

LA GACETA

DE LOS NEGOCIOS

DOCUMENTOS



GUÍA PRÁCTICA

ENTREGA 2 / 2

**GUÍA SOBRE LAS
OBLIGACIONES DE
LAS EMPRESAS
FRENTE A LA LOPD**



LEGALIA ABOGADOS

NT/306/2005

14 DE ENERO DE 2005

X. LA CALIDAD DE LOS DATOS

¿Qué es?

La calidad de los datos personales es el conjunto de obligaciones que tiene mi empresa, como responsable de los ficheros, que afectan al tratamiento de los datos durante su vigencia. Básicamente comprende las siguientes obligaciones:

- Pertinencia de los datos.
- Adecuación del tratamiento.
- Actualización de los datos.

La pertinencia de los datos

La pertinencia de los datos es el deber que tiene mi empresa de almacenar sólo aquellos datos personales que sean adecuados y necesarios para cumplir las finalidades para las que han sido recogidos y el deber que tiene de cancelarlos cuando dejan de serlo.

Por ejemplo, en un Fichero de Proveedores, mi empresa puede tener datos de identificación del proveedor, de los productos o servicios que suministra..., pero no serían pertinentes en un Fichero de Proveedores, datos relativos a sus creencias o ideología.

Adecuación del tratamiento

La adecuación del tratamiento supone que mi empresa sólo puede tratar los datos personales almacenados en sus ficheros con la finalidad para la que se han obtenido, que es la finalidad de la que se informó al titular de los datos.

Si mi empresa ha informado al cliente de que

sus datos se van a utilizar con la única finalidad de gestionar los pedidos que haga, no puede utilizarlos luego para enviarle publicidad de nuevos productos o servicios.

La actualización de los datos

La LOPD dice que los datos de carácter personal serán exactos y puestos al día, de forma que respondan con veracidad a la situación actual del afectado.

Supone que mi empresa, en cuanto tenga conocimiento por cualquier medio, de que un dato no es correcto o ha cambiado (por ejemplo, es erróneo el apellido de un cliente o ha cambiado la dirección de un proveedor), debe rectificar o actualizar ese dato.

Mi empresa es la primera interesada en que los datos almacenados en los ficheros sean correctos y estén actualizados.

Normativa de aplicación:

Artículo 4 LOPD

XI. LA SEGURIDAD DE LOS DATOS

¿Qué es?

La seguridad de los datos personales se manifiesta en el deber que tiene el responsable de los ficheros de adoptar las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos personales y evitar su alteración, pérdida, tratamiento o acceso no autorizado.

Mi empresa tiene que interpretar el cumplimiento de este deber como un beneficio, porque la adopción de las medidas de seguridad

evitan la producción de los perjuicios derivados de la pérdida de información relevante por no tener una copia de seguridad.

¿Qué niveles de seguridad existen?

La normativa española clasifica las medidas de seguridad que deben adoptarse en tres niveles:

- Nivel básico, aplicable a todos los ficheros de datos personales.

- Nivel medio, aplicable a los ficheros con datos relativos a la comisión de infracciones administrativas o penales, entre otros.

- Nivel alto, aplicable a los ficheros que contengan datos especialmente protegidos.

Medidas de seguridad de nivel básico

Todos los ficheros de datos personales deben reunir las medidas de seguridad de nivel básico. Destacan:

- La existencia de un Documento de Seguridad.

- La realización de copias de seguridad semanalmente, salvo que en este periodo no se hayan actualizado los datos.

- Existencia de mecanismos, como las contraseñas, para acceder a los ficheros.

Medidas de seguridad de nivel medio

El nivel medio exige el cumplimiento de las medidas de seguridad propias del nivel básico y de otras adicionales, tales como:

- Existencia de la figura del Responsable de Seguridad.

- Existencia de un registro de entrada y salida de soportes que contengan datos personales.

