**Expediente Nº: E/03948/2013**

**RESOLUCIÓN DE ARCHIVO DE ACTUACIONES**

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad ***PROSEGUR ESPAÑA SL*** en virtud de denuncia presentada por D.ª ***A.A.A.*** y teniendo como base los siguientes

**HECHOS**

**PRIMERO:** Con fecha 3 de junio de 2013, tuvo entrada en esta Agencia escrito de Dª. ***A.A.A.*** en el que denuncia a la empresa PROSEGUR ESPAÑA SL (en adelante PROSEGUR) por conservar los datos de miles de antiguos clientes, siendo sus datos personales accesibles a cualquier trabajador de la compañía. Asimismo manifiesta y aporta grabaciones al efecto, que desde Centro de Gestión de Clientes y Central Receptora de Alarmas se graban las conversaciones con los clientes sin que se informe a los mismos que se va proceder a la grabación, además se encuentran grabadas por una tercera empresa sin haber una custodia efectiva.

Adjunto a la denuncia se ha aportado impresión de pantalla de varios clientes y siete grabaciones.

**SEGUNDO:** Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

1. El denunciante ha aportado impresión de pantalla con datos de varios clientes que han causado la baja obtenidos de las aplicaciones denominadas SIEBEL y MASTER MIND, según sus manifestaciones.

2. En las grabaciones aportadas por el denunciante, la persona que inicia la conversación se identifica como empleado de PROSEGUR y seis de las grabaciones corresponden con requerimientos de pagos y la última con verificación de imágenes.

Dos de las grabaciones correspondientes a requerimiento de deuda corresponde con clientes que son empresas.

En el pen-drive se han etiquetado las grabaciones como realizadas en diciembre de 2012 y una de ellas del 18 de mayo de 2013 asociadas al Departamento de Cobros y al Centro de Gestión de Clientes.

En ninguna de las grabaciones se informa de que se va a proceder a grabar la llamada

3. Tal y como consta en la Inspección E/3948/2013-I/1 realizada en los locales de PROSEGUR en fecha 26 de marzo de 2014:

3.1 El 1 de julio de 2013 se procedió a la segregación de la rama de actividad de PROSEGUR COMPAÑÍA DE SEGURIDAD S.A. a favor de PROSEGUR ESPAÑA SL, siendo esta última compañía la que realiza todas las actividades de seguridad y gestión de los clientes.

4. Respecto de la cancelación de los datos de los clientes

4.1 PROSEGUR manifiesta que los datos personales de los clientes se mantienen

durante la relación contractual y durante los siguientes cinco años tal y como se estipula en el artículo 20 del RD 2364/1994, Reglamento de Seguridad Privada.

Al finalizar la relación contractual con los clientes, durante un periodo de tiempo variable se mantienen sus datos en la Base de Datos de Clientes accesibles a diferentes departamentos mientras duran las actividades de cierre de la relación contractual (desinstalación del sistema de seguridad, entrega de llaves, verificación de cobros,…). Una vez finalizadas se procede al bloqueo de los datos quedando accesibles únicamente para el Responsable de Seguridad y los Administradores de los Sistemas de Información de la compañía.

5. PROSEGUR manifiesta que los empleados de la entidad con acceso a los datos de los clientes utilizan una aplicación denominada "SIEBEL", salvo los empleados de la Central Receptora de Alarmas, ubicada en un domicilio distinto y que está considerada una instalación de "Alta Seguridad" según normativa, los cuales utilizan otra aplicación denominada "MASTER MIND". Este software está considerado también como de alta seguridad y solo se puede acceder a él desde las instalaciones de la Central Receptora.

A este respecto, se verificó que, utilizando identificación y autenticación de un empleado del Departamento de Cobros con el perfil de "*usuario",* no consta información en la base de datos de clientes accesible a través de la aplicación SIEBEL de ninguno de los clientes cuyos datos han sido aportados por el denunciante.

Asimismo se verificó que, utilizando la identificación y autenticación de un Administrador de los Sistemas de Información con el perfil de "*administrador"* se obtiene información de cuatro de los cinco clientes cuyos datos han sido aportados por el denunciante. Dos de los clientes constan con fecha de alta y de baja (2012 y 2010), en otros dos clientes consta únicamente la fecha de alta. PROSEGUR manifiesta al respecto que aunque no figure la fecha de baja los datos se encuentran bloqueados puesto que solo han sido localizados utilizando el perfil de acceso de *administrador*.

