TU MUNDO LEGAL.

Guía Práctica:

Protección de datos para PYMES

Índice del documento

1. ¿Qué es la protección de datos?

La ley Orgánica de Protección de datos fija las obligaciones para todo aquel que tenga ficheros de datos personales en soporte físico y que puedan ser utilizados.

Además, garantiza los derechos para las personas que constan en esos ficheros, especialmente en lo que se refiere a su honor e intimidad.

Se excluyen de la ley los archivos con fines personales, domésticos o sobre investigación sobre delincuencia terrorista. En otros casos, tendrán reglamentos específicos los ficheros con fines electorales, estadísticos, de las Fuerzas Armadas o de cámaras de videovigilancia, así como los del Registro Civil.

2. ¿Cuál es el marco normativo de la protección de datos en España?

- ✓ Constitución Española de 1978.
- ✓ Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

- ✓ Reales Decretos:
  - Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
  - (*) Real Decreto 195/2000, de 11 de febrero, por el que se establece el plazo para implantar las medidas de seguridad de los ficheros automatizados.
  - (*) Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal.
  - Real Decreto 1665/2008, de 17 de octubre, por el que se modifica el Estatuto de la Agencia Española de Protección de Datos, aprobado por el Real Decreto 428/1993, de 26 de marzo.

- Real Decreto 156/1996, de 2 de febrero, por el que se modifica el Estatuto de la Agencia Española de Protección de Datos.
- (*) Real Decreto 1332/94, de 20 de junio, por el que se desarrollan algunos preceptos de la Ley Orgánica.
- Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos .

Cabe mencionar que algunas comunidades autónomas como Cataluña, Galicia, Madrid y País Vasco, han regulado la protección de datos en el ámbito de las relaciones de los ciudadanos con su propia administración territorial.

3. ¿Qué gestión requieren los datos?

2.1 Obtención o adquisición: La empresa consigue los datos personales de los clientes, proveedores, empleados…, para poderlos explotarlos. La ley especifica que estos datos han de ser los adecuados y no excesivos, en función de las finalidades para los que se han obtenido.

2.2 Tratamiento: Son las operaciones que se realizan para la gestión de los datos ya obtenidos, como la introducción en sistemas informáticos, la creación de carpetas o expedientes, su copia, transmisión a través de medios de comunicación, archivado y custodia. Para ello no es necesaria la autorización del titular de los datos si estos forman parte de un contrato y son necesarios para el cumplimiento de este contrato.

2.3 Comunicación, cesión o acceso por terceros: Se entiende por comunicación de datos cuando se revelan a otra persona, lo cual sólo está permitida si sirve para cumplir con los acuerdos pactados con el titular del los datos, que además deberá autorizarlo. Así pues, en el caso de venta de ficheros de datos personales por parte de una empresa es necesario que esta haya informado al interesado y especifique el uso que se le van a dar a los datos y quién los va a comprar.

2.4 Almacenamiento y custodia: La empresa podrá mantener los ficheros de datos personales para sus archivos históricos siempre que *"no sean conservados de forma que permitan la identificación del interesado"* durante más tiempo del necesario para cumplir con los objetivos para los que se adquirieron. Así pues, la empresa deberá tomar las precauciones adecuadas para:

- Asignar un período de vida a sus archivos históricos.
- Destruirlos de forma efectiva una vez se ha cumplido dicho período de vida.
- Asegurarse que durante el período de vida se informe al interesado de la existencia del fichero si así lo pide.

2.5 Destrucción: "*Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios para la finalidad para la cuál hubieran fueron recabados y registrados".E*n este sentido, la empresa deberá tomar las precauciones adecuadas para que la destrucción de los ficheros de datos personales sea efectiva y estos no se puedan volver a recuperar ni siquiera mediante la utilización de técnicas avanzadas de recuperación de datos borrados.

4. ¿Qué derechos y acciones pueden ejercitar los afectados?

3.1. Derecho de información. El artículo 5 de la Ley Orgánica 15/1999 establece la obligación de informar al interesado, previamente a la recogida de sus datos, sobre:

- Si los datos serán incluidos en un fichero automatizado de datos o serán objeto de tratamiento informático.
- Cuál es la finalidad para la que se recogen tales datos.
- Quienes serán los destinatarios de la información recogida.
- Si la respuesta del interesado a las preguntas que les sean planteadas es obligatoria o voluntaria.
- Cuáles son las consecuencias que se derivan de los datos obtenidos.
- Cuáles son las consecuencias que se derivan si se niega a suministrarlos.

