Manual de Formación Básica para trabajadores de *AGUAS DE CASTILLA LA MANCHA*

INDICE

1. INTRODUCCIÓN

A través del presente manual se quiere dar a conocer a los trabajadores de AGUAS DE CASTILLA LA MANCHA unos principios de actuación necesarios en relación con la normativa de Protección de Datos de Carácter Personal.

Este manual trata los aspectos generales de la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) y su Reglamento de Desarrollo que se encuentran directamente relacionados con aquellos puestos de trabajo que dentro de la estructura de la empresa pueden acceder de manera directa o accesoria a datos de carácter personal debiendo por ello seguir y respetar una serie de pautas y procedimientos.

A través de este Manual de Formación Básica de los Trabajadores se pretende transmitir una serie de conocimientos básicos sobre Protección de Datos además de despertar el interés por esta normativa de todos los trabajadores ya que respetar los preceptos incluidos en la normativa es responsabilidad de todos los componentes de AGUAS DE CASTILLA LA MANCHA

Por todo ello, DGE Data pretende aportar con la publicación del presente manual la información necesaria acerca de las medidas a adoptar para favorecer la consecución de los objetivos empresariales en materia de Protección de Datos.

2. NORMATIVA BÁSICA

El objetivo del presente capítulo es introducir al trabajador de AGUAS DE CASTILLA LA MANCHA en la normativa básica que regula la Protección de Datos. En concreto, los dos principales preceptos por los que actualmente se rige la materia son la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal y el Real Decreto 1720/2007 por el que se aprueba el Reglamento de Desarrollo de la LOPD.

Dado que la normativa es muy extensa y el objetivo del presente manual es facilitar al trabajador la necesaria adaptación a la nueva política de Protección de Datos que está adoptando AGUAS DE CASTILLA LA MANCHA, nos limitaremos a hacer referencia a aquellos aspectos concretos de la normativa que estén directamente relacionados con los trabajadores de AGUAS DE CASTILLA LA MANCHA que en el ámbito de sus funciones traten con datos de carácter personal.

Conceptos Básicos

Antes de entrar a analizar en concreto los aspectos antes mencionados, consideramos de interés definir algunos conceptos básicos que irán apareciendo a lo largo del presente manual y sobre los que se asienta toda la normativa. Tanto la Ley Orgánica antes mencionada como el Reglamento que la complementa son de aplicación a datos de carácter personal que estén registrados en soporte físico y a su posterior tratamiento ya sea por entidades públicas como privadas.

- *Datos de carácter personal*: cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables. Ejemplo: nombre y apellidos, teléfono, dirección, datos de actividades comerciales, datos económicos o financieros, datos de salud, de solvencia patrimonial, etc…

- *Afectado o interesado*: persona física titular de los datos objeto de tratamiento. Ejemplo: en un fichero de empleados de una empresa, los afectados serán todos los trabajadores.

- *Fichero*: todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados sin importar su forma o modalidad de creación, almacenamiento, organización y acceso.

- *Fichero no automatizado:* conjunto de datos de carácter personal organizado de forma no automática y estructurado según criterios que permitan su acceso sin esfuerzos desproporcionados.

- *Persona identificable:* persona cuya identidad pueda determinarse mediante cualquier información referida a su identidad. Una persona física **no** se considerará identificable si dicha identificación supone esfuerzos desproporcionados.

- *Tratamiento de datos*: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación de datos. Ejemplo: recoger datos de empleados para confeccionar sus contratos y sus nóminas.

- *Responsable del fichero o tratamiento*: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento. Suele ser la empresa, profesional o ente titular de los ficheros.

- *Encargado del tratamiento*: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento. Ejemplo: la gestoría que confecciona las nóminas de los empleados.

- *Cesión o comunicación de datos*: toda revelación de datos realizada a una persona o entidad distinta del interesado. En algunos casos las cesiones de datos son necesarias para la finalidad de creación del fichero. Ejemplo: ceder datos de empleados a la Seguridad Social o a la Hacienda Pública.

- *Fuentes accesibles al público*: aquellos datos cuya consulta puede ser realizada por cualquier persona. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, las guías de servicios de comunicaciones electrónicas y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación social.

Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal

En este apartado, haremos referencia a aquellos artículos de la LOPD que puedan afectar directamente a los trabajadores de AGUAS DE CASTILLA LA MANCHA que en el ejercicio de las funciones propias del puesto desempeñado dentro de la organización empresarial tratan datos de carácter personal. Haremos por lo tanto una primera exposición teórica de dichos preceptos. En el capítulo 3 del presente manual, el trabajador encontrará la aplicación práctica de lo que a continuación se expone. Esta aplicación práctica se materializa en una serie de procedimientos y obligaciones que todo trabajador deberá cumplir con el fin de respetar la normativa de protección de datos.