Por último, tal y como consta en la documentación aportada por el denunciante, el cliente del que no se ha encontrado ninguna información fue dado de baja de la compañía hace más de 6 años.

También, se verificado que las pantallas accesibles en ambos casos coinciden con las aportadas por el denunciante y corresponden, según manifestaciones de PROSEGUR con la aplicación SIEBEL.

6. En relación con una impresión de pantalla, aportada por el denunciante, donde figuran los datos personales de un cliente y que no coincide con la aplicación SIEBEL, PROSEGUR manifiesta que esta impresión de pantalla corresponde a la aplicación de seguridad denominada "MASTER MIND" y los datos de este cliente se encuentran actualmente bloqueados tal y como se ha verificado al acceder a través de SIEBEL.

A este respecto, PROSEGUR manifiesta que teniendo en cuenta que en el documento aportado por el denunciante no consta la fecha en que se ha obtenido entienden que la pantalla mostrada por los inspectores corresponde a una impresión anterior a la fecha de baja del cliente en abril del 2012.

7. Respecto de las grabaciones de las conversaciones telefónicas

7.1 Todas las conversaciones telefónicas mantenidas con el Centro de Gestión de Clientes, que incluye a los operadores del Departamento de Recobro, son grabadas.

El protocolo de gestión de llamadas telefónicas a clientes incluye grabación de la conversación telefónica e información al cliente sobre ello y sobre los derechos ARCO. En las llamadas entrantes este protocolo fue implementado en el momento de la

creación del Centro de Gestión de Clientes, el cual opera con personal propio y se encuentra ubicado en las instalaciones donde se realiza la presente Inspección. Respecto de las llamadas salientes, el protocolo se implementó en el año 2010.

Si la llamada es entrante a través del número 902******, una locución automática informa de que se va a proceder a la grabación de la conversación como medida de seguridad y control de calidad. Asimismo se indica la forma de ejercer sus derechos ARCO.

Si la llamada es entrante a un número diferente al indicado, generalmente números asignados al Departamento de Recobro, es el operador que atiende la llamada el encargado de informar sobre la grabación siguiendo un argumentario similar al de la locución automática.

En todos los casos cuando la llamada es saliente es el operador que la efectúa el encargado de informar sobre la grabación.

Las conversaciones mantenidas en la Central Receptora de Alarmas también son grabadas siguiendo los criterios descritos.

7.2 PROSEGUR manifiesta que las grabaciones se encuentran accesibles, durante un mes, para los Coordinadores del Centro de Gestión de Clientes. Una vez transcurrido este periodo el acceso se restringe al Responsable del mencionado Centro, al Departamento Jurídico y al Responsable de Seguridad hasta la baja de la relación contractual con el cliente al que corresponde la grabación. A partir de este momento solo es accesible, durante tres años, por el Responsable de Seguridad.

Las grabaciones físicamente se custodian por la empresa BT ESPAÑA con la que tienen suscrito un contrato de prestación de servicios.

7.3 Se ha verificado que, en la fecha de la Inspección realizada, y eligiendo grabaciones de llamadas a clientes al azar (llamadas salientes) el operador que efectúa la llamada informa de la grabación y de lo referente a los derechos ARCO.

7.4 Respecto de las grabaciones aportadas por el denunciante en las que el operador se identifica como empleado de PROSEGUR, la compañía manifiesta que las seis primeras grabaciones corresponden a llamadas salientes del Centro de Gestión de Clientes y la última de ellas de la Central Receptora de Alarmas, no obstante, al no figurar la fecha en la conversación no pueden indicar si las grabaciones son anteriores al año 2010 cuando se comenzó a informar en las llamadas salientes.

## 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

En el presente caso, la denunciante expone que PROSEGUR conserva los datos personales de miles de antiguos clientes siendo accesibles a cualquier trabajador

de la compañía. También, aporta grabaciones llevadas a cabo por dicha empresa, desde el Centro de Gestión de Clientes y la Central Receptora de Alarmas, con las conversaciones con los clientes afirmando que no se informa de que se va proceder a la grabación, además de ser grabadas por una tercera empresa sin haber una custodia efectiva.