- De que en todo momento puede ejercer sus derechos de acceso, rectificación y cancelación.
- Cuál es la identidad y dirección del responsable del fichero.

3.2. Derecho de consentimiento. Existe el derecho a dar o negar su consentimiento para que sus datos personales sean tratados informáticamente.

- Datos especialmente protegidos. Las personas tienen el derecho a no declarar sobre su propia ideología, religión o creencias, y la empresa ha de informar al interesado sobre este derecho.

3.3. Derecho de cesión. El interesado tiene derecho a autorizar previamente la cesión de sus datos, no obligatoria por ley.

3.4. Derecho de impugnación. El interesado tiene derecho a impugnar cualquier valoración de su comportamiento cuando ésta se base exclusivamente en el tratamiento informatizado de sus datos.

3.5. Derecho de consulta. Permite al interesado la realización de consultas al Registro General de Protección de Datos sobre la existencia de ficheros de carácter personal, su finalidad y la identidad de los responsables de tales ficheros.

Derecho a Indemnización. Posibilidad de que el afectado que resulte perjudicado en sus bienes o derechos, como consecuencia de un incumplimiento de la Ley , pueda pedir indemnización por sus daños al responsable del fichero por vía civil.

3.6. Derecho de acceso. El interesado tiene derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal, su origen y las comunicaciones que se van a hacer de ellos. Esta información podrá obtenerse una vez al año visualizando los datos o por escrito. Si se justifica su necesidad, podría tener acceso más veces.

3.7. Derecho de rectificación y cancelación. Los datos que no sean correctos o que vulneren la ley deberán cancelarse o rectificarse en un plazo de 10 días. La cancelación sólo permitirá que puedan ser consultados por la Justicia para poder atender posibles reclamaciones. El responsable del archivo deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado los datos

5. ¿Qué infracciones y sanciones prevé la ley?

A efectos legales, el responsable del fichero será la propia empresa a través de su representante legal. En cuanto al responsable de tratamiento, será quien preste este servicio a la empresa, si es que existe.

Las empresas que tratan directamente sus datos serán consideradas a la vez responsables del fichero y del tratamiento.

- ✓ Son infracciones leves:
  - No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos.
  - No proporcionar la información que solicite la Agencia Española de Protección de Datos para poder cumplir con su tarea..
  - No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.
  - Recoger datos personales sin proporcionar a sus afectados la información que obliga la ley.
  - Incumplir el deber de secreto.

- ✓ Son infracciones graves:
  - Crear ficheros de titularidad pública o iniciar la recogida de datos personales personal para crearlos sin que la autorización haya sido publicada en el *Boletín Oficial del Estado* o Diario oficial de la Comunidad Autónoma.

- Crear ficheros de titularidad privada o iniciar la recogida de datos personales con finalidades distintas a las de la empresa o entidad.
- Recoger datos personales sin tener el consentimiento expreso de las personas afectadas, en los casos en que sea exigible.
- Tratar los datos de carácter personal o usarlos posteriormente sin cumplir las garantías ni las protecciones de la Ley.
- Impedir o dificultar el acceso y o la negativa a facilitar la información que sea solicitada.
- Mantener datos de carácter personal inexactos o no rectificarlos o cancelarlos cuando se afecte a los derechos de las personas.
- No guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.
- Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad.
- No remitir a la Agencia Española de Protección de Datos las notificaciones previstas en la Ley así como no proporcionar en plazo los documentos e informaciones que sean requeridos.
- Obstruir la inspección de la Administración.
- No inscribir el fichero de datos de carácter personal en el Registro General de Protección Datos, cuando haya sido requerido para ello por el Director de la Agencia Española de Protección de Datos.
- Incumplir el deber de información cuando los datos hayan sido recabados de una persona distinta al afectado.

✓ Son infracciones muy graves:

- La recogida de datos de forma engañosa y fraudulenta.
- La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.
- Recabar y tratar los datos de carácter personal sin el consentimiento expreso del afectado.

