



Expediente Nº: E/00152/2010

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la Organización Impulsora del Discapacitado (OID), en virtud de denuncia presentada ante la misma por el Gobierno del Principado de Asturias, y en base a los siguientes

HECHOS

PRIMERO: Con fecha 5 de enero de 2010, tuvo entrada en esta Agencia un escrito remitido por el Gobierno del Principado de Asturias en el que declara que se ha iniciado en esa Dirección General un procedimiento sancionador a la Organización Impulsora del Discapacitado (en lo sucesivo OID), por la organización habitual de un sorteo de ámbito regional, sin contar con la preceptiva autorización administrativa.

Examinada la documentación intervenida e incautada por los miembros de la Sección de Inspección y Control de Juego de la Unidad de Policía Adscrita el día 20 de julio de 2009, la instructora del procedimiento advierte la existencia de documentos que contienen datos de carácter personal y respecto a los que el tratamiento seguido podría ser constitutivo de infracción administrativa.

La documentación referida es la siguiente:

- Resoluciones de la Consejería de Vivienda y Bienestar Social del Principado de Asturias en que se reconoce la condición de discapacitado a los trabajadores-colaboradores de la organización cuyo expediente sancionador se está tramitando, con indicación de las dolencias que los mismos sufren así como los porcentajes de minusvalía que a las mismas corresponden.

- Consignación de los datos indicados en el apartado anterior en determinados documentos como las fichas de socio de la organización, en los que figuran apartados específicos para hacer constar datos como el grado de minusvalía o tipo de afección que los trabajadores-colaboradores sufren, estudios realizados, y demás datos de carácter personal.

- Certificados de organizaciones como FUNDACIÓN C.E.S.P.A., "PROYECTO HOMBRE", en que se indican los tratamientos seguidos por la persona a que el certificado se refiere así como los periodos de rehabilitación seguidos.

SEGUNDO: Tras la recepción de la denuncia, el Director de la Agencia Española de Protección de Datos ordenó a la Subdirección General de Inspección de Datos la realización de las actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

La OID dispone de Documento de Seguridad cuyo contenido principal queda estructurado como sigue:

- Ámbito de la aplicación del documento.

- Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento.

Identificación y Autenticación.

Control de acceso:

Control de acceso físico.

Registro de accesos

Gestión de soportes y documentos.

Registro de entrada y salida de soportes.

Gestión y distribución de soportes.

Criterios de archivo.

Almacenamiento de la información.

Custodia de soportes.

Acceso a datos a través de redes de comunicaciones.

Régimen de trabajo fuera de los locales de la ubicación del fichero

Traslado de documentación.

Ficheros temporales

Copia o reproducción.

Copias de seguridad

Responsable de seguridad

Procedimiento general de información al personal.

Funciones y obligaciones del personal

Procedimiento de notificación, gestión y respuestas ante las incidencias.

Procedimientos de revisión.

Revisión del documento de seguridad.

Auditoría.

Informe mensual sobre el registro de accesos.

Consecuencias del incumplimiento del Documento de Seguridad.

ANEXOS:

ASPECTOS ESPECÍFICOS RELATIVOS A LOS DIFERENTES FICHEROS.

Aspectos relativos al fichero CLIENTES

Aspectos relativos al fichero EMPLEADOS Y NOMINAS

Aspectos relativos al fichero PROVEEDORES



Aspectos relativos al fichero INFORMACIÓN CONTABLE Y FINANCIERA
NOMBRAMIENTOS.

AUTORIZACIONES FIRMADAS PARA LA SAUDA O RECUPERACIÓN DE DATOS

Autorización para la salida de ficheros.

Recuperaciones de datos.

Escrito de solicitud de recuperación de datos.

Autorización de recuperación de datos.

INVENTARIO DE SOPORTES.

Inventario de soportes automatizados.

Gestión de soportes no automatizados.

REGISTRO DE INCIDENCIAS.

Tabla de registro de incidencias.

CONTRATOS O CLÁUSULAS DE ENCARGADOS DE TRATAMIENTO.

Contrato de prestación de servicios.

