- **Procedimiento Nº: E/01085/2020**

940-0419

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 26/12/2018, la directora de la Agencia Española de Protección de Datos (en adelante, AEPD o Agencia) acuerda iniciar actuaciones de investigación con base en el análisis de las reclamaciones recibidas y tramitadas con los números de referencia E/03484/2018, de fecha de entrada en esta AEPD el 4/6/2018 (reclamante 1) y E/06577/2018, de fecha de entrada en esta AEPD el 10/08/2018 (reclamante 2), contra la entidad SECURITAS DIRECT ESPAÑA, S.A., en adelante la investigada.

En ambas reclamaciones se manifiesta que:

1. El personal comercial de la investigada, durante la ejecución de acciones comerciales *"a puerta fría"*, recaba, en ocasiones, de las personas a las que visitan, datos personales de terceros que pudieran estar interesados en los servicios de la entidad.

2. Estos datos de terceros son utilizados para contactar y ofrecer los servicios de la investigada. Así, los reclamantes afirman haber recibido llamadas comerciales de la investigada al tiempo que niegan cualquier relación previa con la entidad. Declaran asimismo desconocer cómo se han obtenido sus datos de contacto y afirman no haber otorgado su consentimiento para acciones comerciales.

SEGUNDO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos objeto de la reclamación, teniendo conocimiento de los siguientes extremos:

(Se debe señalar que el presente expediente de referencia E/01085/2020 trae causa de la continuación de las investigaciones del expediente previo de referencia E/10418/2018).

ENTIDAD INVESTIGADA

- SECURITAS DIRECT ESPAÑA S.A. con NIF A26106013 y con domicilio en C/ Priégola 2, 28224 Pozuelo de Alarcón, Madrid.

ANTECEDENTES

Del análisis de dichos expedientes se pone de manifiesto lo siguiente:

1. El personal comercial de la investigada, durante la ejecución de acciones comerciales *"a puerta fría"*, recaba, en ocasiones, de las personas a las que visitan, datos personales de terceros que pudieran estar interesados en los servicios de la entidad.

2. Estos datos de terceros son utilizados para contactar y ofrecer los servicios de la investigada. Así, los reclamantes afirman haber recibido llamadas comerciales de la investigada al tiempo que niegan cualquier relación previa con la entidad. Declaran asimismo desconocer cómo se han obtenido sus datos de contacto y afirman no haber otorgado su consentimiento para acciones comerciales.

3. Estas llamadas comerciales son efectuadas a través de un *contact center* gestionado por un tercero que ejerce de encargado de tratamiento de la investigada para contactar a potenciales clientes.

4. La investigada reconoce los contactos señalados por los reclamantes en ambos expedientes.

5. Los clientes de la investigada tienen asociado un Plan de Acción *"de acuerdo con la normativa sectorial de seguridad privada"*. Forman parte de éste otras personas (además del titular-cliente) con las que se establecería comunicación en caso de que, ante un salto de alarma, no se pudiera contactar con el titular del servicio.

6. La investigada afirma hacer uso de listas internas de exclusión publicitaria, tanto de clientes como de potenciales clientes. Igualmente, manifiesta recibir periódicamente la lista de exclusión publicitaria gestionada por la Asociación Española de la Economía Digital (en adelante, ADigital o Robinson) reseñada en la sede electrónica de la AEPD.

Es objeto de este expediente la investigación de los procedimientos que la investigada sigue en relación con los tratamientos de datos personales que efectúa en el ámbito de la mercadotecnia directa a través de telefonía.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN.

El resultado de las actuaciones de investigación llevadas a cabo por el Servicio de Inspección de esta AEPD, se plasman a continuación con las debidas omisiones a fin de evitar la revelación de información que pueda afectar a la estrategia mercantil o técnica de la investigada. No obstante, el informe completo de las actuaciones de investigación se encuentra adjunto a la documentación del presente expediente.

El compendio de acciones realizadas es:

- El día 8 de enero de 2019, se remitió la primera solicitud de información a la investigada.

- El día 5 de febrero de 2019, la investigada registra respuesta a la solicitud de información anterior. El número de registro de entrada es 006084/2019 (en adelante, escrito 6084/2019).

- El día 20 de febrero de 2019, se incorpora al expediente, mediante diligencia, la descripción de la interacción del funcionario actuante con la página de internet de la investigada y el operador telefónico de la investigada en relación con el número de teléfono ***TELEF.1.

  El 20 de febrero de 2019 el funcionario actuante accedió al sitio de internet de la investigada (*www.securitasdirect.es*) e introdujo el número ***TELEF.1. Poco después se recibe una llamada en dicho número procedente del número de teléfono ***TELEF.2***. En la llamada le informan de que se habla en nombre de la investigada, ya que el número ha sido introducido a través del sitio de internet como interesado en los servicios de la compañía. El funcionario contesta que debe de tratarse de un error, a lo que el operador responde solicitando consentimiento para guardar su número de teléfono al objeto de mantenerle informado de futuras propuestas. El funcionario lo deniega.

  El audio de la conversación está incorporado al expediente.

- El día 21 de febrero de 2019, se incorpora al expediente mediante diligencia la información descrita en el apartado “antecedentes” relativa a los procedimientos previos de interés para el caso (E/03484/2018 y E/06577/2018).

- El día 25 de febrero de 2019, se incorpora al expediente mediante diligencia la descripción de la interacción del funcionario actuante con el apartado “Calcula Online” del sitio de internet de la investigada.

  El día 20 de febrero de 2019 el funcionario actuante accedió al sitio web de la investigada (www.securitasdirect.es) e hizo uso de la pestaña CALCULA ONLINE. Dicho servicio requiere rellenar teléfono, código postal e indicar el destino de la alarma es una vivienda o un negocio. El funcionario actuante introdujo el número ***TELEF.1. Poco después recibió una llamada del número de teléfono ***TELEF.3*** en nombre de la investigada. En la llamada le informan que el número había sido introducido a través del sitio de internet de la investigada como interesado en los servicios de la compañía. El funcionario contesta que debe de tratarse de un error, a lo que el operador responde solicitando consentimiento para guardar su número de teléfono al objeto de mantenerle informado de futuras propuestas. El funcionario lo deniega.

El audio de la conversación está incorporado en el presente expediente.

- El día 22 de marzo de 2019, se incorpora al expediente mediante diligencia la descripción de la interacción del funcionario actuante con el apartado “Programa Amigos” del sitio de internet de la investigada.

  El día 22 de marzo de 2019 el funcionario actuante accedió al “*Programa amigos”* dentro del sitio web de la investigada (https://www.securitasdirect.es/es/programa-amigos). Esta página anuncia la posibilidad, a los clientes de la investigada, de recibir un regalo por cada “*recomendación a amigos, familiares, conocidos, o si instalas una nueva alarma para ti*”. Además, contiene un enlace denominado “*ver protección de datos”* a la página que describe los términos relativos a la protección de datos personales en relación con el programa.

  Éste enlace informa de lo siguiente:

  <Dado que el CLIENTE facilita datos personales de terceros potenciales clientes, el CLIENTE, antes de dicha comunicación, deberá informar a dichos terceros sobre las finalidades de dicho tratamiento en los siguientes términos:

  (i) se contactará con el interesado a través de los medios facilitados para ofertarle productos y promociones de SECURITAS DIRECT en los que está interesado y con fines estadísticos. Las conversaciones llevadas a cabo podrán ser grabadas para poder acreditar que presta su consentimiento.

  (ii) sus datos personales serán objeto de un tratamiento automatizado y pasarán a formar parte de un fichero de SECURITAS DIRECT.

  (iii) podrá ejercitar los derechos de acceso, rectificación, cancelación, oposición, limitación y portabilidad reconocidos en la normativa vigente en materia de protección de datos de carácter personal dirigiéndose a SECURITAS DIRECT, en la siguiente dirección: SECURITAS DIRECT ESPAÑA, S.A.U., Calle Priégola, núm. 2, 28224 Pozuelo de Alarcón (Madrid) o a través del correo electrónico: dpo@securitasdirect.es. En todo caso, se procederá a la eliminación de los datos, de conformidad con las políticas de retención de datos que SECURITAS DIRECT tenga vigente en cada momento.

  Para cualquier cuestión o reclamación relacionada con el tratamiento de sus datos de carácter personal, deberá dirigirse en primera instancia al Delegado de Protección de Datos de SECURITAS DIRECT a través de la dirección de correo electrónico dpo@securitasdirect.es o por carta a la dirección que aparece previamente. En caso de que no vea satisfecha su reclamación, podrá dirigirse directamente a la autoridad de protección de datos que, para el caso que nos ocupa, será la Agencia Española de Protección de Datos (www.agpd.es).>

- El día 26 de septiembre de 2019, se incorpora al expediente mediante diligencia la información recopilada del servicio *Axesor* relativa a la investigada.

