

Cumplimiento de la Ley de Protección de Datos en la PYME

Jornada TIC

Javier Prenafeta Rodríguez
Abogado

1. Introducción: derechos y obligaciones
2. Niveles y Medidas de Seguridad
3. Funciones y Obligaciones del Personal
4. Checklist para una Auditoría de Protección de Datos
5. Notificación de ficheros a la AEPD

1. Introducción: derechos y obligaciones

Conceptos de dato y fichero

Principios de la LOPD:

- Calidad
- Información
- Consentimiento
- Confidencialidad y Seguridad

1. Introducción: derechos y obligaciones

Derechos de los afectados

- Impugnación de valoraciones
- Consulta al Registro
- Acceso, oposición, rectificación y cancelación
- Indemnización

Obligaciones de las empresas

- Solicitar sólo datos necesarios
- Informar previamente a la recogida de los mismos
- Solicitud de consentimiento para el tratamiento y cesiones
- Implantación de medidas de seguridad
- Inscripción de ficheros

1. Introducción: derechos y obligaciones

Deber de información

¿Qué?

Existencia del fichero, finalidad y destinatarios
Carácter obligatorio/facultativo de las respuestas
Consecuencias
Derechos de los afectados
Identidad y dirección del responsable del tratamiento

¿Cuándo?

Datos facilitados por interesado: previamente a la recogida
Resto de casos: dentro de los tres meses siguientes

¿Cómo?

Formularios
Contratos
Mensajes de correo electrónico/acuses de recibo

1. Introducción: derechos y obligaciones

Modelo de cláusula

De acuerdo con lo dispuesto en el art. 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se le informa de lo siguiente:

- A menos que se indique expresamente lo contrario, debe responder a todas las cuestiones que se le formulan.
- Los datos solicitados son necesarios para *[indicar la finalidad]*, sin los cuales dicho servicio no podrá ser realizado.
- Los datos serán tratados de forma confidencial, incluidos en un fichero propiedad de *[indicar nombre y dirección de la entidad]*, sin que vayan a ser cedidos a entidad ni persona alguna sin su consentimiento, salvo en los casos legalmente permitidos.
- Los afectados podrán, en cualquier momento, ejercer sus derechos de acceso, cancelación, rectificación y oposición en relación con los mismos, dirigiéndose por escrito a *[indicar el nombre de la Unidad, servicio o departamento correspondiente]*.

El firmante de este documento declara que la información facilitada es exacta y completa, y presta su consentimiento al tratamiento de los datos anteriores de acuerdo con los términos que se indican.

Consentimiento

Para el tratamiento de los datos y posteriores cesiones

Forma: inequívoco (expreso, tácito o presunto)

Excepciones:

Relación negocial entre las partes
Fuentes accesibles al público

Posibilidad de revocación

Datos de menores de edad

Especialidades para datos especialmente protegidos
ideología, afiliación sindical, religión y creencias
origen racial, salud o vida sexual
infracciones administrativas y penales

Cesión y transferencias de datos

Finalidades relacionadas

Transferencias internacionales fuera de la Unión Europea

Acceso a datos por cuenta de terceros: *outsourcing*

Celebración de contrato por escrito

- Fines para los que se permite el acceso
- Medidas de seguridad aplicables
- Prohibición de comunicación posterior (no cabe subcontratación)
- Cumplido el servicio, los datos se devuelven o destruyen

Medidas de Seguridad

Nivel básico

- Funciones y obligaciones del personal
- Registro de incidencias
- Identificación y autenticación
- Controles de acceso
- Gestión de soportes
- Copias de respaldo y recuperación

Nivel medio

- Responsable de seguridad
- Auditoría
- Control de acceso físico
- Pruebas con datos reales

Nivel alto

- Distribución de soportes
- Registro de accesos
- Telecomunicaciones

Medidas de Seguridad

1. Acceso físico a los locales e instalaciones donde se encuentren los ficheros
2. Controles de acceso a los ficheros lógicos y físicos. Medidas de identificación y autenticación
3. Definición del régimen de trabajo fuera de los locales donde se encuentren los ficheros
4. Contenido del Documento de Seguridad:
 - Gestión y Administración de contraseñas
 - Gestión de incidencias y procedimientos de prevención y respuesta
 - Funciones y obligaciones del personal
 - Gestión, distribución y almacenamiento de soportes
 - Procedimientos y gestión de copias de respaldo y recuperación

3. Funciones y Obligaciones del personal

Clasificación del personal: responsable del fichero, responsable de seguridad, administradores y usuarios

Responsabilidades y privilegios

Obligaciones generales:

- No comunicar los datos a personas no autorizadas para acceder a los mismos.
- Facilitar los derechos de acceso, rectificación y cancelación a los interesados a petición del Responsable del Fichero.
- Cambiar la contraseña de acceso con la periodicidad establecida o bien cuando sea conocida, accidental o fraudulentamente por compañeros, colaboradores o administradores.
- No escribir, guardar referencia u otros datos de su contraseña de acceso al sistema de información.
- No dejar información visible en la pantalla de su PC cuando abandone su puesto, aunque sea de manera temporal, si hay alguna persona ajena a la empresa.
- Destruir toda la información en soporte papel que pueda resultar delicada de manera que resulte ilegible antes del desecho.
- Hacer las copias de seguridad de toda la información introducida o generada por el sistema informático.