“ La calidad de los datos es el conjunto de obligaciones que tiene la empresa, como responsable de los ficheros, que afectan al tratamiento de los datos ”

- Realización de una auditoría sobre el cumplimiento de la normativa de seguridad, al menos cada dos años.

Normativa de aplicación:
Artículos 9 LOPD y RMS

Medidas de seguridad de nivel alto

El nivel alto exige, junto con el cumplimiento de las medidas de seguridad del nivel básico y del nivel medio, otras medidas adicionales como la existencia de un registro de accesos a los ficheros con datos personales (a través de mecanismos técnicos que tengan incorporada la función de la trazabilidad).

Eso significa que, de cada acceso, debe quedar registrado: la identidad de la persona que ha realizado el acceso, la fecha y hora del acceso, el fichero accedido, el tipo de acceso, si ha sido autorizado o denegado, y el registro concreto al que se ha accedido.

Plazos de adopción de las medidas

Mi empresa tiene el deber de adoptar las medidas del nivel de seguridad que corresponda a los ficheros, según la naturaleza de los datos personales almacenados. Las medidas de seguridad deben adoptarse de forma simultánea a la creación del fichero y tratamiento de los datos. Los plazos transitorios establecidos por la legislación vigente para los ficheros que ya existieran con anterioridad a su entrada en vigor, ya han finalizado salvo para los datos almacenados únicamente en soporte papel, en los que podrán adoptarse las medidas de seguridad hasta el año 2007

Especial referencia al Documento de Seguridad

El Documento de Seguridad debe recoger la normativa de seguridad de mi empresa en lo relativo al tratamiento de datos personales, y en él han de figurar todas las medidas de seguridad que deben cumplirse para garantizar la integridad y confidencialidad de los datos almacenados en los ficheros.

Todos los trabajadores de mi empresa que, en el desarrollo de sus funciones tienen acceso a los datos almacenados en los ficheros, deben conocer y cumplir las medidas de seguridad contenidas en el Documento.

La figura del Responsable de Seguridad

El Responsable de Seguridad es aquella persona designada por mi empresa, de entre sus empleados, u otra persona o empresa ajena a la mía, para coordinar y controlar el cumplimiento de las medidas de seguridad, tanto técnicas como organizativas.

En caso de incumplimiento de las medidas de seguridad, es mi empresa, como responsable de los ficheros, quien asume la responsabilidad que se derive.

Normativa de aplicación:
Artículos 9 LOPD y RMS

XII. EL DEBER DE SECRETO Y LA CONFIDENCIALIDAD

¿Qué es?

El responsable del fichero y quienes intervienen, como empleados o prove-

“ El nivel alto exige
junto con el
cumplimiento de las
medidas de seguridad
del nivel básico y del
nivel medio, otras
medidas
adicionales ”

“ El Responsable
de Seguridad es
aquella persona
designada para
coordinar y controlar
el cumplimiento de
las medidas de
seguridad ”

“ El deber de secreto se impone a la empresa y se extiende a todos los empleados de la misma que tienen acceso a los datos ”

edores, en cualquier fase del tratamiento de los datos personales, están obligados al secreto profesional respecto de los mismos y al deber de guardarlos. Estas obligaciones subsisten aun después de cancelados o anulados los datos y los ficheros, y después de finalizar sus relaciones con el responsable del fichero.

Un claro ejemplo de vulneración del deber de secreto lo constituye el abandono de la documentación de una empresa en contenedores de basura, sin haber procedido a su previa destrucción.

¿A quién se extiende?

El deber de secreto se impone a mi empresa, como responsable de los ficheros de datos personales y se extiende a todos los empleados de la misma que, en el desarrollo de las funciones que les son encomendadas, tienen acceso a los datos.

Los empleados de mi empresa tienen la obligación de guardar el secreto de los datos personales que conozcan incluso después de finalizada la relación laboral.

Es conveniente que los contratos de trabajo incluyan una cláusula de confidencialidad.

