que los ejerce.

Está obligado cualquier **prestador** con sitio Web que realice **actividades económicas, directas o indirectamente** y cuente con la dirección de su negocio centralizada en España, o posea una sucursal en España o cualquier otro tipo de **establecimiento** permanente situado **en el territorio Español**.

## **2. A qué obliga**

### **1. Deber de información general (artículo 10):**

- El prestador debe informar de forma clara, accesible, explícita, permanente, fácil y gratuita:
  1. **Nombre o denominación social.**
  2. **Residencia o domicilio** o en su defecto la dirección de uno de los establecimientos permanentes en España.
  3. **Correo electrónico** y cualquier otro dato que permita una **comunicación directa y efectiva**. Por ejemplo: teléfono móvil, fijo, fax, ...
  4. Los datos de inscripción del registro mercantil o cualquier otro registro en el se encuentre inscrito, ya sea para la simple adquisición de la personalidad jurídica o a los simples efectos de publicidad.
  5. En el caso de que estuviese sujeto a autorización administrativa, los datos relativos a

## **AVISO LEGAL**

### **4.- AUTORIZACIÓN ADMINISTRATIVA Y ÓRGANO SUPERVISOR**

ING DIRECT es un banco que opera bajo la supervisión del Banco de Holanda y además, en España, bajo la supervisión del Banco de España. Está inscrito como sucursal en el registro del Banco de España con el nº 1465.

### **3.- DATOS DE INSCRIPCIÓN EN EL REGISTRO MERCANTIL**

ING DIRECT, NV, Sucursal en España está inscrito en el Registro Mercantil de Madrid, Tomo 18.991, Libro 0, Folio 14, Sección 8, Hoja M-331801.

dicha autorización. Por ejemplo: agencias de viajes, operadores de telefonía móvil...

6. Si ejerce una **profesión regulada** (p.e. abogados, médicos,...) se debe indicar:
  - ⊗ Datos del colegio profesional al que, en su caso, pertenezca y número de colegiado.
  - ⊗ Título académico oficial o profesional.

- ⊗ Estado de la unión europea o espacio económico europeo en el que se expidió dicho título y, en su caso, la correspondiente homologación o reconocimiento. .
- ⊗ Normas profesional aplicables y medios a través de los que se puedan conocer.

## AVISO LEGAL

### 5.- NÚMERO DE IDENTIFICACIÓN FISCAL

CIF: W0032177H

7. **Número de identificación fiscal** (CIF o NIF).
8. Cuando el servicio de la sociedad de la información haga referencia a precios, se facilitará información clara y exacta sobre el **precio del producto o servicio**, indicando si incluye o no los **impuestos** aplicables y, en su caso, sobre los **gastos de envío** o en su caso aquello que dispongan las normas de las Comunidades Autónomas con competencias en la materia.

## Política de precios

Te ofrecemos precios bajos en todos los productos de nuestro catálogo. Todos los precios están indicados en euros. Nuestro precio, tal y como aparece indicado en la página de cada producto, incluye el IVA.

### Tarifas de envío en España

## AVISO LEGAL

### 2.- DATOS GENERALES

ING DIRECT, NV, Sucursal en España es un banco con domicilio social en la Calle Severo Ochoa, nº 2, Parque Empresarial Madrid-Las Rozas, Las Rozas 28232, Madrid.  
Teléfono 901 020 901, email de contacto: [informacion@ingdirect.es](mailto:informacion@ingdirect.es)

Envío 2 a 3 días	2,99 EUR/envío	GRATIS
Envío 1 día	8,99 EUR/envío	2,99 EUR

9. **Códigos de conducta** a los que en su caso esté adherido y la manera de consultarlos electrónicamente<sup>5</sup>. Un código de conducta es un conjunto de normas y obligaciones que asumen las personas y entidades que se adscriben al mismo y mediante las cuales se pretende fomentar la confianza y la seguridad jurídica, así como una mejor tramitación de cualquier problema o incidencia; es decir, los códigos de conducta exponen una serie de principios que las personas/organizaciones se comprometen a seguir.
- La obligación de facilitar esta información se dará por cumplida si el prestador la incluye en su página o sitio de Internet en las condiciones señaladas anteriormente.