Artículo 10 LOPD. Deber de secreto
Según este artículo, todo trabajador que intervenga en alguna fase del tratamiento de datos está obligado al secreto profesional respecto a dichos datos. Esta obligación permanecerá vigente incluso después de finalizar la relación laboral con el titular del fichero.

Artículo 11 LOPD. Comunicación de datos
Para que los datos de carácter personal puedan ser comunicados a un tercero, tiene que existir un fin directamente relacionado con las funciones del cedente y cesionario. Un ejemplo práctico: la empresa AGUAS DE CASTILLA LA MANCHA cede los datos de sus trabajadores al INEM, a la Seguridad Social y a la Hacienda Pública. Esta cesión está justificada para la correcta gestión de nóminas y seguros sociales.
En base a este precepto, hacemos especial referencia a la circulación de este tipo de datos a través de faxes, correos electrónicos, etc. entre empleados de una misma empresa, envíos a empresas colaboradoras que nos lo solicitan o cualquier otro tipo de comunicación de datos. Antes de realizar envíos de este tipo, sería conveniente que el trabajador comprobara si la información que va a enviar contiene datos de carácter personal y si el envío cumple con todos los preceptos incluidos en el art. 11 antes mencionado.

Artículo 12 LOPD. Acceso a datos por cuenta de terceros
Según este precepto, un tercero puede acceder a ficheros con datos de carácter personal cuando sea necesario para prestar un servicio al titular del fichero. Un ejemplo práctico: una empresa realiza la gestión de Recursos Humanos a través de una gestoría. En este caso existiría un tratamiento de datos por cuenta de terceros. Este acceso a datos tiene un fin relacionado con la actividad de la empresa (realización de nóminas, gestión de seguros sociales...) y se realiza en base a un contrato de prestación de servicios.

Art. 25 LOPD. Creación de ficheros
Según este artículo, solo se pueden crear ficheros que contengan datos de carácter personal cuando sea necesario para la actividad u objeto legítimos del titular de ficheros. Un ejemplo práctico: una tienda de ropa crea un fichero llamado "Datos salud proveedores". La información que contiene dicho fichero no es necesaria para la correcta gestión de la relación empresa-proveedor y por lo tanto no sería legítimo mantener un fichero de este tipo.

Real Decreto 1720/2007 de Desarrollo de la LOPD

El Reglamento de Desarrollo de la LOPD, que entra en vigor mediante la publicación del Real Decreto mencionado, establece medidas técnicas y organizativas para garantizar la seguridad de ficheros que contengan datos de carácter personal. Es la puesta en práctica de los preceptos expuestos en la Ley Orgánica.
Como hiciéramos con dicha ley, en este apartado nos limitaremos a profundizar en aquellos aspectos del Reglamento de Medidas de Seguridad que estén directamente relacionados con los trabajadores de AGUAS DE CASTILLA LA MANCHA que en el ámbito de sus funciones laborales, puedan acceder de manera directa o accesoria a datos de carácter personal.
Como premisa, debemos indicar que las Medidas de Seguridad tienen carácter acumulativo por lo que debemos aplicar el nivel básico a todos los ficheros; a ficheros que requieran un nivel medio de protección se les aplicará el nivel básico + medio y del mismo modo a los de nivel alto se les aplicará el básico + medio + alto.

Art. 88 Reglamento de Desarrollo. Documento de Seguridad
En este artículo se detalla el contenido mínimo del documento de seguridad. Para los trabajadores de AGUAS DE CASTILLA LA MANCHA la importancia de este artículo reside en que **el documento de seguridad es de obligado cumplimiento para todo el personal con acceso a datos automatizados de carácter personal.**

Art. 89 Reglamento de Desarrollo. Funciones y obligaciones del personal
Las funciones y obligaciones de los trabajadores que acceden a datos de carácter personal tienen que estar claramente definidas; será tarea del responsable del fichero hacer conocer estas normas a todos los empleados y las consecuencias de su incumplimiento.

Art. 91 Reglamento de Desarrollo. Control de acceso
Los usuarios de sistemas de información que contengan datos de carácter personal dispondrán de acceso autorizado solo para datos y recursos necesarios para el desarrollo de sus funciones.

Art. 99 Reglamento de Desarrollo. Control de acceso físico (Para ficheros con nivel de seguridad MEDIO)
Solo el personal que figure autorizado en el Documento de Seguridad podrá tener acceso a los locales donde se sitúen los sistemas de información que manejan datos de carácter personal.

Art. 104 Reglamento de Desarrollo. Telecomunicaciones (Para ficheros con nivel de seguridad ALTO)
Tanto la distribución de soportes como la transmisión de datos de carácter personal a través de redes de telecomunicaciones de deberá realizar cifrando dichos datos para garantizar que la información no pueda ser inteligible o manipulada por terceros.