La AEPD tiene conferida *"potestad inspectora"* en el artículo 40, apartado 1, que recoge: *"Las autoridades de control podrán inspeccionar..."* El Reglamento 1720/2007 de 21/12, por el que se aprueba el Reglamento de desarrollo de la LOPD en su artículo 122 prevé: *" 1…., se podrán realizar actuaciones previas con objeto de determinar sin concurren circunstancias que justifiquen tal iniciación..."* y el R. D. 1398/1993, de 4/08, del Reglamento del Procedimiento para el ejercicio de la Potestad Sancionadora en su artículo 12 dispone lo siguiente: " *Con anterioridad a la iniciación del procedimiento, se podrán realizar actuaciones previas de investigación.."*

De acuerdo con la normativa citada corresponde al Director de la Agencia Española de Protección de Datos -AEPD- determinar si, a la vista de la denuncia formulada y de los elementos aportados en justificación de la misma, concurre causa justificativa que lleve a la realización de actuaciones previas de inspección, de suerte que en el presente caso, se realizaron dichas actuaciones previas con el resultado expuesto en el Hecho Segundo de la presente resolución.

En la inspección "in situ" realizada por el personal de la Inspección de Datos se centró, básicamente , en la comprobación de los hechos denunciados, consistentes en:

a) En la "conservación" de los datos de los clientes una vez cumplida la finalidad y su acceso por cualquier trabajador.

b) En que no se "informa" a los clientes, tanto de llamadas entrantes como salientes de que sus conversaciones pueden ser grabadas, y

c) De la "custodia " de las grabaciones por terceras empresas sin la custodis debida.

**III**

La LOPD en su artículo 4, recoge:

*" 5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.*

*No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados".*

Respecto de la cancelación de los datos de los clientes, PROSEGUR ha alegado en la inspección que los datos personales de los clientes se mantienen durante la relación contractual y durante los siguientes cinco años, tal y como se estipula en el

artículo 20 del, Reglamento de Seguridad Privada y que al finalizar la relación contractual durante un periodo de tiempo variable mantienen sus datos en la Base de Datos de Clientes accesibles a diferentes departamentos mientras duran las actividades de cierre de la relación contractual ( desinstalación del sistema de seguridad, entrega de llaves, verificación de cobros,…) y que una vez finalizadas se procede al "bloqueo" de los datos quedando accesibles únicamente para el Responsable de Seguridad y los Administradores de los Sistemas de Información de la compañía.

La inspección ha comprobado que los empleados de la entidad con acceso a los datos de los clientes utilizan una aplicación denominada "SIEBEL", salvo los empleados de la Central Receptora de Alarmas que utilizan otra aplicación denominada "MASTER MIND" de alta seguridad y solo se puede acceder a él desde las instalaciones de la Central Receptora. Se verifica que, utilizando la identificación y autenticación de un empleado del Departamento de Cobros con el perfil de "*usuario",* no consta información en la base de datos de clientes accesible a través de la aplicación SIEBEL de ninguno de los clientes cuyos datos han sido aportados por el denunciante y que utilizando la identificación y autenticación de un Administrador de los Sistemas de Información con el perfil de "*administrador"* se obtiene información de cuatro de los cinco clientes cuyos datos han sido aportados por el denunciante, de suerte que dos de ellos constan con fecha de alta y de baja (2012 y 2010) y en otros dos consta únicamente la fecha de alta y, aunque no figura la fecha de baja, los datos se encuentran bloqueados puesto que solo han sido localizados utilizando el perfil de acceso de *administrador* y respecto al cliente del que no se ha encontrado ninguna información fue dado de baja de la Compañía hace más de 6 años.