- Desobedecer al Director de la Agencia Española de Protección de Datos cuando exija que se dejen de tratar de forma no reglamentaria los datos.
- Transferir datos de carácter personal a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia Española de Protección de Datos.
- Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías de la ley atentando contra los derechos de las personas.

- La vulneración del deber de guardar secreto sobre los datos de carácter personal, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.
- No atender u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.
- No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

✓ Tipo de sanciones:

La cuantía de las sanciones irá en función de los derechos que se hayan vulnerado, el volumen de datos tratados, los beneficios obtenidos, el grado de intencionalidad, la reincidencia, los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de incumplimiento de la ley y de culpabilidad en la infracción.

- Las infracciones leves serán sancionadas con multa de 100.000 a 10.000.000 de pesetas.
- 2. Las infracciones graves serán sancionadas con multa de 10.000.000 a 50.000.000 de pesetas.
- 3. Las infracciones muy graves serán sancionadas con multa de 50.000.000 a 100.000.000 de pesetas.

✓ Prescripción:

- Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves al año.

- El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido.
- Interrumpirá la prescripción el inicio, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador se paralizara durante más de seis meses por causas no imputables al presunto infractor.

➢ Procedimiento sancionador:

Las resoluciones de la Agencia Española de Protección de Datos u órgano correspondiente de la Comunidad Autónoma agotan la vía administrativa, durando un máximo de seis meses.

6. ¿Qué es la agencia española de Protección de datos?

Se trata de un ente de público que vigila el cumplimiento de la protección de datos. Sus funciones son de registro y control de los ficheros con datos personales, autorización de los movimientos internacionales de datos, atender las consultas y realizar inspecciones:

- Velar por el cumplimiento de las leyes en materia de protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos
- Emitir las autorizaciones.
- Atender las peticiones y reclamaciones de las personas afectadas.
- Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de datos de carácter personal.
- Instar a los responsables y encargados de los tratamientos de datos a que adopten las medidas necesarias para cumplir con la Ley de Protección de Datos. Si no lo hicieran, ordenar el cese de los tratamientos y la cancelación de los ficheros.
- Sancionar los incumplimientos de la ley.
- Informar sobre las modificaciones de la ley.
- Recabar ayuda e información de los responsables de los ficheros para poder llevar a cabo sus tareas.

- Publicar periódicamente una relación de los ficheros de datos personales para incentivar que se publicite su existencia.
- Redactar una memoria anual y remitirla al Ministerio de Justicia.
- Ejercer el control y autorizar los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.
- Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico así como dictar las condiciones necesarias para su seguridad.

7. ¿Qué pasos ha de seguir una PYME para adaptarse a la normativa de protección de datos?

Para que una empresa adapte sus sistemas de información a la Normativa sobre protección de datos ha de seguir una serie de etapas:

1. Identificar los ficheros con datos de carácter personal.
2. Notificar los ficheros con datos personales a la Agencia de protección de Datos.
3. Designar a un responsable de seguridad.
4. Identificar los riesgos de seguridad que pueden afectar a cada fichero.
5. Elaborar el Documento de Seguridad para cada fichero o grupo de ficheros de un mismo nivel de seguridad.
6. Poner en la práctica los procedimientos y medidas descritos en cada Documento de Seguridad.
7. Revisar los incidentes de seguridad, analizar sus causas y aplicar las medidas correctoras precisas.
8. Auditar el funcionamiento de las medidas establecidas en cada Documento de Seguridad.

8. ¿Cuál es el procedimiento de inscripción de datos en el registro de la Agencia Española de Protección de Datos?

El Registro General de Protección de Datos es el órgano de la Agencia Española de Protección de Datos que vela por la publicidad de la existencia de los ficheros y tratamientos de datos de carácter personal, cumpliendo con las exigencias de información, acceso, rectificación y cancelación de datos que prevé la ley.