- El día 23 de octubre de 2019, se incorpora al expediente mediante diligencia la descripción de la interacción del funcionario actuante con el apartado *"Programa Amigos"* del sitio de internet de la investigada en relación con el número ***TELEF.4.

- El día 7 de noviembre de 2019, se finaliza la actuación inspectora presencial realizada en la sede central de la investigada cuyo acta y documentación forman parte del presente expediente (procedimiento de inspección E/10418/2018/I-01).

- El día 18 de noviembre de 2019, la investigada registra, con el número de registro de entrada 054548/2019, la documentación que había quedado requerida durante el procedimiento de inspección E/10418/2018/I-01 (en adelante, escrito 54548/2019).

- El día 4 de marzo de 2020 se remitió una solicitud de información a la investigada.

- El día 11 de junio de 2020 se recibe la contestación de la investigada al requerimiento anterior bajo el número de registro de entrada en la AEPD 019512/2020 (en adelante, 19512/2020).

A continuación, se detallan los procedimientos seguidos por la investigada en el contexto de la mercadotecnia directa telefónica. Toda la información aquí expuesta se basa en la información recogida en el marco de las acciones listadas anteriormente. Para facilitar su comprensión, se divide la exposición en los siguientes apartados:

1. Contexto

2. Procedimiento del área de ventas

3. Procedimiento del área de *marketing-captación*

4. Procedimiento del área de *marketing-cliente*

5. Volumen de datos personales almacenados

6. Proyectos de la investigada en marcha sobre sus tratamientos de datos personales

7. Auditorías de protección de datos

1. CONTEXTO

Las acciones comerciales telefónicas de la investigada pueden subdividirse en tres áreas en atención a sus particularidades: ventas, marketing-captación y marketing-cliente.

La nomenclatura interna utilizada por la investigada para referir a las distintas categorías de personas en función de su vínculo con la entidad es:

- Clientes. Personas que tienen suscrito un contrato en vigor con la compañía.
- Exclientes. Personas que tuvieron en el pasado un contrato, ya vencido, con la investigada.
- Miembros de los Planes de Acción de los clientes y exclientes.
- *"Prospectos"*.
    - Para el departamento de ventas, personas que han recibido una oferta comercial personalizada.
    - Para el departamento de marketing-captación, personas que han aceptado una visita comercial.
- *"Leads"*, "*preprospectos"* o potenciales clientes:
    - Personas que se han mostrado interesadas (ya sea a través del sitio de internet de la investigada, enlaces a la investigada desde otros sitios web, teléfono o de un agente comercial).
    - Personas cuyos datos han sido referidos por otros, clientes o potenciales clientes (a través del sitio de internet de la investigada o de un agente comercial).

La investigada cuenta con dos Centros de Proceso de Datos (CPDs) propios situados en España, uno activo y otro de respaldo, en los que se alojan los datos que gestionan sus sistemas. Además, tiene contratado un servicio de *hosting* para el alojamiento de la capa de presentación.

2. PROCEDIMIENTO DEL ÁREA DE VENTAS

En el proceso de venta *"a puerta fría"*, la investigada facilita a su fuerza de ventas una aplicación llamada *ForceManager* que éstos tienen embebida en los teléfonos móviles

y/o tabletas digitales que la investigada pone a su disposición para el desempeño de sus funciones.

ForceManager requiere la introducción de usuario y contraseña de acceso. Una vez dentro de la aplicación, a través de la opción de menú “Venta Directa”, se puede dar de alta a un potencial cliente. El primer dato que se solicita del potencial cliente es su número de teléfono. Éste se valida en los sistemas de la investigada en busca de los antecedentes que pudiera haber relacionados con él (si los hubiera se muestran en pantalla). A continuación, la aplicación permite rellenar los campos siguientes:

- Origen, de carácter obligatorio, es un campo tabulado con los siguientes valores (las iniciales RP son de “Recurso Propio”):

    - *CALL RP – Referidos*: dato de un tercero facilitado por otro cliente o potencial cliente en una visita comercial.

      Cuando se rellena el campo origen con este valor desaparece la posibilidad de rellenar los campos de dirección, nombre y apellidos.
    - *CALL RP – Contacto*: el comercial ha hablado con el potencial cliente, pero no ha vendido el servicio ni ha agendado una visita posterior.

      Cuando se rellena el campo origen con este valor desaparece la posibilidad de rellenar los campos de dirección, nombre y apellidos.
    - *CALL RP – Visita Concertada*: el comercial tiene una visita agendada con el potencial cliente.

    - *CALL RP – Visita Argumentada No Vendida*: el comercial realiza la visita, pero no se ha culminado con venta.

    - *Prospecto RP*: corresponde con un potencial cliente que ha recibido una oferta comercial personalizada.

  La incorporación del valor *CALL RP – Referidos* se produjo en agosto de 2018. Antes de esa fecha los datos de terceros referidos por clientes o potenciales clientes se introducían en la base de datos con otro origen. De esta forma no hay manera de identificar los potenciales clientes referidos en la base de datos con anterioridad a agosto de 2018.
- Tipo de Instalación, cuyos posibles valores son: chalet individual; chalet adosado; chalet pareado; oficinas; piso; tienda; industrial; bar, restaurante; comunidad de propietarios; caseta de obra; oficina en altura.

- Nombre Empresa

- Nombre, Primer apellido, Segundo apellido

- Dirección: dispone de un sistema de validación automática con el catastro.

- Gran cuenta, cuyos posibles valores son "*SÍ"* o "*NO"*.

- Recurso, de carácter obligatorio, es un campo tabulado con los siguientes posibles valores:

    - RPSTD: Recurso Propio Estándar. El potencial cliente ha sido "captado" por un comercial (sea cual sea el valor del campo origen)

    - RPPR: Recurso Propio de Prescriptor. El potencial cliente ha sido introducido por el comercial en el *ForceManager*, si bien la fuente es un Colaborador de la investigada.

      Los colaboradores son autónomos o empresas que mantienen un contrato con la investigada por el cual facilitan periódicamente datos de potenciales clientes a un agente comercial que tienen asignado como enlace con la investigada. El agente comercial una vez recibe los datos del colaborador los introduce en el sistema de la investigada a través de *ForceManager*. La selección de colaborador se realiza con base en la relación de su actividad con la investigada (inmobiliarias, cerrajerías, fontanerías, etc.).

      El documento *E_10418_2018_I01_DOC4*, contiene, a modo de ejemplo, varios acuerdos suscritos por la investigada con colaboradores (más adelante se amplía la información al respecto).

    - RPPA: Recurso Propio de "*Programa de Amigos"*. El potencial cliente ha sido introducido por el comercial en el *ForceManager* si bien la fuente es otro cliente.

- Cliente original (dato a rellenar para el caso de recurso del tipo RPPA, especifica el código del cliente que recomienda el contacto).

- Producto, cuyos posibles valores son: sistema de alarma; cámaras.

- Tipo de Venta, cuyos posibles valores son: Normal; *Renove*; RBE. Recuperación de cliente de baja; RBE *Upgrade*. Recuperación de cliente de baja con actualización de equipo; CMC. Conexión en memoria de calidades (cliente de plataforma); CMC Upgrade. Conexión en memoria de calidad con actualización de equipo (clientes de plataforma); Equipo compatible. Conexión

de una alarma compatible con Securitas Direct; Rescate. Cliente que se recupera de una baja en menos de un año.

En el escrito 6084/2019, la investigada señala que no se recaban datos personales propiamente dichos dado que, por un lado, la dirección postal se recoge sin número, piso y/o letra asociado (esta información sirve para tener constancia de la zona donde reside el potencial cliente) y, por otro, el número de teléfono de contacto generalmente es el número de teléfono móvil. Durante la inspección E/10418/2018/I-01 se aclara que, en el caso de clientes cuyo origen es *Referido* o *Contacto* no se introducen nombre, apellidos, ni dirección; si la tipología de potencial cliente es otra sí existe la posibilidad de rellenar estos campos, incluida la dirección completa. Con respecto al número de teléfono, si el número introducido en *ForceManager* corresponde al sistema de numeración de telefonía fija, el único origen elegible es *Prospecto RP*. Esto se traduce en que no podrían captarse números de telefonía fija de otro tipo de potenciales clientes. El motivo que la investigada manifiesta es doble: la investigada considera, basándose en la jurisprudencia, que el número de teléfono fijo sí es un dato personal (a diferencia del número de teléfono móvil), y el *contact center* externo únicamente realiza llamadas a números de teléfono móviles.

Los datos introducidos a través de la aplicación *ForceManager* se insertan en una base de datos de la investigada denominada *CRM41*, contenedora de la información de los potenciales clientes y de los consentimientos facilitados.