3. FUNCIONES Y OBLIGACIONES ESPECÍFICAS DEL PERSONAL EN MATERIA DE PROTECCIÓN DE DATOS

Puestos de trabajo

Entendemos por puesto de trabajo todo tipo de dispositivo por el que se pueda acceder a ficheros con datos de carácter personal.

Para una mejor implantación de las medidas de seguridad requeridas por la normativa, recomendamos que cada puesto de trabajo esté bajo la responsabilidad de una persona autorizada en el apartado del Documento de Seguridad relativo a Usuarios del Sistema con el fin de garantizar que la información a la que se accede a través del puesto de trabajo que se encuentra bajo su responsabilidad no pueda ser vista por personas no autorizadas. Para tal fin, es conveniente que pantallas, impresoras y demás dispositivos que formen parte del puesto de trabajo estén ubicados físicamente en lugares donde se pueda garantizar confidencialidad.

Cuando el responsable de un puesto de trabajo se ausente deberá dejarlo en un estado que impida visualizar datos de carácter personal. Esto se puede realizar a través de un protector de pantalla que requiera contraseña para su desactivación.

Cuando se trabaja con impresoras es importante asegurarse que en la bandeja de salida no queden documentos impresos que contengan datos de carácter personal. Si las impresoras son recursos compartidos con otros usuarios que no están autorizados a acceder a datos de carácter personal, la persona que realiza la impresión deberá retirar los documentos que contienen este tipo de datos según vayan saliendo de la impresora.

Contraseñas personales

Las contraseñas son unas de las claves para la correcta implantación de las medidas de seguridad en los datos. Se pueden considerar como llaves de acceso al sistema de información que contiene ficheros con datos de carácter personal; es por esto que deberán ser confidenciales y personales siendo cada usuario autorizado el responsable de su buen uso. Si en algún momento la confidencialidad se viera comprometida el usuario deberá comunicarlo, mediante la notificación de una incidencia, al responsable de ficheros para que se proceda a la asignación de una nueva contraseña.

Incidencias

Se considera incidencia cualquier evento que se pueda producir de forma esporádica y que pueda suponer un peligro para la seguridad de los ficheros que contienen datos de carácter personal. La normativa exige que se mantenga un registro de incidencias actualizado en todo momento.
Los usuarios que tengan conocimiento de una incidencia de cualquier tipo deberán comunicarla al responsable del fichero y proceder a su registro. Si se conoce una incidencia y no se notifica al responsable, se puede considerar como falta contra la seguridad de ficheros.

Gestión de soportes

Entendemos por soporte informático cualquier medio de grabación o recuperación de datos que se usen para realizar copias o cualquier otro proceso intermedio en la gestión de ficheros (disquetes, CD-ROM, unidades Zip...)

Los soportes reutilizables que contengan datos de ficheros de nivel medio de seguridad deberán ser borrados completamente antes de su reutilización para que no sea posible recuperar las copias de datos de carácter personal que en ellos se almacenaban.

Así mismo todos los soportes que contengan datos de carácter personal se tienen que almacenar en lugares accesibles solo a personas autorizadas.

Cuando se vaya a realizar una salida de soportes que contengan datos de carácter personal de nivel medio se deberá pedir autorización previa al responsable del fichero.

La distribución de soportes en el caso de ficheros con datos de nivel alto se deberá realizar con un sistema de encriptación para garantizar que la información no sea inteligible o manipulada durante el transporte.

Movimiento de datos a través de redes de telecomunicaciones

A fin de controlar las entradas y salidas de datos de carácter personal mediante correo electrónico se recomienda que dichos movimientos se realicen desde cuentas de correo controladas por usuarios autorizados por el responsable del fichero.

En el caso de ficheros que contengan datos de nivel alto que deban ser enviados por correo electrónico o por sistemas de transferencia de ficheros por redes públicas o no protegidas será necesario encriptar dichos datos para que solo puedan ser leídos por el destinatario

Gestión Documental

Se considera fichero no automatizado aquel conjunto de datos de carácter personal organizado de forma no automatizada que se encuentre estructurado con criterios específicos y a los que se pueda acceder sin esfuerzo desproporcionado. Ejemplos de este tipo de sistema de información son las fichas para gestionar inscripciones o carnets, archivos de curriculum vitae en carpetas, etc…

La documentación no mecanizada requiere igualmente la aplicación de normas y procedimientos de seguridad. Incluso se hace necesario establecer pautas y criterios claros y estrictos ya que el manejo de este tipo de ficheros hoy en día sigue siendo muy común dentro de las organizaciones.

