

ADAPTACIÓN DE EMPRESAS. A LA L.O.P.D.



AUDITORES LOPD

TRUST CONSULTING ASESORES SL



COMO ADAPTARSE A L.O.P.D.

DESARROLLO DE LA ADAPTACIÓN

Conocimiento de la empresa

Análisis

Registro ficheros

DOCUMENTACIÓN

ADAPTACIÓN

Madrid, 2012

▶ **Ley O. de Protección de Datos Ley 15/1999, de 13 de diciembre**

El derecho a la protección de datos personales es un derecho fundamental de todas las personas, que se traduce en la potestad de control sobre el uso de sus datos personales. Este control permite evitar que, a través del tratamiento de nuestros datos, se pueda disponer de información sobre nosotros que afecte a nuestra intimidad y demás derechos fundamentales y libertades públicas.

▶ **Real Decreto 1720/2007, de 21 de diciembre, reglamento de desarrollo de la Ley Orgánica**

▶ **Instrucciones de la Agencia Española de Protección de Datos sobre diversas materias**

▶ **Legislación sectorial con incidencia en materias sanitarias, bancarias, telecomunicaciones, etc.**

Artículo 1. Ley Orgánica de Protección de Datos

Garantizar y proteger en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar

DETERMINAR SU CUMPLIMIENTO

ADAPTACIÓN DE LAS EMPRESAS A LA LOPD

EVITAR SANCIONES DE LA APD

OBJETIVO DE LA LEGISLACIÓN

Obligatoriedad de la Ley

Esta ley obliga a todas las personas, empresas y organismos -tanto privados como públicos que dispongan de datos de carácter personal- a cumplir una serie de requisitos y aplicar determinadas medidas de seguridad en función del tipo de datos que posean.

A grandes rasgos las obligaciones legales fundamentales son:

Dar de alta los ficheros en la Agencia Española de Protección de Datos.

Elaborar y mantener actualizado el Documento de Seguridad.

Obtener la legitimidad de los afectados.

Conocimiento y cumplimiento de las normas por empleados

El conocimiento y cumplimiento de estas normas afectan a todos los empleados de la empresa que intervengan de forma directa o indirecta en el tratamiento de datos de carácter personal.

PRINCIPIOS BÁSICOS DE LA LOPD 1

CALIDAD DE LOS DATOS (Art. 4 LOPD)

ADECUADOS, PERTINENTES, NO EXCESIVOS Y ACTUALES

Cancelar datos cuando dejen de ser necesarios o pertinentes para la finalidad para la cual hubiesen sido recabados. P.ejm. Curriculum, campañas de marketing.

DERECHO DE INFORMACIÓN DURANTE LA RECOGIDA (Art.5 LOPD)

Informar al titular de los datos, en el momento de la recogida de los diversos aspectos

CONSENTIMIENTO DEL AFECTADO (Art. 6 LOPD)

Siempre necesario para tratar datos personales, salvo excepciones: Que sean necesarios para la relación comercial, laboral o administrativa.

DATOS ESPECIALMENTE PROTEGIDOS: consentimiento expreso o expreso y por escrito del interesado, salvo: - Prevención/Diagnóstico médico; Prestación asistencia sanitaria o tratamientos médicos; Gestión servicios sanitarios

DEBER DE SECRETO: Obligado para todo el personal de la empresa que intervenga en el tratamiento de datos personales (firma cláusula de confidencialidad)

- ◆ **Notificación de ficheros al Registro General de Protección de Datos.**
 - ◆ **Ejercicio de los derechos**
 - ◆ **Análisis del tratamiento de los datos (Derecho de información, consentimiento, Acceso de datos por cuenta de terceros, Cesiones, transferencias internacionales)**
 - ◆ **Calidad de los datos**
 - ◆ **Auditoria Bienal.**
-

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

www.agpd.es

Ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada. Actúa con plena **independencia** de las Administraciones Públicas en el ejercicio de sus funciones.

Su **finalidad principal** es velar por el cumplimiento de la legislación sobre protección de datos personales y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, oposición, rectificación y cancelación de datos.