4. Realización de una Auditoría de Protección de Datos

Checklist legal básico

1. ¿Qué tipos de ficheros/datos hay en la empresa?

- Clientes y proveedores
- Recursos humanos, gestión de nóminas, procesos de selección
- Contactos
- Servicio de Atención al cliente
- Actividades de promoción/mailling
- Actividades de formación

2. ¿Cómo se obtienen los datos?

3. ¿Con qué finalidades se usan?

4. ¿Existen terceros implicados en el tratamiento?

5. ¿Se han definido las funciones del personal en materia de protección de datos?

6. ¿Existe un procedimiento para el ejercicio de los derechos?

4. Realización de una Auditoría de Protección de Datos

Checklist técnico básico

1. ¿Existe Documento de Seguridad?
2. ¿Existe un control para el acceso, modificación o supresión de los datos?
3. ¿Existen restricciones al acceso, modificación o supresión de los datos?
4. ¿El personal conoce las obligaciones básicas en materia de protección de datos?
5. ¿Existen registros de incidencias, soportes, privilegios del personal, contraseñas, copias de seguridad,...?
6. ¿Se ha asignado a alguien de la empresa la función de controlar el cumplimiento de la normativa de protección de datos?
7. Se realizan auditorías o controles periódicos de lo anterior?

4. Realización de una Auditoría de Protección de Datos

Elaboración o revisión de formularios, contratos y comunicaciones

Comprobación del deber de información, consentimientos, uso de los datos y confidencialidad

- Contratos con clientes y proveedores
- Contratos de trabajo
- Ofertas publicitarias y promociones, comunicaciones comerciales por vía electrónica
- Facturas
- Formularios web

Sensibilización del personal

Información acerca de sus deberes, gestión de los datos, Documento de Seguridad (firma)

4. Realización de una Auditoría de Protección de Datos

Adaptación de las medidas de seguridad

Determinación del nivel de seguridad en función de los datos

Comprobación y revisión de las medidas implantadas

· Informe o **Documento de Seguridad**
· Revisión de documentación: registros (accesos, incidencias, entrada y salida de soportes, copias de seguridad), lista de usuarios, privilegios,...

Informe de auditoría con propuesta de medidas correctoras

Implicación del personal informático o empresa de mantenimiento

5. Notificación de los ficheros

Notificación de la existencia de los ficheros

Modelos de la Agencia Española de Protección de Datos

Sistema NOTA

Declaración en papel, Internet y con firma electrónica

Ficheros previamente inscritos: modificación o cancelación, en su caso

1. Fichero de clientes y proveedores

2. Fichero de personal/recursos humanos

Tipos de datos

- Nombre y apellidos
- DNI
- Dirección física/correo electrónico
- Teléfono/fax
- Empresa
- Sector de actividad
- Productos y servicios recibidos/prestados
- Datos bancarios
- Créditos

Nivel de seguridad: recomendable medio

No se requiere consentimiento para el tratamiento de los datos

Deber de información (contratos, comunicaciones, facturas,...)

Finalidad: Gestión de clientes y proveedores, gestión económica y contable, facturación

Cesiones de datos

- Agencia Tributaria: retenciones e ingresos a cuenta
- Bancos y Cajas de Ahorro: pagos por transferencia bancaria

No requieren consentimiento

Terceros con acceso a los datos

- Gestoría fiscal y contable
- Empresa de mantenimiento informático
- Servicios de envío de correspondencia
- Servicios de transporte de mercancías

Confidencialidad en servicios de limpieza

Tipos de datos

- Nombre y apellidos
- DNI
- Número de la Seguridad Social
- Imagen
- Dirección física/correo electrónico
- Teléfono/fax
- Profesión, titulaciones, historial académico, experiencia profesional
- Aficiones y estilo de vida
- Datos bancarios
- Ingresos (nóminas)

Otros posibles: afiliación sindical, salud

Nivel de seguridad: generalmente medio

No se requiere consentimiento para el tratamiento de los da

Deber de información en contratos

6. Ejemplos prácticos
Personal/Recursos Humanos

Finalidades: gestión de personal, procesos de selección, gestión de nóminas, prevención de riesgos laborales

Cesiones de datos

- Agencia Tributaria
- INAEM
- Tesorería General de la Seguridad Social
- Bancos y Cajas de Ahorro
- Mutualidades
- Sindicatos
- Aseguradoras

Terceros con acceso a los datos

- Gestoría laboral
- Servicios de mantenimiento informático

Gracias por su atención