Por último, en relación con una impresión de pantalla aportada por la denunciante, donde figuran los datos personales de un cliente y que no coincide con la aplicación "SIEBEL", PROSEGUR manifiesta que esta impresión de pantalla corresponde a la aplicación de seguridad denominada "MASTER MIND" y los datos de éste cliente se encuentran actualmente bloqueados, tal y como se ha verificado al acceder a través de SIEBEL, si bien la inspeccionada señala que el documento aportado por la denunciante no consta la fecha en que se ha obtenido, por lo que, la pantalla mostrada por los inspectores corresponde a una impresión anterior a la fecha de baja del cliente en abril del 2012.

**IV**

En lo concerniente a la información a los clientes, tanto de llamadas entrantes como salientes de que sus conversaciones pueden ser grabadas, se verifica que todas las conversaciones telefónicas mantenidas con el Centro de Gestión de Clientes, que incluye a los operadores del Departamento de Recobro, son grabadas.

PROSEGUR tiene un protocolo de gestión de llamadas telefónicas a clientes que incluye grabación de la conversación telefónica e información sobre ello y sobre los derechos ARCO, de forma que en las llamadas entrantes el protocolo fue implementado en el momento de la creación del Centro de Gestión de Clientes, el cual opera con personal propio y se encuentra ubicado en las instalaciones donde se realiza la presente Inspección, y respecto de las llamadas salientes, el protocolo se implementó en el año 2010.

Añaden que, si la llamada es entrante a través del número 902******, una locución

automática informa de que se va a proceder a la grabación de la conversación como medida de seguridad y control de calidad e indica la forma de ejercer sus derechos ARCO y, si la llamada es entrante a un número diferente al indicado, generalmente números asignados al Departamento de Recobro, es el operador que atiende la llamada el encargado de informar sobre la grabación siguiendo un argumentario similar al de la locución automática y, en todos los casos, cuando la llamada es saliente es el operador que la efectúa el encargado de informar sobre la grabación.

Las conversaciones mantenidas en la Central Receptora de Alarmas también son grabadas siguiendo los criterios descritos.

En consecuencia, se verificó que, en la fecha de la Inspección realizada, y eligiendo grabaciones de llamadas a clientes al azar (llamadas salientes) el operador que efectúa la llamada informa de la grabación y de lo referente a los derechos ARCO. Y respecto de las grabaciones aportadas por el denunciante en las que el operador se identifica como empleado de PROSEGUR, la compañía manifiesta que las seis primeras grabaciones corresponden a llamadas salientes del Centro de Gestión de Clientes y la última de ellas de la Central Receptora de Alarmas, no obstante, al no figurar la fecha de la conversación no pueden indicar si las grabaciones son anteriores al año 2010 cuando se comenzó a informar en las llamadas salientes.

**V**

Respecto a la custodia de las grabaciones, PROSEGUR alegó que las grabaciones se encuentran accesibles, durante un mes, para los Coordinadores del Centro de Gestión de Clientes y una vez transcurrido este periodo el acceso se restringe al Responsable del mencionado Centro, al Departamento Jurídico y al Responsable de Seguridad hasta la baja de la relación contractual con el cliente al que corresponde la grabación y ,a partir de este momento, solo es accesible, durante tres años, por el Responsable de Seguridad.

Las grabaciones físicamente se custodian por la empresa BT ESPAÑA con la que tienen suscrito un contrato de prestación de servicios.

**VI**

Al Derecho Administrativo Sancionador, por su especialidad, le son de aplicación, con alguna matización pero sin excepciones, los principios inspiradores del orden penal, resultando clara la plena virtualidad del principio de presunción de inocencia.

En tal sentido, el Tribunal Constitucional, en Sentencia 76/1990 considera que el derecho a la presunción de inocencia comporta *"que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponda a quien acusa, sin que nadie esté obligado a probar su propia inocencia; y que cualquier insuficiencia en el resultado de las pruebas practicadas, libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio".* De acuerdo con este planteamiento, el artículo 130.1 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en lo sucesivo LRJPAC), establece que *"Sólo podrán ser sancionados por hechos constitutivos de infracción administrativa las*

*personas físicas y jurídicas que resulten responsables de los mismos aun a título de simple inobservancia."*

En consecuencia , los hechos denunciados se considera han quedado desvirtuados en las comprobaciones realizadas por la inspección en el establecimiento de PROSEGUR.

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 ***PROSEGUR ESPAÑA SL*** y a D.ª ***A.A.A..***

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.

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