

CASO PRÁCTICO: APLICACIÓN L.O.P.D.

Recientemente se ha creado una agencia de titularidad pública cuya finalidad es gestionar subvenciones y ayudas a autónomos. Dentro de su plan estratégico de lanzamiento, ha decidido externalizar en una empresa de hosting la gestión de los sistemas de información utilizados para la gestión de las ayudas. El resto de la información gestionada por la agencia se almacenará y tratará en sistemas propios.

Los solicitantes de ayudas deben aportar entre otros estos datos:

Nombre y apellidos, NIF, N° de afiliación a la seguridad social, últimos tres recibos abonados a la seguridad social como autónomos.

Para la gestión interna de su personal, la agencia ha previsto la implantación de un sistema de fichaje mediante huella digital. En su sede, los empleados deberán portar una tarjeta identificativa con su fotografía.

La agencia cuenta entre su personal con algunos que tienen reconocido un cierto grado de minusvalía, aspecto que debe ser tenido en cuenta en la gestión de las nóminas a efectos de aplicación de las correspondientes deducciones en el tipo de IRPF aplicado. Dentro del expediente del servicio médico de la agencia almacena un historial clínico de cada empleado, en formato papel que posteriormente se digitaliza.

Por otra parte la agencia ha contratado la seguridad de sus instalaciones con una empresa privada. Se han instalado cámaras CCTV y un circuito cerrado de televisión. Para el visionado de imágenes de dichas instalaciones. No está previsto el almacenamiento de dichas imágenes para su posterior reproducción.

Los únicos proveedores de la agencia son empresas. Existe un fichero de proveedores donde se almacenan los datos de contacto profesionales de sus representantes: teléfono, fax, email y dirección postal. Cuando asisten a reuniones en la sede de la agencia, seguridad recaba su DNI a efectos de control de visitas.

Diseñar un plan de adecuación que resuma las acciones principales que deberá llevar a cabo la citada agencia para cumplir la normativa de protección de datos, con especial énfasis en las medidas de seguridad a implantar.

1.IDENTIFICACIÓN DE LOS FICHEROS

IDENTIFICACIÓN DE LOS FICHEROS		
FICHEROS/TRATAMIENTOS	NIVEL MEDIDAS SEGURIDAD	OBSERVACIONES
Ayudas a autónomos	Básico	
Empleados	Básico	
Nóminas	Básico	Aunque el grado de minusvalía es un dato de salud, su uso en este caso constituye una de las excepciones previstas en el artículo 81.6 del RLOPD, por lo que sólo sería exigible el nivel de medida de seguridad básico.
Gestión económica-administrativa	Básico	
Control de visitas	Básico	La agencia es responsable del fichero aunque la gestión del mismo la realice la empresa de seguridad.
Video-vigilancia	Básico	Hay tratamiento de datos pero no existe fichero, puesto que las imagenes no se almacenan.No procede inscripción en RGPD.
Historiales clínicos de los empleados	Alto	Almacena datos de salud . Sistema de tratamiento mixto : automatizado y no automatizado

2. Determinar y formalizar los contratos de prestación de servicios:

Contrato por escrito , encargado del tratamiento de datos y medidas de seguridad estipuladas con la empresa de Hosting y la empresa de seguridad.

3. Elaboración del documento de seguridad. (artículo 88 LOPD) : documento interno, identificación del responsable de seguridad , realizar controles periódicos para verificar el cumplimiento del documento.

4. Implantación de las medidas de seguridad recogidas en el documento de seguridad

5. Como consecuencia de datos personales de nivel alto, debe establecerse un plan de auditoría de medidas de seguridad que habrá que realizarse al menos cada dos años (artículo 96 RLOPD)

6. Deben incluirse en todos los formularios de recogida de datos de personas físicas cláusulas informativas conforme a lo establecido en el artículo 5 de la LOPD. EL cumplimiento del deber de información en el caso de visionado de imágenes del circuito CCTV debe hacerse efectivo mediante la colocación de distintivos informativos ubicados en lugares suficientemente visibles (instrucción 1/2006, 8 noviembre AEPD) sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

7. Habilitar los medios para el ejercicio de los derechos ARCO (por ejemplo establecer diversos canales de atención : número de teléfono gratuito , dirección postal , correo electrónico...).