Procedimiento Nº: A/00192/2013

RESOLUCIÓN: R/02467/2013

En el procedimiento A/00192/2013, instruido por la Agencia Española de Protección de Datos a la entidad **NUBESIS S.L.**, en virtud de su auto denuncia presentada y en virtud de los siguientes,

ANTECEDENTES

PRIMERO: En fecha 22 de julio de 2013 tiene entrada un escrito firmado por el Director Técnico de NUBESIS, S.L., en el que pone en conocimiento de la Agencia un fallo técnico en el servicio que esta compañía presta a The Phone House, S.L.U. a través de la agenda electrónica Bookitit, como consecuencia del cual se vieron comprometidos el nombre y el teléfono de una cliente de esta segunda compañía, datos que fueron indebidamente remitidos por error a 72 receptores, según les fue reportado el 30 de mayo de 2013 por el responsable del fichero.

Según expone NUBESIS, S.L., la incidencia, que fue oportunamente comunicada a la persona afectada, fue resuelta el 6 de junio de 2013, reflejándose en el Documento de seguridad de la compañía.

La compañía, en su calidad de encargado de tratamiento por cuenta de The Phone House, S.L.U., solicita a la Agencia que se analice si la incidencia es merecedora de *"inspección y, en su caso, sanción"* y se valore la posibilidad de atender a lo previsto en el artículo 45.6 de la LOPD, al tratarse de la primera vez en que pudiera haber faltado a su deber (puntualmente y por un desafortunado fallo técnico, inmediatamente resuelto) y al bajo nivel de ingresos de la empresa.

SEGUNDO: Con fecha 1 de octubre de 2013, el Director de la Agencia Española de Protección de Datos acordó someter a trámite de audiencia previa el presente procedimiento de apercibimiento A/00192/2013, con arreglo a lo dispuesto en el artículo 45.6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), por la auto denuncia de la citada entidad, por la presunta infracción del artículo 9 de dicha norma, en relación con los artículos 91 y 93 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, tipificada como grave en el artículo 44.3.h) de la citada Ley Orgánica. Dicho acuerdo fue notificado a NUBESIS, S.L.

TERCERO: Con fecha 11/10/2013 se recibe en esta Agencia escrito de la citada entidad en el que comunica: *"…Que no existe ninguna argumentación adicional que añadir a lo ya expuesto en el escrito de Auto-denuncia presentado por Nubesis S.L. el 22 de junio de 2013, al no haber tenido lugar, hasta la fecha, hecho o consecuencia posterior alguno en relación con el presente procedimiento…"*

HECHOS PROBADOS

En fecha 22 de julio de 2013 tiene entrada un escrito firmado por el Director Técnico de NUBESIS, S.L., en el que pone en conocimiento de la Agencia un fallo técnico en el servicio que esta compañía presta a The Phone House, S.L.U. a través de la agenda electrónica Bookitit, como consecuencia del cual se vieron comprometidos el nombre y el teléfono de una cliente de esta segunda compañía, datos que fueron indebidamente remitidos por error a 72 receptores, según les fue reportado el 30 de mayo de 2013 por el responsable del fichero.

Según expone NUBESIS, S.L., la incidencia, que fue oportunamente comunicada a la persona afectada, fue resuelta el 6 de junio de 2013, reflejándose en el Documento de seguridad de la compañía (folios 1 a 24).

FUNDAMENTOS DE DERECHO

I

Es competente para resolver este procedimiento el Director de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 37. g) en relación con el artículo 36 de la LOPD.

II

Los hechos expuestos (el nombre y el teléfono de una cliente de la compañía The Phone House, S.L.U., fueron indebidamente remitidos por error a 72 receptores), lo que supone la comisión por parte de la entidad NUBESIS, S.L., de una infracción del artículo 9.1 de la LOPD, según el cual "*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",* en relación con lo dispuesto en el Título VIII del citado Real Decreto 1720/2007, concretamente en los artículos 91 y 93, que establecen lo siguiente:

Artículo 91. *Control de acceso.*

"1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.
2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.
3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.
4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio".

Artículo 93. *Identificación y autenticación.*

"1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.
2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.
3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.
4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible".

III

La vulneración de los preceptos citados aparece tipificada como infracción grave en el artículo 44.3.h) de la LOPD, que considera como tal, "*Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen".*

IV

El apartado 6 del artículo 45 de la LOPD establece lo siguiente:

"*Excepcionalmente el órgano sancionador podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, no acordar la apertura del procedimiento sancionador, y en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que concurran los siguientes presupuestos:*

Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.
Que el infractor no hubiese sido sancionado o apercibido con anterioridad.

Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento".

A este respecto, procede considerar lo establecido en el artículo 45.4 y 5 de la LOPD, que establece lo siguiente:

"4. La cuantía de las sanciones se graduará atendiendo a los siguientes criterios:

a) El carácter continuado de la infracción.
b) El volumen de los tratamientos efectuados.
c) La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.
d) El volumen de negocio o actividad del infractor.
e) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
f) El grado de intencionalidad.
g) La reincidencia por comisión de infracciones de la misma naturaleza.
h) La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas.
i) La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor.
j) Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

5. El órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate, en los siguientes supuestos:

a) Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el apartado 4 de este artículo.
b) Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.
c) Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.
d) Cuando el infractor haya reconocido espontáneamente su culpabilidad.
e) Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente".

En el presente supuesto se cumplen los requisitos recogidos en los apartados a) y b) del citado artículo 45.6 de la LOPD. Junto a ello se constata una cualificada disminución de la culpabilidad de la entidad denunciada por la concurrencia de varios criterios de los enunciados en el artículo 45.4 de la LOPD, concretamente, la ausencia de beneficios y el grado de intencionalidad apreciado.

En el presente caso, ha quedado acreditado que el denunciado ha comunicado a esta Agencia las medidas correctoras adoptada. Teniendo en cuenta estas circunstancias, no procede requerimiento alguno.

De acuerdo con lo señalado,

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

SE ACUERDA:

1.- APERCIBIR (**A/00192/2013**) a **NUBESIS S.L.** con arreglo a lo dispuesto en el artículo 45.6 de la LOPD, en base a la auto denuncia de la citada entidad, por la presunta infracción del artículo 9 de dicha norma, en relación con los artículos 91 y 93 del citado Real Decreto 1720/2007, tipificada como grave en el artículo 44.3.h) de la citada Ley Orgánica.

2.- NOTIFICAR el presente Acuerdo a D. ***A.A.A.*** representante legal de **NUBESIS S.L.**

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 esta acto, según lo previsto en el artículo 46.1 del referido texto legal.

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.

José Luis Rodríguez Álvarez
Director de la Agencia Española de Protección de Datos