Los documentos *E_10418_2018_I01_DOC15* y *E_10418_2018_I01_DOC16* facilitados en el marco de la inspección E/10418/2018/I-01 incluyen el modelo de datos almacenado por la investigada en relación con los potenciales clientes y sus consentimientos.

La inserción de cada nuevo potencial cliente en *CRM41* provoca una llamada al procedimiento *create_lead* de un servicio web publicado por la empresa proveedora del *contact center* externo. Con ello, los datos del potencial cliente son trasladados a los sistemas del *contact center* externo y gestionados en los mismos por el proveedor del servicio. Alternativamente, en caso de que la comunicación a través del servicio web falle, la información se traslada manualmente a través de la aplicación *myfiles*.

En el Documento E_10418_2018_I01_DOC6 facilitado en el marco de la inspección E/10418/2018/I-01 se incluye la correspondiente a la definición de los servicios web utilizados por la investigada y la entidad Atento (más adelante se detalla su participación) para el intercambio de información.

En el escrito 6084/2019, la investigada manifiesta que "*cuando se recibe un número de teléfono de un potencial cliente interesado en el servicio, la política de la compañía es contactar con dicho número para confirmar tal interés o no sin perjuicio de que se encuentre incluido en una lista robinson (interna o externa). Si, como consecuencia de esa primera llamada en la que se confirma el posible interés, ese potencial cliente solicita la inclusión de su número de teléfono en la lista robinson interna (aunque esté ya en la externa), además de cumplir con su petición, es en las campañas salientes de*

llamadas a potenciales clientes cuando se pasan estos filtros, tanto la lista interna como la externa, para evitar la inclusión de personas que se han opuesto a esos contactos garantizando así que ese número no es vuelto a contactar (salvo que entrase de nuevo como potencial cliente interesado en cuyo caso, esa primera llamada no afecta a que siga estando en la lista robinson interna o externa)".

No obstante lo anterior, en el contexto del procedimiento de inspección E/10418/2018/I-01, la investigada señala que el proveedor del *contact center* externo actual, antes de ejecutar la llamada, cruzaría el dato del potencial cliente recibido con una lista de exclusión publicitaria que la investigada le facilita, de forma que no se contacte con los números ahí inscritos (ver documento *E_10418_2018_I01_DOC7*). Esta lista (en adelante, *ListaExclConsolidada*) es un compendio de:

- Última lista de exclusión publicitaria descargada de ADigital. Según manifiesta la investigada en el escrito 6084/2019, la lista se descarga con una periodicidad de 2-3 meses.

- Lista de potenciales clientes que han manifestado su negativa a la investigada a recibir comunicaciones comerciales.

- Lista de potenciales clientes que han ejecutado su derecho de oposición al tratamiento de sus datos con fines comerciales.

  El filtrado descrito, según señalan, se realiza en todo caso, sea el potencial cliente referido o no.

  Los ficheros que se envían al *contact center externo* para realizar la exclusión son dos:

- De forma automática a través de SFTP (protocolo para el envío de ficheros de forma segura) y otro fichero que contiene los números de teléfono de potenciales clientes que dan su negativa al consentimiento para comunicaciones comerciales.

- De forma manual a través de la aplicación *myfiles* se envía el fichero *Robinson_SDE_actualizaciones_ayer (CON TODO)*, que contiene los números de teléfono descargados de ADigital y los de las personas que han ejercido el derecho de oposición.

El servicio de *contact center* externo para el departamento de ventas lo proveyó, desde septiembre de 2017 hasta junio de 2019, ALPHABET GLOBAL, S.L., (en adelante, Alphabet). Tras la resolución del contrato con Alphabet, el proveedor pasó a ser ATENTO TELESERVICIOS ESPAÑA S.A.U (en adelante, Atento). La rúbrica del contrato por el cual Atento asume este servicio está, a día 7 de noviembre de 2019, pendiente. No obstante, como parte del *E_10418_2018_I01_DOC3* se encuentra una copia de la redacción del mismo fechada a 11 de junio de 2019 que tiene forma de

adenda sobre un contrato preexistente. La cláusula cuarta de éste especifica que el "*volumen de registros a contactar con carácter mensual será de xxxxxxxx, permitiéndose una desviación de dicho volumen de hasta un máximo del 10% con carácter mensual. El TMO (Tiempo Medio Operativo) deberá ser de x minutos".*

Se ha facilitado a la AEPD una copia del certificado de entrega a la investigada de la información propiedad de la investigada de la que disponía Alphabet firmado a fecha 4 de septiembre de 2019 (documento *E_10418_2018_I01_DOC1*).

Recogidos los datos del potencial cliente y hecho el filtrado, el *contact center* externo trata de establecer contacto telefónico. La primera llamada se ejecuta de forma prácticamente instantánea tras la introducción del número de teléfono en la base de datos (según manifiesta la investigada, se hacen uso de sistemas de marcación automática). Según indican, el objeto de estas llamadas es, bien concertar una visita comercial con el potencial cliente, bien confirmar una cita ya agendada. En el caso de potenciales clientes cuyo origen sea *CALL RP – Referidos* o *CALL RP - Contactos* en esta llamada además se recaban los datos personales restantes (nombre, apellidos, dirección completa) que permitan efectuar la visita.

Además, la captura del consentimiento no se lleva a cabo en la interacción con el agente comercial sino en la llamada telefónica que realiza el *contact center* tras la introducción de los datos. Al agente comercial, tras concluir la inserción de los datos, *ForceManager* le muestra una pantalla en la que le informa de la necesidad de informar al interlocutor de la finalidad del tratamiento y del responsable del mismo.

La traslación del consentimiento a los sistemas de la investigada se ejecuta de la siguiente forma. El operador telefónico de Atento (antes Alphabet) recoge el valor del consentimiento en sus sistemas y éstos lo trasladan a los de la investigada a través de una llamada a un servicio web publicado por la investigada. El campo que se actualiza en la tabla de consentimientos de *CRM41* se denomina *CONSENTVALUE*. El consentimiento puede ser afirmativo (*CONSENTVALUE* igual a <uno>), negativo (*CONSENTVALUE* igual a <cero>), o no figurar registro (según indica la investigada, ocurre tanto cuando no se ha podido establecer contacto con el número de teléfono como cuando el interlocutor manifiesta durante la llamada que ha habido algún error ya que él no ha facilitado su número a la investigada).

Según manifiesta la investigada, las directrices sobre la gestión de la ausencia de consentimiento para el tratamiento de los datos personales con fines comerciales del potencial cliente son las siguientes:

- Si el potencial cliente acepta la realización de una visita comercial, pero deniega el consentimiento para futuras acciones comerciales, sus datos (nombre, apellidos, dirección completa, además de teléfono) permanecen en la base de datos hasta tres días después de la fecha de la visita. Pasado ese tiempo se ofuscan -a excepción del número de teléfono- (ver documento *E_10418_2018_I01_DOC8*).

La ofuscación consiste en la inserción del valor *ROBINSON* en los campos *nombre, apellido1, apellido2, numvia, restovia,* de forma que se sobrescribe lo que hubiera previamente.

- Para los casos en que el potencial cliente no acepta la visita de un comercial y deniega el consentimiento para la realización de comunicaciones comerciales futuras (sea o no referido), hasta el mes de noviembre de 2019 no había nada programado.

  Manifiestan que está en proyecto la ofuscación automática de los datos (a excepción del número de teléfono) pasados treinta días. Según indican este cambio ya estaría desarrollado en los sistemas de Atento aunque de esta investigación no se ha advertido constancia de la planificación ni implantación de este requisito. Sí existe, sin embargo, en el documento *E_10418_2018_I01_DOC17, Análisis Funcional – Casos de Uso. GDPR – Captación y Ventas Versión 1.1,* un apartado (3.4.1) que especifica como requisito para el *contact center* de ventas que la negativa al consentimiento desencadenará dos acciones: el envío de un correo electrónico a la dirección *lopd.marketing@securitasdirect.es* para la inclusión manual del teléfono en la lista de exclusión publicitaria; y la ofuscación de los datos del *preprospecto* en *CRM41.*

- Para los casos en que no se consigue contactar con el potencial cliente o éste manifiesta que ha habido un error (no existe registro de consentimiento) hasta el mes de noviembre de 2019 no había nada programado. Manifiestan que está en proyecto la ofuscación automática de los datos (a excepción del número de teléfono) pasados treinta días. Según indican este cambio ya estaría desarrollado en los sistemas de Atento, aunque de esta investigación no se ha advertido constancia de la planificación ni implantación de este requisito concreto. Sí figura, sin embargo, en el documento *E_10418_2018_I01_DOC17, Análisis Funcional – Casos de Uso. GDPR – Captación y Ventas Versión 1.1,* un apartado (3.8.1) que refiere el caso de uso relativo al proceso de ofuscación de información de *preprospectos* y *prospectos*. Describe el caso especificando que "*se ofuscará (ocultará) la información personal de los preprospectos y prospectos de los que no se tenga el consentimiento de comunicaciones comerciales que hayan sido creados antes de X días (parametrizable en el SSIS)".*

El ejercicio del derecho de oposición de potenciales clientes (así como de clientes y exclientes) no provoca cambios en el valor del campo *CONSENTVALUE* de *CRM41*, sino que se gestionan de manera independiente a través de una base de datos desarrollada sobre la tecnología *Microsoft Access*.