¿Cómo garantizar su cumplimiento?

Mi empresa tiene que adoptar una adecuada política de confidencialidad de los datos personales con la finalidad de garantizar su secreto.

Esta política de confidencialidad debe ser conocida por todos los trabajadores que tienen acceso a los datos personales almacenados en los ficheros. Esto se garantiza bien a través de cláusulas contractuales, bien a través de la realización

de cursos o jornadas de formación, con la precaución de que los trabajadores firmen el certificado de asistencia obligatoria a las mismas.

Modelo de cláusula de confidencialidad para contratos de trabajo.

En el contrato de trabajo suscrito con cada empleado que acceda a datos personales, deberá incluirse una cláusula del siguiente tenor literal:

“El trabajador tiene y asume la obligación de guardar el secreto y la confidencialidad de toda la información de la empresa a la que tenga acceso durante la vigencia del presente contrato, especialmente la información relativa a personas físicas recogida en ficheros de datos personales. Esta obligación subsistirá aun después de finalizada la relación laboral.

El trabajador será responsable de todos los daños y perjuicios que para la empresa se deriven como consecuencia del incumplimiento doloso o culposo de dicha obligación”.

Normativa de aplicación:
Artículos 10 LOPD

XIII. TRANSFERENCIA INTERNACIONAL DE DATOS

¿Qué es?

La transferencia internacional de datos personales es la exportación de los mismos a países que no ofrecen un nivel

de protección equiparable al español.

El movimiento de datos personales entre los Estados que forman la Unión Europea es enteramente libre porque en todos ellos se garantiza un nivel de protección semejante, a través de las Directivas europeas y las leyes internas dictadas en su desarrollo.

Requisitos

Únicamente pueden exportarse datos personales a países distintos de los que integran la Unión Europea si su normativa ofrece un nivel de protección de datos de carácter personal equiparable al comunitario.

Las Órdenes del Ministerio de Justicia e Interior y del Ministerio de Justicia de 2 de febrero de 1995 y de 31 de julio de 1998 establecen la relación de países cuya normativa tiene un nivel de protección de datos de carácter personal equiparable a la Ley española.

Evaluación por la Agencia

Si mi empresa pretende exportar los datos almacenados en los ficheros a un país que no forma parte de la Unión Europea y que no aparece en las citadas Órdenes, debe pedir autorización previa a la APD.

En tal caso, la APD valorará si el país de destino ofrece un adecuado nivel de protección de los datos personales, y autorizará o no la transferencia internacional solicitada.

Excepciones

La LOPD establece una serie de excepciones, en las que no es necesario solicitar y obtener la previa autorización de la APD para realizar la

transferencia internacional de los datos.

De entre esas excepciones, como empresario me afectará el supuesto en el que el titular de los datos personales haya dado su consentimiento inequívoco a la transferencia, para lo cual debe haber sido informado adecuadamente.

Normativa de aplicación:
Artículo 33 LOPD

XIV. LOS DERECHOS DE LOS INTERESADOS

¿A qué obligan a la empresa los derechos de los interesados?

El titular de los datos personales almacenados en los ficheros de mi empresa tiene una serie de derechos con respecto al tratamiento de los mismos. Esos derechos son:

- Impugnación de valoraciones
- Consulta al Registro General
- Derecho de acceso a sus datos
- Derecho de rectificación de sus datos
- Derecho de cancelación de sus datos
- Derecho de oposición al tratamiento

Algunos de estos derechos suponen correlativos deberes para mi empresa como responsable de los ficheros.

Mi empresa tiene la obligación de facilitar el ejercicio de tales derechos por parte del interesado.

El derecho de impugnación de valoraciones

El afectado puede impugnar los actos administrativos o decisiones privadas que

implican una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos personales que ofrezca una definición de sus características o personalidad.