Serán objeto de inscripción en el Registro General de Protección de Datos:

1. Los ficheros de las Administraciones Públicas
2. Los ficheros de titularidad privada
3. Las autorizaciones de transferencias internacionales de datos de carácter personal con destino a países que no presten un nivel de protección equiparable al que presta España.
4. Los códigos tipo
5. Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

Para realizar la inscripción inicial del fichero o una modificación o supresión, existe el formulario electrónico NOTA (titularidad pública y titularidad privada) a través del que deberán efectuarse las solicitudes.

Este formulario permite la presentación de forma gratuita de notificaciones a través de Internet con certificado de firma electrónica . En caso de no disponer de un certificado de firma electrónica, también puede presentarse la notificación a través de Internet, para lo cual se deberá remitir a la Agencia la Hoja de solicitud firmada. Por último, también se puede optar por presentar la solicitud en soporte papel.

También se pueden notificar de forma simplificada los ficheros de titularidad privada de comunidades de propietarios, clientes, libro recetario de farmacias, pacientes, gestión escolar, nóminas, recursos humanos y video vigilancia y los de titularidad pública de recursos humanos, gestión del padrón, gestión económica o

control de acceso. A través de esta opción, el formulario electrónico muestra una notificación precumplimentada que se podrá completar o adaptar a las necesidades de cada caso. Si ninguna de las notificaciones tipo previstas por la AEPD se adapta al fichero que se pretende notificar, se podrá seleccionar la opción de notificación normal.

Además, para los responsables que utilicen sus propios programas informáticos o los desarrolladores de aplicativos de protección de datos, se encuentran disponibles los formatos y especificaciones XML que deben cumplir sus aplicaciones para enviar notificaciones a la AEPD.

9. ¿Quién debe notificar la creación o modificación de ficheros a la Agencia Española de Protección de Datos?

Están obligados a notificar la creación de ficheros para su inscripción en el RGPD las personas físicas o jurídicas, de naturaleza pública o privada, u órgano administrativo, que vayan a crear ficheros de carácter personal.

La creación, modificación o supresión de los ficheros de las Administraciones Públicas sólo podrán hacerse por medio de **disposición general** publicada en el Boletín Oficial del Estado o diario oficial correspondiente.

Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando sea necesario para llevar a cabo la actividad legítima de la persona, empresa o entidad titular y se respeten las garantías establecidas en la ley.

Toda persona o entidad que vaya a crear ficheros de datos de carácter personal lo notificará previamente a la Agencia Española de Protección de Datos.

Cualquier modificación posterior en el contenido de la inscripción de un fichero deberá comunicarse a la Agencia Española de Protección de Datos, mediante una solicitud de modificación o de supresión de la inscripción. En ambos casos será necesario citar el Código de Inscripción asignado por el RGPD al fichero.

En el supuesto de ficheros y tratamientos no automatizados, creados con posterioridad a la fecha de entrada en vigor de la ley (14 de enero de 2000), también deberán ser notificados para su inscripción en el RGPD.

La no notificación de la existencia de un fichero supondría una infracción leve o grave.

10. ¿Cuál es el alcance del consentimiento en el tratamiento de datos de carácter personal en el caso de fusión absorción o escisión de empresas?

Según lo establecido en la Ley de 13 de diciembre de 1999 sobre protección de datos, el tratamiento de los datos de carácter personal requiere un consentimiento por parte del titular de esos datos.

¿Qué sucede con ese consentimiento dado a una empresa cuando ésta es absorbida por otra o se escinde?

La normativa mercantil prevé que en los casos de fusión, absorción o escisión de sociedades hay una transmisión en bloque de sus patrimonios a la nueva sociedad que nazca, que, por tanto, adquiere por sucesión universal los derechos y obligaciones de las anteriores entidades, incluyendo los ficheros de datos.

El Acuerdo de fusión, o de absorción, una vez adoptado debe publicarse tres veces: en el Boletín Oficial del Registro Mercantil y en dos periódicos de gran circulación en las provincias en las que cada una de las sociedades tengan sus domicilios.

La jurisprudencia reconoce como válido el consentimiento dado a la entidad originaria. Eso sí, cumpliendo con los requisitos de publicidad y comunicación al titular de los datos.

Así pues, en caso de fusión, absorción o escisión, el consentimiento para tratar datos dado a la entidad originaria seguirá siendo válido con la nueva entidad siempre y cuando estén reunidos los requisitos de publicidad y de comunicación al interesado.