Como se ha comentado anteriormente, la actualización por parte de los operadores de Atento de los datos asociados al potencial cliente (cambio de estado, introducción de

datos personales, actualización del consentimiento) provoca a su vez una llamada a los servicios web publicados por la investigada de forma que la información se actualiza al momento en la base de datos *CRM41*. Según señala la investigada, las llamadas a los servicios web se realizan de forma segura (autenticada, autorizada, y cifrada).

Los operadores telefónicos de Atento (y antes de Alphabet) utilizan dos argumentarios (ver documento *E_10418_2018_I01_DOC9* facilitado en el marco de la inspección E/10418/2018/I-01), dependiendo del caso:

- *Argumentario Confirmación Leads*. Se utiliza cuando el origen del contacto es *CALL RP – Referidos* o *CALL RP – Contacto* con el objetivo de fijar una visita comercial y obtener el consentimiento para el tratamiento de los datos personales con fines comerciales.

- *Argumentario Visita Concertada*. Se utiliza cuando el origen del contacto es *CALL RP – Visita Concertada* con el objetivo de confirmar una visita comercial agendada y obtener el consentimiento para el tratamiento de los datos personales con fines comerciales.

Los argumentarios anteriores incluyen el siguiente texto sobre la finalidad de los tratamientos de los datos personales recogidos:

Don XXX, para garantizarle un correcto tratamiento de sus datos personales que usted nos ha facilitado, queremos informarle de que éstos serán incluidos en un fichero de Securitas Direct, y los trataremos con el fin de informarle de promociones comerciales que puedan ser de su interés en el ámbito de la seguridad privada, así como realizar evaluaciones de riesgos que son necesarias para poder realizarle las mejores propuestas comerciales.

¿Está UD conforme?

Además, le informamos de que se podrán tratar sus datos de forma anónima con fines estadísticos y, en todo caso, podrá ejercer sus derechos de protección de datos dirigiéndose al delegado de protección de datos de Securitas Direct en la dirección: dpo@securitasdirect.es o podrá acudir a la Agencia Española de Protección de Datos para realizar cualquier tipo de gestión en relación con sus datos.

Sobre la finalidad de "*realizar evaluaciones de riesgos"*, la investigada manifiesta que se trata de riesgos económicos (*scoring*) que sirven para adaptar la oferta a las características singulares del potencial cliente. Añaden que, como parte de este tratamiento, se consultan ficheros de solvencia patrimonial y de crédito.

Como parte del escrito 6084/2019, la investigada facilitó un tercer argumentario, el *Argumentario Referidos Plan Acción*. Según aclara durante el procedimiento de inspección E/10418/2018/I-01, éste se utilizaba para hacer una llamada informativa a los miembros de los planes de acción, si bien dicha llamada actualmente no se ejecuta.

Las llamadas del *contact center* externo se graban y auditan con base en distintos parámetros (KPIs), que incluyen si se ha realizado correctamente o no la parte del argumentario correspondiente a la protección de datos personales. La auditoría la realiza semanalmente la propia empresa que ejerce el servicio de *contact center* (Atento, actualmente) bajo las directrices de la investigada. Para ello, toman una muestra del total de las llamadas, que analizan y valoran según distintos parámetros. El parámetro relativo a la protección de datos tiene un umbral crítico bajo el cual se podrían tomar medidas correctoras o, en su caso, disciplinarias. Realizada la auditoría se comunican los resultados a cada operador implicado y, en su caso, se elabora un plan de acción personalizado. El documento *E_10418_2018_I01_DOC10* facilitado en el marco de la inspección E/10418/2018/I-01 contiene información de ejemplo del registro que hace Atento de estas auditorías.

El departamento de ventas no realiza otro tipo de actuaciones telefónicas de tipo "campaña comercial" ("barrido" de una base de datos en un período temporal concreto). No constan, por tanto, documentos del tipo *"Anexo de Campaña"* descrito en el *Acuerdo Marco para la Prestación de Servicios* suscrito entre la investigada y Alphabet el 7 de septiembre de 2017 (facilitado a la AEPD como parte del escrito 6084/2019).

Se realiza, en el marco de la inspección E/10418/2018/I-01, la inserción a través de *ForceManager* del número ***TELEF.5*.* Se recoge la siguiente información de esta prueba en los documentos *E_10418_2018_I01_DOC5* y *E_10418_2018_I01_DOC20*:

- Interacción realizada sobre *ForceManager* en la que se observan los campos descritos anteriormente, y la introducción del número ***TELEF.5.

- Evidencias de existencia en *CRM41* de registros asignados al número ***TELEF.5. Entre los datos asociados consta la fecha de inserción, 9 de octubre a las 12:02, y el origen, *CALL RP - Referidos*.

- Información de la *cabecera WSDL* del método *create_lead* del servicio web de Atento al que se llama para transferir los datos del potencial cliente desde los sistemas de la investigada hasta los de Atento.

- Registro de la tabla de *CRM41* en que se guarda el resultado de la llamada al servicio web de Atento, con resultado *OK*.

- Impresión de pantalla de la recepción de la llamada el día 9 de octubre a las 12:06 en nombre de la investigada. En la llamada se informa a la investigada de que el alta del número ha debido de tratarse de un error.

- Resultado del valor del consentimiento para dicho contacto. No figura registro ni positivo ni negativo. Según manifiesta el personal de la investigada se debe

a que no se ha contestado ni una cosa ni otra, sino simplemente se ha indicado que la llamada era errónea.

La investigada facilita información adicional sobre la figura del colaborador (se extrae del Documento *E_10418_2018_I01_DOC4* facilitado en el marco de la inspección E/10418/2018/I-01):

Se entiende por COLABORADOR a efectos del presente Acuerdo, la persona física o jurídica (incluyendo empresarios individuales), mayores de edad, que a cambio del percibo de una comisión, realiza a favor de SECURITAS DIRECT la actividad de prescripción de los sistemas de alarma de SECURITAS DIRECT en los términos establecidos en este Acuerdo. El COLABORADOR queda obligado a recabar y entregar los datos de los potenciales clientes interesados a SECURITAS DIRECT.

(…) Obligaciones del COLABORADOR

- *Informar a los Potenciales Clientes sobre los productos y servicios de SECURITAS DIRECT.*

- *Cumplir con todos los principios recogidos en el Código de Conducta de SECURITAS DIRECT, el cual estará disponible para su lectura en la web de SECURITAS DIRECT, www.securitasdirect.es, haciéndolo extensible a todos sus empleados, contratistas, subcontratistas que desarrollen alguna actividad para SECURITAS DIRECT en el marco del presente Acuerdo.*

- *Facilitar a SECURITAS DIRECT los datos de contacto que se indican en la Estipulación OCTAVA del presente Acuerdo sólo de aquellos Potenciales Clientes que hayan dado su autorización al COLABORADOR para que, en nombre y por cuenta de SECURITAS DIRECT, éste facilite sus datos a SECURITAS DIRECT con el fin de que SECURITAS DIRECT pueda contactarles con el fin de concertar una visita con los Potenciales Clientes.*

- *El COLABORADOR no podrá realizar llamadas salientes ni de carácter informativo, ni comercial sobre productos y servicios de SECURITAS DIRECT a los Potenciales Clientes.*

8. PROTECCIÓN DE DATOS PERSONALES

El COLABORADOR recabará, en nombre y por cuenta de SECURITAS DIRECT, los siguientes datos relacionados con los Potenciales Clientes (nombre y número de teléfono móvil y/o fijo). Asimismo, en el momento de la recogida de datos, el COLABORADOR deberá informar a los Potenciales Clientes que SECURITAS DIRECT tratará ese dato con la única finalidad de contactar con él para recabar información complementaria del Potenciales Clientes, cumplir con las obligaciones en materia de protección de datos de carácter personal que correspondan, ofrecerle productos y servicios de SECURITAS DIRECT y concertar una visita.