Es el caso, por ejemplo, de las técnicas de "scoring" en la contratación. Permiten valorar de forma automática si las características de una persona se adecuan a los requisitos exigidos por una empresa que le va a contratar.

El derecho de consulta al Registro

Cualquier persona puede dirigirse al Registro General de Protección de Datos con la finalidad de conocer la existencia de tratamientos de sus datos personales, las finalidades con que se tratan y la identidad del responsable del fichero donde están almacenados.

El Registro General de Protección de Datos es de consulta pública y gratuita. Para mi empresa supone la obligación correlativa de inscribir mis ficheros en ese registro.

El derecho de acceso

El afectado tiene derecho a solicitar a mi empresa, como responsable del fichero donde se almacenan sus datos, que le informe sobre cuáles son los datos almacenados, el modo en que mi empresa los ha obtenido y las cesiones que mi empresa haya hecho a terceras personas.

Recibida la solicitud, si mi empresa tiene datos del afectado en sus ficheros, debe contestarle en el plazo de diez días atendiendo el ejercicio del derecho de acceso.

Normativa de aplicación:

Artículos 13, 14 y 15 LOPD

El derecho de rectificación

El afectado puede solicitar a mi empresa, como responsable del fichero, que corrija o complete uno o varios de sus datos que estén almacenados en el fichero de forma errónea o incompleta.

Tiene derecho a que actualicemos datos como cambios de domicilio, u otros similares. Mi empresa tiene la obligación de corregir o completar los datos en el plazo de 10 días desde que el afectado ha formulado su solicitud.

El derecho de cancelación

El interesado, alegando una causa justificada, puede solicitar a mi empresa que sus datos sean excluidos del fichero, revocando el consentimiento que en su día otorgó para que fueran incorporados al mismo. Puede ser total o parcial, por afectar a todos o sólo a parte de los datos tratados en nuestro fichero.

Mi empresa tiene la obligación de hacer efectivo el derecho de cancelación en el plazo de 10 días, salvo que el mantenimiento de sus datos en el fichero sea necesario para el mantenimiento o cumplimiento de la relación que le une con mi empresa.

El derecho de oposición

Consiste en el derecho que tienen los titulares de datos, cuando su consentimiento no sea necesario para el tratamiento, de oponerse al mismo una vez tengan conocimiento de que se ha pro-

“ El interesado, alegando una causa justificada, puede solicitar a la empresa que sus datos sean excluidos del fichero ”

ducido. La oposición puede ser total o parcial en cuanto a las finalidades del fichero en el que sus datos están almacenados.

En tal supuesto, mi empresa tiene la obligación de cancelar sus datos del fichero, a su simple solicitud y sin gastos, en el mismo momento en que se reciba el requerimiento.

La tutela de los derechos

El afectado al que se deniegue, total o parcialmente, el ejercicio de sus derechos de oposición, acceso, rectificación o cancelación puede ponerlo en conocimiento de la APD.

Se inicia entonces un procedimiento para la atención del ejercicio de la tutela, que termina con una resolución de la APD y puede dar lugar a la imposición de sanciones.

Normativa de aplicación:

Artículos 16 y 18 LOPD

XV. LA AGENCIA DE PROTECCION DE DATOS

Cuestiones generales ¿Qué es?

La Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones.

El Estatuto de la Agencia de Protección de Datos (APD) fue aproba-

do por el Real Decreto 428/93, de 26 de marzo.

¿Para qué sirve?

Las funciones que la APD tiene encomendadas se resumen en una principal: velar por el cumplimiento de la legislación sobre protección de datos y controlar e interpretar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de los datos.

La facultad inspectora

- La APD, a través de sus autoridades de control, puede inspeccionar los ficheros de datos de carácter personal de mi empresa.

- A tal efecto, pueden solicitar a mi empresa la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados por mi empresa para el tratamiento de los datos, accediendo a los locales donde se hallen instalados.

- Los funcionarios que ejerzan la inspección tienen la consideración de autoridad pública en el desempeño de sus cometidos.