El personal que maneje habitualmente estos ficheros y aquellos que puedan acceder de manera esporádica a archivos y soportes debe cumplir con las siguientes normas de seguridad.

El ***archivo de oficina*** de cada departamento se debe generar con criterios de separación y diferenciación según la utilidad de cada documento de manera que no se mezclen expedientes generados para distintas funciones. De hecho, los expedientes se deben conservan físicamente diferenciados y separados.

El responsable de cada departamento o unidad administrativa elaborará un ***cuadro de clasificación de fondos*** donde se incluyen todas las ***series documentales*** que se generen en dicho departamento. Este cuadro será la base para transferir el archivo de oficina al general de la empresa. Las series documentales incluidas en este cuadro se ordenarán siguiendo un criterio que permita recuperar de forma sencilla la información contenida. A modo de ejemplo, las nóminas de empleados se ordenarán cronológicamente y los curriculum vitae alfabéticamente o por puesto a desempeñar.

Cada unidad y departamento de AGUAS DE CASTILLA LA MANCHA deberá disponer de archivadores, armarios y cajoneras con llave. Como regla general, los dispositivos de almacenamiento permanecerán bajo llave, siendo responsable de su

custodia el trabajador que genera y archiva dicha documentación. En los casos en que deban acceder a una misma documentación varias personas del mismo departamento se solicitará la llave al responsable y se devolverá lo antes posible.

Cuando la documentación se encuentre fuera de los dispositivos de almacenamiento, el responsable de su custodia se encargará de impedir accesos por personas no autorizadas. Además, no está permitido extraer documentos aislados de una serie documental para general otras series o expedientes. En caso de ser necesario, se fotocopiará dicha documentación y se destruirá una vez haya cumplido sus fines.

Cada departamento o unidad es responsable de la documentación que genera hasta su transferencia al archivo general. Por tanto es necesario evitar acumulaciones de documentos incluyéndolos en sus correspondientes expedientes o serie documental en cuanto sea posible para de este modo evitar pérdidas o accesos no autorizados.

En caso de manejar documentación no mecanizada considerada de ***nivel alto***, los armarios y archivadores se aislarán en áreas con acceso protegido con puertas y llaves o dispositivo equivalente que permanecerán cerradas cuando no sea necesario el acceso. En cualquier caso solo podrá acceder a este tipo de documentación el personal autorizado en el Documento de Seguridad.
No podrán fotocopiarse o reproducir documentos con datos de nivel alto sin la autorización previa del personal designado en el Documento de Seguridad. Una vez desechadas las copias se deberá proceder a su destrucción inmediata.

Consecuencias del Incumplimiento

Artículo 58.1 del Estatuto de los Trabajadores: Los trabajadores podrán ser sancionados por la empresa por incumplimientos laborales de acuerdo con la graduación de faltas y sanciones que se establezcan en las disposiciones legales o en el convenio colectivo que sea aplicable.

Capítulo I Código Penal

Artículo 197.1: se podrán imponer penas de prisión y multa a quien utilice en perjuicio de tercero datos reservados de carácter personal o familiar que se hallen registrados en ficheros o cualquier archivo o registro público o privado.

Artículo 199.1: quien revele secretos ajenos de los que tenga conocimiento por razón de su oficio o sus relaciones laborales será castigado con pena de prisión y multa.

Título IV LOPD

Este título hace referencia a las infracciones en las que puede incurrir la empresa por incumplimiento de los deberes descritos en la norma. Algunos de estos deberes en la

práctica se trasladan a los trabajadores que habitualmente manejan los datos dentro de la organización.

Artículo 43.2e: Se considerará infracción leve* el incumplimiento del deber de secreto establecido en el art. 10 de la propia ley.

*Debido a las consecuencias profesionales que pueden derivarse del incumplimiento del deber de secreto, podría ser considerado como falta grave o muy grave para el trabajador.

Artículo 43.3h: Será infracción grave no respetar las medidas de seguridad* establecidas en el Documento de Seguridad y en el Reglamento de Medidas de Seguridad.

*Las medidas de seguridad que influyen directamente en el trabajador hacen referencia al mantenimiento de sus claves de acceso, acceder a datos que no le sean necesarios para su trabajo, dejar documentación sin custodiar, ausentarse de su puesto de trabajo y no activar el salvapantallas con contraseña, crear y sacar fuera de los locales soportes magnéticos con datos personales sin autorización…

Artículo 43.4b: Se considerará infracción muy grave comunicar o ceder* datos sin consentimiento previo del titular de esos datos.

*El trabajador no debe nunca pasar datos personales de clientes, proveedores, comerciales, trabajadores… a empresas que no estén autorizadas. En caso de duda, consultar siempre con el Departamento Jurídico para confirmar que la cesión es legítima.