Los datos de los Potenciales Clientes que enviará EL COLABORADOR a SECURITAS DIRECT, de acuerdo con lo establecido en el párrafo anterior, se hará a través del correo electrónico colaboradores@securitasdirect.es. Con carácter mensual, SECURITAS DIRECT comunicará al COLABORADOR, por esta misma vía, las prescripciones del COLABORADOR que finalmente se han convertido en clientes finales de SECURITAS DIRECT, indicando únicamente el nombre y el número de teléfono y/o fijo.

El COLABORADOR garantiza que los datos recabados en nombre y por cuenta de SECURITAS DIRECT han sido facilitados por el propio interesado en contratar los productos y servicios de SECURITAS DIRECT y estos son veraces y exactos.

En virtud de lo anterior, el COLABORADOR actuará como encargado del tratamiento de los datos que recabe en nombre y por cuenta de SECURITAS DIRECT, debiendo ser tratados por el COLABORADOR únicamente para cumplir con sus obligaciones como COLABORADOR y no podrá destinar los datos recabados de los Potenciales Clientes a otro fin distinto que no sea la prescripción de productos y servicios de SECURITAS DIRECT. Los datos recabados en nombre y por cuenta de SECURITAS DIRECT podrá ser conservados por parta del COLABORADOR únicamente durante el tiempo que dure su relación contractual y las partes deban liquidarse cualesquiera cantidades pendientes derivadas de la prestación del Servicio. Una vez que todas las cantidades estén limitadas, el COLABORADOR deberá destruir los datos que hubiera conservado en cumplimiento de tal circunstancia.

Asimismo, el COLABORADOR no podrá facilitar los datos recabados a ningún otro tercero distinto a SECURITAS DIRECT y del mismo modo no podrá explotarlos ni obtener ningún beneficio económico de los mismos más allá de lo previsto en el presente Acuerdo. (…)

1. PROCEDIMIENTO DEL ÁREA DE *MARKETING-CAPTACIÓN*

El área de *marketing-captación*, a través de un *contact center* propio, emite llamadas a potenciales clientes cuyos datos han sido introducidos a través del sitio de internet de la investigada. Asimismo, contesta a las llamadas entrantes que se reciben en los números de teléfono habilitados para potenciales clientes (el análisis del procedimiento ejecutado durante las llamadas entrantes no es objeto de este informe).

El origen de los números de teléfono a los que se realizan llamadas salientes es, en todo caso, el sitio de internet de la investigada. Éste cuenta con varias páginas de internet distintas *(landing pages)* en las cuales una persona puede introducir un número de teléfono para ser contactado. Dispone, además, de una página de internet dedicada al llamado *Programa Amigo*, en el cual un cliente puede facilitar los datos de un tercero al objeto de, cumplidas unas condiciones, obtener una recompensa. Según indica la investigada, este plan se creó en 2013 y durante los dos primeros años se impulsó enviando correos electrónicos informativos a los clientes. En el escrito 19512/2020 registrado de entrada en la AEPD el pasado 11 de junio de 2020, la investigada actualiza la información con respecto a este programa señalando que la sección que referenciaba a este programa dentro del sitio de internet de la investigada

fue suprimida el pasado 3 de febrero de 2020. Se constata que, a 2 de julio de 2020, al tratar de acceder a la página de internet correspondiente al *Programa Amigos* de la investigada se produce una redirección al *home* de la investigada (ver diligencia al respecto).

La información que se introduce a través de internet incluye, en todo caso, el número de teléfono (fijo o móvil) del potencial cliente. Además, dependiendo de la *landing page* concreta, pueden solicitarse datos adicionales, bien referidos a las particularidades del inmueble en el que instalar la alarma (incluyendo el código postal pero no la dirección completa), bien datos sobre el potencial cliente como su nombre y, en el caso del *Programa Amigo* (hasta su supresión el pasado 3 de febrero de 2020), el número de teléfono del cliente de la investigada que lo recomienda.

Estos datos se almacenan automáticamente en una aplicación informática comercial de telemarketing denominada *Altitude* que utiliza el *contact center* interno para desarrollar su labor. Una vez recogidos los datos del potencial cliente, se realiza la primera llamada de contacto de forma "inmediata". El objetivo de esta llamada es agendar una visita comercial. Además, durante la misma, se recoge el consentimiento del interlocutor para tratar sus datos personales.

El documento *E_10418_2018_I01_DOC12* facilitado en el marco de la inspección E/10418/2018/I-01 contiene los argumentarios utilizados por el *contact center* interno de *marketing-captación* en su relación con los potenciales clientes.

El primero de ellos, denominado *SPEECH TELEVENTA,* se utiliza para llamar a clientes (para una segunda instalación) o potenciales clientes que tiempo atrás solicitaron información a la investigada al objeto de sondear nuevamente su interés. Contiene, entre otros, los siguientes párrafos:

- *(NOMBRE POTENCIAL) por su seguridad, vamos a guardar el teléfono para mantenerle informado de futuras propuestas que puedan ser de su interés ¿está de acuerdo?*

  Si dice que sí:

  Finalmente, queremos informarle que podrá ejercitar sus derechos de protección de datos a través de la dirección dpo@securitasdirect.es o acudir a la Agencia Española de Protección de Datos.

- *(Si no tiene ningún otro lugar sin proteger, le daremos la opción de que nos proporcione un referido)*

  En cualquier caso, es una propuesta excepcional, por lo que sería interesante que se lo ofreciera a algún familiar cercano, obviamente tiene que ser alguien que Vd. quiera cederle esta propuesta, porque es solo para clientes, tendría que ser un hijo, hermano, o un amigo pero que sea muy cercano para Vd.)

  Facilíteme su teléfono para poder darle toda la información.

En el contexto del procedimiento de inspección E/10418/2018/I-01 ha podido observarse que, en el sistema *Altitude* se pueden consignar, entre otros, los siguientes datos durante esta primera interacción:

- Consentimiento: cuyas opciones son tres:

    1. sin consentimiento;

    2. consentimiento para una próxima interacción (este valor estaría pensado para la interacción en la visita comercial agendada);

    3. consentimiento para futuras interacciones (este valor estaría pensado para el tratamiento del dato, además de en la visita comercial agendada, en futuras acciones comerciales de la compañía).

- Consentimiento *WhatsApp*: si es positivo se podría utilizar por el comercial para contactar a través de esta vía con el potencial cliente para confirmar una visita agendada (en la práctica, según señala la investigada, no se está utilizando).

- *Robinson:* el operador lo marcará a petición del interesado. Ello provoca que el número de teléfono entrante se introduzca en una lista de exclusión que gestiona directamente *Altitude*.

- *BlackList:* se marca cuando se considera que el número es erróneo (bromas, descalificaciones, errores, etc.) para no atender ni emitir llamadas a esos números. La gestión de los números que se introducen en esta “lista negra” es interna de *Altitude*.

- Género de la persona.

- Código postal.

El *contact center* interno no realiza cruce con la lista de exclusión publicitaria especificada anteriormente (*ListaExclConsolidada*). Sí excluye de sus llamadas los números que se hayan marcado como *Robinson* y *Blacklist* en el propio *Altitude*.

Según manifiesta la investigada, para trasladar los números marcados *Robinson* en *Altitude* a la *ListaExclConsolidada,* el operador telefónico debe rellenar un formulario que manualmente un equipo de *backoffice* gestiona. Según avanzan, ahora mismo hay un proyecto en marcha de automatización para que se genere directamente desde *Altitude* la inserción en la lista de exclusión (evitando la gestión manual).

Durante este primer contacto se recaba el consentimiento del potencial cliente. Como se ha visto, los posibles valores que *Altitude* permite anotar son:

- Sin Consentimiento: genera un registro asociado al número de teléfono en la tabla de consentimientos de *CRM41* con valor <cero> en el campo *CONSENTVALUE* (señalando que el interesado no da su consentimiento) y valor <uno> en el campo *IDCONSENTTYPE* (indicación de consentimiento para la realización de comunicaciones comerciales).

- Consentimiento para una próxima interacción: genera un registro asociado al número de teléfono marcado en la tabla de consentimientos de *CRM41* con valor <uno> en el campo *CONSENTVALUE* (señalando que el interesado sí da su consentimiento) y <tres> en el *IDCONSENTTYPE* (indicación de consentimiento para el tratamiento de sus datos con la finalidad de realizar la visita comercial acordada).

- Consentimiento para futuras interacciones: genera un registro con valor <uno> tanto en el campo *CONSENTVALUE* como en el *IDCONSENTTYPE* asociados a ese número de teléfono.

- Si no se consigue contactar no se genera registro en la tabla de consentimientos de *CRM41* (caso del número ***TELEF.6).

Si el interesado manifiesta interés en la visita de un comercial, el operador telefónico, a través de la opción de *Altitude, Crear Prospecto,* introducirá, entre otros, los siguientes datos: teléfono, nombre, apellidos, dirección completa (en este caso la validación se realiza con un servicio de *Google*).