Normativa de aplicación:

Artículos 35 y 40 LOPD

La potestad sancionadora

¿Qué es?

Es la facultad que tiene la APD de imponer sanciones a los responsables de los ficheros de datos personales que hayan incumplido las obligaciones que establece la normativa de protección de datos.

“ El afectado al que se deniegue el ejercicio de sus derechos puede ponerlo en conocimiento de la Agencia de Protección de Datos ”

“ Los funcionarios que ejerzan la inspección tienen la consideración de autoridad pública en el desempeño de sus cometidos ”

Los responsables de los ficheros están sujetos al régimen sancionador que se expone a continuación.

Infracciones

El incumplimiento de los deberes impuestos a mi empresa, como responsable de los ficheros, puede ser constitutivo de las siguientes infracciones:

- Leves, como el incumplimiento del deber de secreto profesional.
- Graves, como impedir el ejercicio de los derechos del interesado.
- Muy graves, como la cesión de datos personales fuera de los casos permitidos.

Sanciones

Tramitado el correspondiente procedimiento sancionador, si la APD considera que la conducta del responsable del fichero es constitutiva de alguna de las infracciones que establece la LOPD, puede imponer las siguientes sanciones:

- Leves: multa de hasta 60.101 euros.
 - Graves: hasta 300.506 euros.
 - Muy graves: hasta 601.012 euros.
- Plazos de prescripción:
- Leves: 1 año.
 - Graves: 2 años.
 - Muy graves: 3 años.
- Leves: 1 año.
- Graves: 2 años.
- Muy graves: 3 años.

Normativa de aplicación:
Artículos 43, 44, 45 y 47 LOPD

XVI. LA INSCRIPCIÓN DE LOS FICHEROS

¿Qué es?

La inscripción de los ficheros de datos perso-

nales es el deber que tiene mi empresa de notificar a la Agencia de Protección de Datos la existencia y creación de los ficheros de los que sea responsable.

Dentro de la APD, el Registro General de Protección de Datos es el órgano que tiene por objeto la inscripción de los ficheros.

¿Quién y cuándo tiene que llevarla a cabo?

Mi empresa, como responsable, tiene la obligación de notificar previamente a la APD la creación de sus ficheros de datos personales.

Si antes del 14 de enero de 1999 mi empresa ya tenía los ficheros de datos personales, y éstos son automatizados, deben inscribirse en el plazo de 3 años desde esa fecha.

Si son ficheros no automatizados (recogidos únicamente en formato papel) el plazo finaliza el 24 de octubre de 2007.

¿Cómo se hace?

El procedimiento de inscripción de los ficheros es sencillo. Consiste en cumplimentar un "Modelo de notificación de tratamiento de datos de carácter personal" por cada fichero y remitirlo a la APD, bien en soporte papel o a través de la página web www.agenciaprotecciondatos.org

Deben cumplimentarse obligatoriamente la "Hoja de Solicitud" y los apartados de: "Responsable", "Nombre del Fichero", "Sistema de Tratamiento", "Medidas de Seguridad", "Estructura", "Finalidad" y "Procedencia".

¿Dónde se inscriben los ficheros?

La inscripción del fichero se acuerda por el

Director de la Agencia de Protección de Datos, a propuesta del Registro General de Protección de Datos, siempre que la notificación contenga la información necesaria. A tal fin, si no se hace a través del página web, deberá remitirse a la APD (C/ Sagasta, 22. C.P. 28004 - Madrid)

Si la APD considera que faltan datos o no son correctos, lo comunicará a mi empresa para que pueda corregirlo o completarlo en el plazo de diez días.

Normativa de aplicación:

Artículo 26, 39 y Disp. Adicional 1ª LOPD

XVII. LA MODIFICACION DE LOS FICHEROS

¿Qué es?

