

## INFORMACIÓN DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS

### PROTECCION DE DATOS DE CARÁCTER PERSONAL

Tanto la Ley Orgánica 15/1999 de 13 de Diciembre, como el Real Decreto 994/1999 de 11 de Junio tienen como finalidad la garantía del derecho a la intimidad de los ciudadanos.

La primera medida a adoptar por profesionales y empresarios para su adaptación a la normativa en esta materia está recogida en el artículo 26 de la mencionada Ley. Esto implica la obligación de realizar una comunicación a la Agencia de Protección de Datos, donde se relacionen todos los ficheros con datos de carácter personal que los particulares o las personas jurídicas creen o tengan establecidos de antemano, para el desarrollo de su actividad profesional o societaria.

La realización de esta comunicación tiene como consecuencia la inscripción, en el plazo de un mes desde la presentación de la misma, de los ficheros en el Registro General de Protección de Datos, Organismo encargado de velar por la protección de datos personales.

El paso posterior a la inscripción de los indicados ficheros, es la elaboración de un Documento de Seguridad Obligatorio, en el que se reflejan los recursos tanto humanos como materiales de los que la empresa dispone. La finalidad del mencionado documento es servir de pauta de conducta tanto a los responsables del fichero como a los usuarios de los mismos, aunque no manejen tal información.

El documento de seguridad no debe presentarse ante la Agencia de Protección de Datos, pero debe encontrarse siempre a disposición de la misma ante posibles inspecciones.

Tanto los ficheros como el documento de seguridad deben permanecer continuamente en actualización, mediante la correspondiente comunicación a la Agencia de Protección de datos (declaración) o mediante modificaciones (documento de seguridad).

Teniendo en cuenta el tipo de datos que se manejen deben aplicarse sobre cada fichero diferentes tipos de seguridad, teniendo en cuenta que cada medida supone el cumplimiento de la anterior. Se establece la siguiente clasificación de niveles:

- **Básico:** se incluyen todos los ficheros que contengan datos de identificación de personas, así como nombre, D.N.I., dirección, teléfono, etc...
- **Medio:** ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y prestación de servicios de solvencia y crédito.
- **Alto:** ficheros con información altamente sensible (ideología, religión, creencias, raza, salud, etc...).

Los contenidos mínimos exigidos en los niveles de seguridad son los siguientes:

- **Nivel Básico:** deben recogerse el ámbito de aplicación del documento y los recursos protegidos, la adopción de medidas que garanticen la seguridad exigida, la estructura de los ficheros y descripción de los sistemas, los procesos de registro de incidencias, así como las copias de respaldo y recuperación, y establecimiento de las funciones y obligaciones del personal.
- **Nivel Medio:** en este nivel deben reflejarse la identificación del responsable de seguridad del fichero, el acceso personalizado con los datos y establecimiento de un registro de entrada y salida de soportes, además de aquellas otras pautas que aseguren la eliminación de soportes, la autorización por escrito del responsable del fichero para a recuperación de datos y, la

verificación de las medidas y controles periódicos al menos con carácter bianual por el responsable de seguridad, que deberá plasmar en una auditoria las deficiencias y medidas correctoras, comunicándoselo posteriormente al responsable del fichero.

- **Nivel Alto:** se incluyen todos los requisitos contenidos en los dos niveles anteriores y el registro personalizado con fecha y hora de acceso a los ficheros, un informe elaborado por el responsable de seguridad donde se analice las revisiones realizadas, la conservación por un periodo no inferior a dos años, las distribuciones de soportes encriptados como garantía de seguridad y la conservación de una copia de seguridad en sitio distinto al que se encuentren los equipos.

El plazo de implantación de estas medidas de seguridad prescribieron en junio de 2001. No existe sanción por la realización de estos trámites fuera de plazo, aunque si existiría que caso de que la Agencia de Protección de Datos iniciase una inspección y no se hubieran cumplido.

Todas los obligados que no hayan realizado estos trámites se encuentran en una situación de ilegalidad y deben adaptarse a la normativa lo antes posible ya que pueden incurrir en distintos tipos de sanciones:

La cuantía de las sanciones leves oscila entre los 601,01€ hasta 60.101,21€, las de las graves desde 60.101,21€ hasta 300.506,05€ y las muy graves desde 300.506,05€ a 601.012,10 €

*Tipos de infracciones.*

1. Son infracciones leves:

- a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.
- b) No proporcionar la información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.
- c) 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.
- d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la LO 15/1999.
- e) Incumplir el deber de secreto establecido en el artículo 10, salvo que constituya infracción grave.

3. Son infracciones graves:

- a) Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el «[Boletín Oficial del Estado](#)» o Diario oficial correspondiente.
- b) Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.
- c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.
- d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.
- e) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.
- f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.
- g) La vulneración del deber de 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.

h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

i) No remitir a la Agencia de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.

j) La obstrucción al ejercicio de la función inspectora.

k) 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 de Protección de Datos.

l) Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado.

4. Son infracciones muy graves:

a) La recogida de datos en forma engañosa y fraudulenta.

b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.

c) Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7.

d) No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.

e) La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.

- f) Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.
- g) La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.
- h) No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.
- i) No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.