El documento *E_10418_2018_I01_DOC11* facilitado en el marco de la inspección E/10418/2018/I-01 recoge las impresiones de pantalla de una interacción con *Altitude* que incluye la ventana de creación de un *Prospecto*.

En cuanto al almacenamiento de los datos recogidos, la gestión es la siguiente:

- Si en *Altitude* no se llega a crear el *prospecto,* es decir, la conversación no concluye con la concertación de una visita comercial, los datos que se recaban, a excepción de los relativos a la gestión del consentimiento (incluyendo número de teléfono), no se vuelcan a *CRM41*. Quedarían en *Altitude* por tanto el número de teléfono y, en su caso (si el operador ha llegado a preguntarlo y el interlocutor a facilitarlos) el género, y el código postal del interesado. Podrían quedar datos adicionales si se genera el prospecto y se rellenan determinados datos pero no se termina de agendar la cita comercial porque el interlocutor desistiera por el camino.

- Si en *Altitude* se genera el *prospecto* se vuelcan a *CRM41* los datos recogidos (que incluyen nombre, apellidos, dirección completa y valor de origen *Prospecto*, además del teléfono) incluyendo la gestión del consentimiento. En *CRM41* estos datos están sujetos a la política general de ofuscación vista en el

apartado anterior. Con posterioridad el agente comercial asignado para la visita comercial gestionara esta información a través de *ForceManager.*

En relación con el proyecto de ofuscación de los datos gestionados en *Altitude*, el documento *E_10418_2018_I01_DOC17, Análisis Funcional – Casos de Uso. GDPR – Captación y Ventas Versión 1.1* de fecha 6 de marzo de 2018 facilitado en el marco de la inspección E/10418/2018/I-01, dispone de un apartado (3.6) titulado *Altitude*, si bien se encuentra vacío.

Se realizan, en el marco de la inspección E/10418/2018/I-01, consultas a los sistemas de la investigada en relación con el número ***TELEF.1, introducido previamente a través del sitio web de la investigada y sobre el que, en la llamada recibida, se indica que debe ser un error y se niega el consentimiento para el tratamiento de los datos personales con fines comerciales. En el documento que refleja estas consultas, Documento *E_10418_2018_I01_DOC21* facilitado en el marco de la inspección E/10418/2018/I-01*,* consta:

- Consulta de la tabla de consentimientos, en la que figura un único registro que consigna la negativa al consentimiento (CONSENTVALUE tiene valor “0”) con fines comerciales (IDCONSENTTYPE tiene valor “1”) y la fecha en la que se recogió el dato (20 de febrero de 2019).

- Búsqueda del número en la lista de exclusión que se facilita a Atento (se encuentra el ***TELEF.1)

Se realizan, en el marco de la inspección E/10418/2018/I-01, consultas a los sistemas de la investigada para consulta de la situación del número ***TELEF.6 (número introducido previamente a través del sitio web de la investigada y en el que se han recibido llamadas que no han sido contestadas). El documento que refleja estas consultas, Documento *E_10418_2018_I01_DOC22* facilitado en el marco de la inspección E/10418/2018/I-01*,* contiene:

- Búsqueda del consentimiento asociado al número en la tabla de consentimientos. No existen registros.

- Impresión de pantalla de la información en *Altitude* relativa a dicho número. Dos intentos de llamada realizados el día 2 de octubre de 2019 sin contestar y otra, ese mismo día, en la que se indica que saltó el contestador automático. El campo de consentimiento en *Altitude* se encuentra vacío ya que no se produjo interacción entre el operador y el titular del número de teléfono.

Según manifiesta la investigada, en febrero de 2018 actualizaron la versión de *Altitude* (de la versión 7 a la versión 8). Ambas plataformas gestionan distintas bases de datos sin ninguna interacción (no se han migrado los datos de una a otra). El campo que hace referencia al consentimiento se generó en *Altitude* versión 8 con la entrada en

vigor del RGPD. Anteriormente, se consideraba válido el consentimiento tácito (existía una leyenda que incluía el consentimiento para las comunicaciones comerciales en la propia página de internet de la investigada en la que se insertaba el teléfono para ser llamado, y durante la llamada no se solicitaba nuevamente el consentimiento). El documento *E_10418_2018_I01_DOC13* facilitado en el marco de la inspección E/10418/2018/I-01*,* que reproduce dicha leyenda, dispone, entre otra, la siguiente información:

El usuario consiente que sus datos personales sean objeto de tratamiento automatizado y formarán parte de los ficheros de SECURITAS DIRECT ESPAÑA S.A.U. los cuales se encuentran inscritos en el Registro General de la Agencia Española de Protección de Datos. El tratamiento automatizado de los datos proporcionados por los Usuarios a SECURITAS DIRECT ESPAÑA S.A.U. tendrán las siguientes finalidades:

- *Ofertarle productos y promociones de SECURITAS DIRECT ESPAÑA S.A.U., conforme a sus necesidades y a través de los medios facilitados.*

- *Enviarle comunicaciones informativas mediante medios electrónicos, incluyendo mensajes instantáneos a través de canales como WhatsApp (para lo cual sus datos serán transferidos internacionalmente a WhatsApp Inc.).*

- *Podrán utilizarse con fines estadísticos.*

De conformidad con lo establecido en el Título Tercero de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se informa a los Usuarios de la posibilidad de darse de baja de las comunicaciones así como de ejercitar, en el caso de que lo estimen oportuno, los derechos de acceso, rectificación, cancelación y oposición de sus datos personales, en la siguiente dirección: (…)

En la actualidad, para los potenciales clientes, se está ejecutando una regularización del consentimiento consistente en:

- En el marco del procedimiento de inspección E/10418/2018/I-01 culminado el día 7 de noviembre de 2019, la investigada informa de que se encuentra en proceso un plan de regularización de potenciales clientes captados con posterioridad al 1 de enero de 2015 de los que se dispone de consentimiento tácito.

- Así, el documento adjunto número 1 del escrito 54548/2019 facilitado por la investigada el 18 de noviembre de 2019 explica que "*se ha establecido un plan de contacto a los prospectos obtenidos desde el 2015, excluyéndose los registros anteriores a esta fecha 2015. Así, por ejemplo, en agosto de 2019 se ha contactado con los prospectos obtenidos en abril de 2018, abril + agosto + diciembre de 2017, abril + agosto + diciembre de 2016 y abril + agosto de 2015. Es decir, cada mes, se trata de regularizar un bloque de prospectos de*

los años anteriores. Debido a que durante el 2019 no se ha podido contactar con todos los prospectos obtenidos con anterioridad a la entrada en vigor del GDPR, este esquema se podrá repetir durante los próximos años".

- En el escrito 19512/2020 registrado de entrada en la AEPD el pasado 11 de junio de 2020, la investigada explica que *"el proyecto de regularización estaba previsto finalizarlo a fecha 31 de mayo de 2020, dos años después de la entrada en vigor del Reglamento General de Protección de Datos. Al llegar a esa fecha, la compañía había tomado la decisión de ofuscar todos los datos personales de todos aquellos prospectos no regularizados. Sin embargo, y a raíz de la situación excepcional que estamos viviendo y que ha impactado significativamente en nuestra compañía, toda nuestra actividad comercial, tanto telefónica, como de door to door, se ha visto completamente suspendida desde la citada declaración del estado de alarma. Adicionalmente, queremos destacar que, empleados del área de Marketing Captación (aproximadamente un 75% del total del área), entre cuyas funciones estaba la de regularizar a esta cartera de prospectos, se han visto afectados por un ERTE de fuerza mayor. Por este motivo, el proyecto de regularización se ha visto seriamente impactado debido a que con la reactivación paulatina de la actividad comercial el pasado 25 de mayo, los empleados de Marketing Captación que se han ido desafectando de dicho ERTE de fuerza mayor están priorizando la gestión de los prospectos que se están generando actualmente. Por eso, y con todo lo anterior, la compañía tiene el compromiso de finalizar este proyecto de regularización el 31 de diciembre de 2020, procediendo a partir de esa fecha a la ofuscación de todos los datos personales asociados a los prospectos no regularizados".*

- En el escrito 19512/2020 registrado de entrada en la AEPD el pasado 11 de junio de 2020, se refiere la situación con respecto al plan de regularización de prospectos recabados desde el 1 de enero de 2015 hasta el 25 de mayo de 2018 apuntando que:

    - Hay 3.300.000 *prospectos* que cumplen estas condiciones, de los cuales 1.400.000 son "*Prospectos potenciales clientes Residenciales"* y 1.800. son *"Prospectos potenciales clientes Negocio".* De los 1.400. "*Prospectos potenciales clientes Residenciales"*, se han regularizado el 35 por ciento, de los cuales el ochenta por ciento han dado un consentimiento positivo. Quedarían algo más de 900.000 "*Prospectos potenciales clientes Residenciales"* pendientes de regularizar.