<sup>5</sup> Procedimientos extrajudiciales para la resolución de los conflictos que surjan por la prestación de los servicios de la sociedad de la información, protección de los destinatarios frente al envío por vía electrónica de comunicaciones comerciales no solicitadas, ...

- Es habitual incluir dentro del Aviso Legal no solo la información a la que se refiere el artículo 10 de la LSSI, sino también las referidas a propiedad intelectual, uso de los contenidos, responsabilidades y protección de datos.

## 2. Contratación electrónica (art. 23-29):

- Si la empresa realiza contratos de compra-venta en línea o por vía electrónica a través de su página web, deberá:
  1. Cumplir el deber de información general.
  2. Antes de iniciar el procedimiento de contratación deberá poner a disposición del usuario, mediante técnicas adecuadas al medio de comunicación utilizado, de forma permanente, fácil y gratuita, información clara, comprensible e inequívoca sobre:
    - Los trámites o pasos a seguir para celebrar el contrato.
    - Si va a archivar el documento electrónico del contrato y si va ser accesible.
    - Los medios técnicos que pone a su disposición para identificar y corregir los errores en la introducción de los datos, antes de confirmarlos.
    - La lengua o lenguas en las que puede formalizarse el contrato.
  3. Una vez que el consumidor haya enviado su aceptación, la empresa deberá:
    - Básicamente, se pide que se muestren las condiciones del contrato, las condiciones de uso y la Política de Privacidad.
    - La empresa habrá de enviarle una confirmación de recepción en un plazo máximo de 24 horas.
    - O se establece un medio alternativo de confirmación, tan pronto como el usuario lo permita, que la confirmación sea archivada.

### Normas profesionales aplicables:

- [Estatuto General de la Abogacía](#)
- [Código Deontológico de la Abogacía](#)

**Título:** Licenciado en Derecho

**Colegio:** Ilustre Colegio de Abogados de Alicante

**Nº Colegiado:** [REDACTED]

**País Expedición Título:** España

Tu pedido de Amazon.es Ocultar detalles

DE: auto-confirm@amazon.es +

PARA: [REDACTED]

sábado 8 de octubre de 2011 15:19

---

**amazon.es** Ver el contenido de la cesta | Lista de deseos | Mi cuenta | Ayuda

**¡Gracias por tu pedido, [REDACTED]!**  
**¿Quieres gestionar tu pedido online?**  
 Si necesitas comprobar el estado de tu pedido o hacer cambios, visita nuestra página de inicio en Amazon.es y haz clic en Mi cuenta al principio de cualquier página.

**Información de compra:**

**Dirección de e-mail:** [REDACTED]

**Dirección de facturación:** [REDACTED] **Dirección de envío:** [REDACTED]

**Importe total del pedido: EUR 168,63**

**Resumen del pedido:**

Tu compra se ha dividido en 2 pedidos.

**Pedido #1 : (el pedido llegará en 1 envío)**

<b>Pedido nº:</b>	403-957 [REDACTED]
<b>Velocidad de envío:</b>	3 a 5 días
<b>Preferencia de envío:</b>	Agrupar mis productos en el menor número de envíos posible
<b>Productos:</b>	EUR 130,52
<b>Envío:</b>	EUR 0,00
<b>Total antes de impuestos:</b>	EUR 130,52
<b>Impuestos: *</b>	EUR 5,22
<b>Importe total:</b>	<b>EUR 135,74</b>

- La obligación de poner a disposición del destinatario toda esta información se dará por cumplida si el prestador la incluye en su página o sitio de Internet en las condiciones señaladas anteriormente.
- Cuando el prestador diseñe específicamente sus servicios de contratación electrónica para ser accedidos mediante dispositivos que cuenten con pantallas de formato reducido, se entenderá cumplida la obligación establecida en este apartado cuando facilite de manera permanente, fácil, directa y exacta la dirección de Internet en que dicha información es puesta a disposición del destinatario.
- El prestador no tendrá la obligación de facilitar la información anterior en los siguientes casos:
  - Cuando ambos contratantes así lo **acuerden** y ninguno de ellos tenga la consideración de **consumidor**.
  - El contrato se haya celebrado **exclusivamente** mediante **correo electrónico**.