La modificación de los ficheros de datos personales es el deber que tiene mi empresa de notificar a la Agencia de Protección de Datos las modificaciones que se han producido en los ficheros de los que sea responsable.

Lógicamente, mi empresa sólo puede notificar las modificaciones producidas en los ficheros que previamente se hayan inscrito. Es necesario indicar el código de inscripción del fichero que se modifica, que fue asignado por la APD en el momento de su inscripción.

¿Quién y cuándo tiene que llevarla a cabo?

Mi empresa, como responsable de los mismos, tiene que notificar a la Agencia de Protección de

“ La modificación de los ficheros de datos personales es el deber que tiene la empresa de notificar a la APD las modificaciones que se han producido ”

Datos los cambios que se puedan producir en los ficheros que están inscritos a su nombre en el Registro General de Protección de Datos.

Por ejemplo, en el caso de que mi empresa almacene nuevos datos en su Fichero de Clientes, que por tanto no figuran en el modelo de notificación que se envió a la APD cuando se inscribió el fichero.

“ El proceso finaliza con la notificación por la Agencia de Protección de Datos de la supresión del fichero ”

¿Cómo se hace?

Mi empresa tiene que cumplimentar determinados apartados del "Modelo de notificación de tratamiento de datos de carácter personal". En concreto:

- La denominada "Hoja de solicitud", indicando que se solicita la "inscripción de modificación del fichero", los datos de la persona que efectúa la notificación y la dirección a efectos de notificación.

- El apartado de "Modificación" de la página 12.

- La página o páginas correspondientes a los apartados que se quieren modificar.

¿Dónde se notifica la modificación de los ficheros?

El "Modelo de notificación de tratamiento de datos de carácter personal" puede obtenerse a través de la página web de la APD www.agencia-protecciondatos.org.

Una vez cumplimentados los apartados correspondientes, se remitirá a la Agencia de Protección de Datos.

Las modificaciones producidas y notificadas serán inscritas en el Registro General de Protección de Datos.

Normativa de aplicación:

Artículos 26 y 39 LOPD

XVIII. LA SUPRESION DE LOS FICHEROS

¿Qué es?

La supresión de los ficheros consiste en la notificación a la Agencia de Protección de Datos, por medio de la cual se pone en su conocimiento que un fichero de los que mi empresa sea responsable ha dejado de existir.

Lógicamente, sólo se notifica a la APD la supresión de ficheros que previamente habían sido inscritos en el Registro General de Protección de Datos.

¿Quién y cuándo tiene que llevarla a cabo?

La supresión puede afectar a todos los ficheros, por ejemplo en el caso de extinción de la empresa, con la consiguiente supresión de todos los ficheros que fueron creados para el desarrollo de su actividad u objeto social.

Es posible que la supresión afecte sólo a alguno de los ficheros de mi empresa, como el Fichero de Clientes Potenciales, en el caso de que se tome la decisión de no hacer publicidad desde la propia empresa y contratar estos servicios a una empresa de marketing.

¿Cómo se hace?

Mi empresa tiene que cumplimentar determinados apartados del "Modelo de notificación de tratamiento de datos de carácter personal". En concreto:

- La denominada "Hoja de solicitud", indicando que se solicita la "inscripción de supresión del fichero", los datos de la persona que efectúa la notificación y la dirección a efectos de notificación.

- El apartado de "Supresión" de la página 12.

La página o páginas correspondientes a los apartados que se quieren modificar

¿Dónde se notifica la supresión de los ficheros?

El "Modelo de notificación de tratamiento de datos de carácter personal" puede obtenerse a través de la página web de la APD www.agencia-protecciondatos.org.

Una vez cumplimentados los apartados correspondientes, se remitirá a la Agencia de Protección de Datos.

El proceso finaliza con la notificación por la APD de la supresión del fichero.

Normativa de aplicación:

Artículo 39 LOPD

Próxima entrega:
Lupicínio Eversheds analiza la normativa de Gobierno Corporativo.