    - *De todos aquellos prospectos regularizados con consentimiento positivo, se han mantenido todos los datos personales que éstos tienen asociados, salvo el DNI que, como hemos comentado previamente, se*

ha eliminado de cualquier prospecto (salvo los que se hayan recabado en los últimos tres meses que se irán borrando según vayan superando los tres meses de antigüedad). Al disponer del consentimiento expreso positivo para poder tratar sus datos de carácter personal con fines comerciales, mientras no manifiesten lo contrario se conservarán en nuestros sistemas.

- *De todos los prospectos con consentimiento negativo, se han ofuscado, sin posibilidad de recuperación, todos los datos personales a excepción del número de teléfono que pasan a formar parte de la lista Robinson interna de la compañía.*

- *De todos los prospectos que quedan pendientes de regularizar de este bloque se han ofuscado, sin posibilidad de recuperar, todos los datos personales a excepción del nombre junto con el número de teléfono, que son los dos mínimos datos de carácter personal necesarios para poder contactar con ellos en el marco del proyecto de regularización. Éste bloque de prospectos sólo serán contactados a efectos de regularización y no serán incluidos en ninguna campaña de tipo comercial mientras no hayan dado un consentimiento afirmativo para ello.*

- En el documento número 2 adjunto al escrito 19512/2020, fechado el 8 de junio de 2020 y titulado "*Informe de análisis de los procesos de regularización de prospecto y exclientes",* la auditora señala que *"se ha comprobado que, previa entrada en aplicación del RGPD el 25 de mayo de 2018, el tratamiento de los datos personales de prospecto de Securitas Direct se amparaba en el consentimiento tácito de los mismos"*. Al respecto continúa diciendo que, *"dado que este consentimiento tácito no constituye una de las bases jurídicas reguladas en el RGPD, la Compañía ha realizado un esfuerzo en la regularización de dichos consentimientos"*. Y añade que *"durante la revisión de cumplimiento realizada por la auditora, la Compañía ha presentado el plan de acción elaborado para la regularización del tratamiento de los datos personales de la categoría de interesados mencionada con anterioridad"*. Así, concluye que *"se ha establecido una planificación para contactar con dichos prospectos, retrospectivamente a 4 años respecto al año actual, con el objetivo de legalizar el tratamiento de sus datos*".

Por otro lado, en relación con los datos personales de prospectos recogidos con anterioridad al 1 de enero de 2015, en el escrito 19512/2020 del 11 de junio de 2020, la investigada expone que, *"habiendo realizado un análisis de la información de la que se disponía de este bloque de información, podemos confirmar a la Agencia que Securitas Direct dispone únicamente del 100% de los nombres y números de teléfono*

de todos esos prospectos, teniendo un 98% de direcciones postales recogidas. El resto de categoría de datos el porcentaje es residual (p.e. 7% de correos electrónicos o 58% de primeros apellidos)". Cita además que *"el volumen de prospectos anteriores al 1 de enero de 2015 es de 2.000.000"* e indica que *"esa bolsa de prospectos no forma parte del proyecto de regularización de la compañía"*. No obstante, añade lo siguiente:

"Por ese motivo, además, Securitas Direct avanzando en los proyectos de ofuscación de datos personales en nuestros sistemas, informó a la Agencia de que se estaba trabajando la aplicación de una serie de algoritmos de ofuscación de datos personales asociados a los prospectos sobre CRM41. Si bien es cierto que, durante la inspección se informó de que dicho proyecto estaba en una fase muy inicial, hemos podido seguir trabajando y desarrollando el mismo, de tal forma que podemos decir que durante el pasado mes de mayo, se ha procedido a ofuscar (sin posibilidad de recuperación) todos los datos personales asociados a los citados 2.000.000 prospectos anteriores a 2015 (nombre y apellidos, correo electrónico, dirección postal, DNI y números de teléfono), no quedando ningún dato de carácter personal asociado a dichos prospectos. A este respecto y haciendo un ejercicio de aproximación al número total de datos personales que se podrían haber eliminado tras este ejercicio, suponiendo que tuviésemos de cada prospecto un total de entre 4 v 7 datos personales, estamos hablando de la ofuscación de entre 8 y 14 millones de datos personales asociados a esos 2.000.000 prospectos.

Asimismo, y en el marco de esta misma operación, se decidió ofuscar. sin posibilidad de recuperación, todos y cada uno de los DNIs o CIFs asociados a cualquier prospecto, no sólo los asociados a todos los prospectos anteriores al año 2015, sino también todos los asociados a los prospectos posteriores y hasta la actualidad, conservando los DNIs o CIFs asociados a los prospectos recabados durante los últimos tres meses, que se irán borrando una vez que tengan una antigüedad superior a tres meses. En total, se han ofuscado un total de más de 4 millones de DNIs o CIFs relacionados a prospectos posteriores a 2015."

Como se ha comentado anteriormente, si no se genera el prospecto, los datos recopilados -a excepción de los relativos al consentimiento- no se trasladan a *CRM41* -permanecen únicamente en *Altitude- sine die*. La investigada manifiesta que existe un proyecto de ofuscación actualmente en marcha que incluirá los datos de las dos versiones de *Altitude* que utilizan (V7 y V8).

Las llamadas del *contact center* interno se graban y auditan en base a distintos parámetros (KPIs), que incluyen si se ha realizado correctamente o no la parte del argumentario correspondiente a la protección de datos personales. El equipo que realiza la auditoría es interno. Seleccionan un subconjunto del total de llamadas y otorgan una puntuación a varios parámetros, entre los que se encuentra uno relativo a la protección de datos personales. El informe con las puntuaciones se envía a los supervisores internos que, en su caso, retroalimentan con los resultados al personal. El documento *E_10418_2018_I01_DOC14* facilitado en el marco de la inspección

E/10418/2018/I-01 contiene información sobre las auditorías del *contact center* interno de *marketing-captación* (cuadros numéricos de auditorías y ejemplos de sanciones a operadores).

1. PROCEDIMIENTO DEL ÁREA DE *MARKETING-CLIENTE*

Al área de *marketing-cliente* le corresponden las actividades de mercadotecnia directa enfocadas en clientes y exclientes. Según manifiesta la investigada, la gestión de los datos de exclientes a estos efectos es análoga a la de los clientes. Además, los miembros de los planes de acción, tanto de clientes como de exclientes, no serían objeto de este tipo de acciones.

El sistema de gestión de clientes, exclientes, y miembros de los planes de acción asociados a éstos, es *SBN* (herramienta comercial). *SBN* es una aplicación cliente-servidor (su acceso no se realiza a través de un navegador de internet, sino que requiere la instalación de una aplicación en los ordenadores de los usuarios que se conecta a los servidores de la investigada para acceder al repositorio de datos). Hasta 2017 la adaptación de *SBN* para la investigada era realizada por una empresa externa. Desde entonces, el soporte se lleva a cabo desde un centro de desarrollo del grupo *Verisure* (grupo empresarial al que pertenece la investigada) en Suecia. El grupo *Verisure* mantiene dos versiones de *SBN*: una utilizada por los países del norte de Europa (el llamado *clúster norte*) y otra por los del sur (*clúster sur*). Las bases de datos del *clúster sur* residen en el Centro de Proceso de Datos (CPD) de Madrid. Cada país, no obstante, tiene su propia instancia de *SBN* independiente sin posibilidad de acceso o cruce de datos entre países.

Las actividades realizadas por el área de *marketing-cliente*s incluyen:

- Acciones orientadas a la fidelización de clientes, como por ejemplo explicar el contenido de las facturas, hacer recomendaciones de seguridad o realizar llamadas de bienvenida.

- Acciones de venta dirigidas a clientes y exclientes.

Ambos tipos de actividades se ejecutan en el contexto de “campañas”. Así, en primer lugar, se definen las características de la campaña y se plasman en una plantilla. Esto incluye realizar la parametrización del público objetivo, determinar las fechas de inicio y fin, especificar los filtros a ejecutar, etc. El documento *E_10418_2018_I01_DOC26 facilitado en el marco de la inspección E/10418/2018/I-01* muestra ejemplos de plantillas que definen campañas concretas orientadas a clientes y exclientes.