The screenshot shows the homepage of the Agencia Española de Protección de Datos. The header features the agency's name and logo, a coat of arms, and a banner image of people walking. The main content area is divided into several sections:

- Navigation Menu:** Includes links for 'Conozca la Agencia', 'Ficheros y tratamientos inscritos', 'Canal del ciudadano', 'Canal del responsable de ficheros', 'Canal de documentación', 'Resoluciones', and 'Internacional'.
- Search:** A search bar for 'Búsqueda en el mapa web' and 'Búsqueda en documentos'.
- News and Updates:** Several articles with brief descriptions, such as 'El director de la Agencia Española de Protección de Datos expondrá en el Congreso sus consideraciones al proyecto de Ley de lucha contra el dopaje en el deporte.', 'El Tribunal de Justicia Europeo anula el acuerdo de transmisión de datos de pasajeros a EEUU.', and 'La Agencia Española de Protección de Datos publica una nueva Guía de Recomendaciones a Usuarios de Internet con motivo de la celebración del Día de Internet.'
- Red Iberoamericana de Protección de Datos:** A section highlighting international cooperation.
- Sede Institucional de la Agencia:** A section about the agency's institutional seat.
- TRIBUNA:** A section featuring a quote from José Luis Piñar Mañas, Director of the Agency, regarding a parliamentary hearing.

FICHEROS CON DATOS DE NIVEL BÁSICO



CLIENTES, PROVEEDORES, PERSONAL. ETC.

- ◆ Documento de Seguridad
 - ◆ Funciones y obligaciones del personal
 - ◆ Identificación y autenticación
 - ◆ Control de acceso lógico
 - ◆ Gestión de soportes. Registro de salidas.
 - ◆ Registro de incidencias
 - ◆ Copias de respaldo y procedimientos de recuperación
-

OBLIGACIONES ORGANIZATIVAS y TÉCNICAS



FICHEROS CON DATOS DE NIVEL MEDIO



- ◆ *Medidas de nivel básico*
 - ◆ **CLIENTES, PROVEEDORES, PERSONAL**
 - ◆ Responsable de seguridad
 - ◆ Auditoria bianual y controles periódicos
 - ◆ Identificación y autenticación. Inequívoca y personalizada. Reintentos.
 - ◆ Control de acceso físico. Exclusivo a personal autorizado
 - ◆ Gestión de soportes. Fecha de desecho. Registro de entradas.
 - ◆ Registro de incidencias + procedimiento de recuperación de los datos
 - ◆ No se realizarán pruebas con datos reales
-

OBLIGACIONES ORGANIZATIVAS y TÉCNICAS



FICHEROS CON DATOS DE NIVEL ALTO



- ◆ *Medidas de nivel básico*
 - ◆ *Medidas de nivel medio*
 - ◆ Registro de accesos a los ficheros. Identificación usuario, fecha, hora, fichero, registro y tipo de acceso.
 - ◆ Distribución cifrada de soportes.
 - ◆ Copia de respaldo y procedimiento de recuperación en ubicación diferente
 - ◆ Telecomunicaciones. Cifrando los datos. Encriptación.
-

FICHEROS DE DATOS OBTENIDOS DE BASES ACCESIBLES AL PÚBLICO

- ◆ Origen de datos: del titular o de Fuentes Accesibles al Público (FAP).
- ◆ Tipos de FAP: Registros Públicos (Registro de la propiedad, B.O.E., e.t.c.) listas de personas pertenecientes a grupos profesionales, diarios, boletines y medios de comunicación.
- ◆ Particularidades de las FAP (Caso Fichero páginas blancas o amarillas de telefónica):
 - ◆ Nombre, actividad, dirección.
 - ◆ Finalidad: Obtención de datos para la explotación.

Datos con nivel de seguridad básico, medio, alto.

PROCEDIMIENTO SANCIONADOR

Comienza de Oficio o a través de denuncia. Tiene los siguientes pasos:

1

Iniciación

- Acuerdo del Director de la Agencia
- Notificación al Responsable
- Realización de las pruebas
- Alegaciones

2

Resolución

- Resolución
- Elevación al director
- Más pruebas
- Resolución del director

3

Recursos

- Pago en período voluntario
- Recurso de reposición
- Recurso contencioso-administrativo

Infracciones y sanciones

Leves

601,01 a
60101,21 €

Graves

60101,22 a
300506,05 €

Muy graves

300506,06 a
601012,10 €