REGISTRO DE ENTRADA Y SALIDA DE SOPORTES

Registro de entrada.

Registro de salida.

RELACIÓN DE USUARIOS.

TRATAMIENTO DE FICHEROS EN DISPOSITIVOS PORTÁTILES.

DOCUMENTO DE USO INTERNO SOBRE PROTECCIÓN DE DATOS DE CARÁCTER
PERSONAL.

CONTROL DE ACCESO DEL PERSONAL EXTERNO.

REGISTRO GENERAL DE ACCESOS.

MÉTODOS DE CIFRADO.

- Concretamente, los ficheros sujetos a las medidas de seguridad establecidas en este documento, con indicación del nivel de seguridad correspondiente, son los siguientes:

CLIENTES: Datos personales de los clientes, con nivel de seguridad bajo

EMPLEADOS Y NOMINAS: datos personales de los empleados, con nivel de seguridad medio

PROVEEDORES: datos personales de los proveedores, con nivel de seguridad bajo

INFORMACIÓN CONTABLE Y FINANCIERA: información sobre datos bancarios, contabilidad y facturación, con nivel de seguridad medio

- En el Anexo I del documento de seguridad se describen detalladamente cada uno de los ficheros o tratamientos, junto con los aspectos que les afectan de manera particular

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el Director de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

II

La denuncia recibida se concreta en que la OID tiene documentación que contiene datos de carácter personal, desconociendo el denunciante si su tratamiento constituye infracción administrativa.

El artículo 26 de la LOPD, dispone lo siguiente:

“1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia Española de Protección de Datos.

2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros.

3. Deberán comunicarse a la Agencia Española de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.

4. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles.

En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.

5. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia Española de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos”.

La OID procedió a la inscripción de los ficheros de clientes, empleados y nóminas, proveedores, e información contable y financiera en el mes de junio de 2009.

III

En cuanto al tratamiento de los datos personales, el artículo 6 de la LOPD dispone: *“1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del*



afectado, salvo que la Ley disponga otra cosa.

Añadiendo el apartado 2 del citado artículo que *“no será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación comercial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado”*.

El tratamiento de datos de carácter personal tiene que contar con el consentimiento del afectado o, en su defecto, debe acreditarse que los datos provienen de fuentes accesibles al público, que existe una Ley que ampara ese tratamiento o una relación contractual o comercial entre el titular de los datos y el responsable del tratamiento que sea necesaria para el mantenimiento del contrato.

El tratamiento de datos sin consentimiento de los afectados constituye un límite al derecho fundamental a la protección de datos. Este derecho, en palabras del Tribunal Constitucional en su Sentencia 292/2000, de 30 de noviembre (F.J. 7 primer párrafo) *“consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el estado o un particular (...)”*.

Son pues elementos característicos del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos.

En el presente caso, los documentos encontrados parecen acreditar que la Organización trata los datos de las personas que allí trabajan, para lo que encuentra habilitación legal en el apartado 2 del mencionado artículo 6 de la LOPD.

IV

El artículo 9 de la LOPD establece lo siguiente:

“1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados

y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley”.

Durante las actuaciones previas de investigación se ha podido constatar que la OID ha elaborado un documento de seguridad que cumple las especificaciones establecidas reglamentariamente. A pesar de que esta Agencia no ha tenido acceso a la documentación que tiene el Gobierno del Principado de Asturias, si se recoge en sus manifestaciones que han encontrado documentación que puede tener datos de salud de las personas asociadas. En este sentido hay que señalar que el Real Decreto 1720/2007 establece que si en los ficheros, tanto automatizados como en papel, se conservan datos de salud, considerados como sensibles o especialmente protegidos, es preciso implementar las medidas de seguridad de nivel alto.

Por lo tanto, de acuerdo con lo señalado,

Por el Director de la Agencia Española de Protección de Datos,

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
2. **NOTIFICAR** la presente Resolución a la Organización Impulsora del Discapacitado y al Gobierno del Principado de Asturias.

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con



arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

Madrid, 6 de septiembre de 2010

EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCIÓN DE DATOS

Fdo.: Artemi Rallo Lombarte