### 3. Publicidad por Internet (art. 19-22):

- Si el prestador de servicios realiza publicidad en Internet, por su propia página u otras páginas:
  - En dicha publicidad se tiene que **identificar** claramente a **quién** se anuncia.
  - Los mensajes se tienen que **identificar** claramente como **publicidad**.
- Si se realizan **comunicaciones comerciales, ofertas promocionales y concursos**:
  - Deben ser claramente identificables y tienen que indicar la persona en el nombre de la cual la realizan.
  - Si se realicen por medio de correo electrónico deberán incluir la palabra "publicidad" o "publi" al principio.
  - Expresar de forma clara e inequívoca las condiciones de participación.
  - Cuando se quieran realizar comunicaciones comerciales a clientes o usuarios registrados, es imprescindible contar con la autorización expresa, previa, informada y que haya existido una relación contractual previa o bien se haya obtenido los datos de las llamadas fuentes accesibles al público.
- Cuando se envíe publicidad por correo electrónico, mensajes SMS/MMS o similares:
  - Se debe obtener con carácter previo el consentimiento del destinatario del mensaje.
  - Se debe identificar el mensaje con la palabra "publicidad" o "publi".
  - Se deben establecer procedimientos sencillos para facilitar la revocación del consentimiento por el usuario.

En cumplimiento de la LEY 3472002 de 11 de julio de servicios de la sociedad de la información y de comercio electrónico y Ley Orgánica 13-12-1999 de Protección de Datos, estamos obligados a comunicarle que su dirección de correo electrónico figura en la base de datos de [REDACTED], para el envío de tarifas, ofertas, nuevos productos y noticias, formando parte de un fichero automatizado, informarle de su opción de cancelación o modificación de sus datos.

Si no desea seguir recibiendo e-mails de [REDACTED] sólo tiene que contestar este mensaje especificando en el asunto **ELIMINAR PUBLICIDAD**, es imprescindible que nos facilite la dirección del e-mail en la que recibe nuestros comunicados.

Si no recibimos ningún e-mail por su parte, si dirección de correo electrónico seguirá en nuestra base de datos, entendiéndose que acepta y nos da su consentimiento y autorización expresa de envíos para futuros correos electrónicos.

Queda prohibido, por tanto, el envío de comunicaciones comerciales publicitarias o promocionales por correo electrónico que no hubieran sido solicitadas o autorizadas expresamente por los destinatarios, salvo que anteriormente existiera una relación contractual previa, siempre que los datos se hubieran obtenido de una forma lícita y se vayan a emplear para comunicaciones comerciales referentes a los servicios de la empresa similares a los que fueron objeto de contratación con el cliente.

#### 4. Sanciones (art. 38-39):

Por la comisión de las infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones:

- Infracciones muy graves:
  - Multa de 150.001 hasta 600.000 euros.
  - La reiteración en el plazo de tres años de dos o más infracciones muy graves, sancionadas con carácter firme, podrá dar lugar, en función de sus circunstancias, a la sanción de prohibición de actuación.
- Infracciones graves:
  - Multa de 30.001 hasta 150.000 euros.
  - El incumplimiento significativo de lo establecido en los párrafos a) y f) del artículo 10.1.
  - El envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente o el envío, en el plazo de un año, de más de tres comunicaciones comerciales por los medios aludidos a un mismo destinatario, cuando en dichos envíos no se cumplan los requisitos establecidos en el artículo 21.
- Infracciones leves:
  - Multa de hasta 30.000 euros.
  - No informar en la forma prescrita por el artículo 10.1 sobre los aspectos señalados en los párrafos b), c), d), e) y g) del mismo, o en los párrafos a) y f) cuando no constituya infracción grave.
  - El incumplimiento de lo previsto en el artículo 20 para las comunicaciones comerciales, ofertas promocionales y concursos.
  - El envío de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente cuando en dichos envíos no se cumplan los requisitos establecidos en el artículo 21 y no constituya infracción grave.

La reiteración en el plazo de tres años de dos o más infracciones muy graves, sancionadas con carácter firme, podrá dar lugar, en función de sus circunstancias, a la sanción de prohibición de actuación en España, durante un plazo máximo de dos años.