A partir de la plantilla, se extraen de la base de datos los clientes y/o exclientes que serán objeto de la acción comercial. Para ejecutar esta tarea, la investigada se apoya en una herramienta comercial de *IBM*. Ésta está instalada en los servidores de la investigada y ha sido adaptada a las necesidades de la compañía por un proveedor externo que continua a día 7 de noviembre de 2019 facilitando el soporte del sistema. El documento *E_10418_2018_I01_DOC28* facilitado en el marco de la inspección

E/10418/2018/I-01 muestra un ejemplo de definición de campaña a través de la herramienta *IBM.*

El consentimiento de los clientes para la realización de actividades comerciales se recoge a la firma del contrato. La concesión de este consentimiento en el marco del contrato no distingue el canal de realización de la comunicación comercial. Con posterioridad, los clientes pueden retirar el consentimiento por canal: postal, teléfono, correo electrónico*,* fax. Esta gestión se encuentra embebida en *SBN* en un campo denominado *Class14*. Los distintos valores que puede tomar este campo son:

- C, el cliente no ha dado su consentimiento para las comunicaciones comerciales por correo postal.

- E, el cliente no ha dado su consentimiento para las comunicaciones comerciales por correo electrónico.

- F, el cliente no ha dado su consentimiento para las comunicaciones comerciales por fax.

- L, el cliente no ha dado su consentimiento para las comunicaciones comerciales por teléfono.

- T, el cliente no ha dado su consentimiento para ningún tipo de comunicación comercial.

- Si está vacío, el consentimiento ha sido facilitado, bien sea tácitamente en el caso de los anteriores a la implantación del RGPD, o expresamente con posterioridad (la distinción de uno u otro en base de datos sólo puede realizarse a través del campo que indica la fecha de recogida).

La distinta tipología de clientes y exclientes se almacena en el campo *Monitoring Status* de *SBN*. Los miembros del plan de acción se encuentran asociados a cada cliente o excliente correspondiente.

En el marco de la inspección E/10418/2018/I-01 se realiza la búsqueda en el sistema SBN de la información correspondiente al número de teléfono ***TELEF.7**,* cuya titularidad es de un cliente de la investigada. El documento que refleja estas consultas, *E_10418_2018_I01_DOC30,* contiene los datos del cliente, entre los que se encuentran el nombre, apellidos y número de teléfono de las personas asociadas a su plan de acción.

La investigada expone que, a los clientes cuyo consentimiento para la realización de comunicaciones comerciales se recogió antes de la entrada en vigor del RGPD (de los cuales el consentimiento era tácito), se les envió por correo electrónico o SMS una comunicación en relación con el tratamiento de sus datos personales. El documento

adjunto número 2 del escrito 54548/2019 contiene información sobre esta comunicación entre las que se encuentran las finalidades, el responsable, el delegado de protección de datos, las categorías de datos tratadas, el plazo de conservación, los derechos que asisten a los interesados, etc.

Según manifestó la investigada en el marco de la inspección E/10418/2018/I-01 concluida el día 7 de noviembre de 2019, tiene un proyecto en marcha de recogida del consentimiento expreso de los exclientes de los que se tiene consentimiento tácito (anteriores a la entrada en vigor del RGPD). Sobre este particular se destaca la siguiente información:

- En el documento número 2 adjunto al escrito 19512/2020, fechado el 8 de junio de 2020 y titulado "*Informe de análisis de los procesos de regularización de prospecto y exclientes", la auditora* (autora del informe como parte de la auditoría de protección de datos) señala que "*se ha comprobado que, antes del 25 de mayo de 2018, los clientes de cartera de Securitas Direct, en el proceso de contratación del servicio, otorgaban un consentimiento tácito para el envío de comunicaciones comerciales"*. Añade que la investigada *"ha establecido un proceso de regularización de esta categoría de interesados*".

- En el escrito 19512/2020 registrado de entrada en la AEPD el pasado 11 de junio de 2020, la investigada informa que la cartera de exclientes a regularizar ascendía a 520.000. Añade que, de éstos se conservan *"todos los datos personales que facilitaron en el momento de la contratación y que eran necesarios para prestar el servicio (nombre y apellidos, DNI, dirección postal, teléfono de contacto, DNI, correo electrónico y cuenta bancaria)"*. Sobre este particular, la investigada hace constar que, siendo una empresa perteneciente al sector de la seguridad privada, está sujeta a una regulación que le impone la obligación de conservación de la información de los clientes *"durante un período de cinco años con posterioridad a la baja del servicio, para poder ser compartida con las Fuerzas y Cuerpos de Seguridad cuando sea requerida en el marco de cualquier investigación que estén llevando a cabo"*. Así, se citan los artículos 11 y 54 de la Ley 5/2014, el artículo 20 del Real Decreto 2364/1994, y el artículo 17 de la Orden INT/314/2011.

- En el escrito 19512/2020 registrado de entrada en la AEPD el pasado 11 de junio de 2020, la investigada describe la evolución de su política de conservación de datos aprobada con motivo de la entrada en vigor del RGPD enunciando que:

    - Inicialmente la política de conservación contemplaba dos momentos de ofuscación de los datos personales de los clientes tras su baja.

Un primer momento, pasados seis años de la baja, en el que *"se procedería a ofuscar (sin posibilidad de recuperar) una serie de datos de carácter personal no necesarios (p.e. DNI o cuenta bancaria)*". Justifica este primer momento en la necesidad de contar con los datos para ejercer su defensa ante una eventual reclamación sobre distintos ámbitos: *"Seguridad Privada, Consumo, Civil, Penal, Protección de Datos, etc."*.

Un segundo momento pasados diez años tras la baja en el que se ofuscan el resto de los datos personales. Justifica este segundo momento en *"el impacto económico que supone para la compañía ofuscar datos personales de los exclientes con mayor o menor antigüedad"*.

- No obstante, *"si bien esa fue la primera política que se acordó en la compañía, en el transcurso de los trabajos que se vienen realizando desde el año 2018 dentro del proyecto de conservación de datos, debido a la complejidad técnica que entraña dicho proyecto, se ha decidido modificar la política de conservación de datos descrita en el apartado anterior, del que más adelante, se detallará su evolución, dejando únicamente un plazo total de conservación de datos de carácter personal de 10 años desde que el cliente se haya dado de baja (este plazo es sin perjuicio de que un ex cliente ejercite su derecho de cancelación de datos) transcurrido el cual, todos los datos personales de esos ex clientes serán ofuscados sin posibilidad de recuperación".*

  Así, añade que *"una vez que el proyecto de conservación de datos esté ejecutándose que, como se puso en conocimiento de la Agencia durante la inspección, será a finales de este año 2020, deberán quedar ofuscados un primer bloque de aproximadamente 155.000 exclientes, con más de 10 años desde que dejaron la compañía"*.

- En el escrito 19512/2020 registrado de entrada en la AEPD el pasado 11 de junio de 2020, la investigada afirma que *"no ha incluido a ningún excliente dado de baja con anterioridad al 25 de mayo de 2018 en ninguna campaña comercial. Si han sido contactados desde esa fecha, únicamente ha sido con el fin de recabar su consentimiento expreso y regularizar su situación".* Añade que *"el proyecto de regularización de exclientes que se inició en Securitas Direct, estaba dirigido únicamente a recuperar el consentimiento de un total de 520.000 exclientes anteriores al 25 de mayo de 2018, divididos entre 270.000 exclientes residenciales y 250.000 exclientes negocio".* Añade que se están utilizando cuatro canales para realizar esta regularización:

  - Llamadas salientes. En estas llamadas lo primero que se hace es solicitar al excliente su consentimiento expreso para hacerle

comunicaciones comerciales de los productos y servicios de la investigada. Según indica, *"el promedio de exclientes contactados al mes a través de este canal es de 2.500 (de los cuales un 32% se corresponden generalmente con exclientes negocio y 68% exclientes residenciales), siendo llamadas que se vienen realizando incluso con anterioridad a la entrada en vigor del Reglamento General de Protección de Datos. De todos los contactos realizados, conseguimos el consentimiento positivo del 91% de los exclientes contactados. Actualmente se han regularizado, a través de esta canal, un total de 27.400 exclientes (9.000 exclientes negocio y 18.200 exclientes residenciales). De esa cantidad, hemos recogido un total de 24.660 de consentimientos positivos de forma expresa"*.

- Carta y llamada *Inbound.* Se envían comunicaciones postales a exclientes en las que se informa sobre aspectos técnicos y de uso de dispositivos de seguridad que permanecen instalados en sus domicilios (cita, por ejemplo, el traslado de dispositivos entre estancias). Así, según señala, *"si ese excliente, tras recibir la carta informativa contacta con nosotros telefónicamente para pedir más información porque quiere desprenderse de los dispositivos que tiene instalados en su domicilio, lo primero que se hace es pedir su consentimiento expreso para poder tratar sus datos con fines comerciales. El número promedio de cartas informativas enviadas al mes es de 7.000. El número de exclientes que han contactado telefónicamente y han dado su consentimiento a través de esta acción, forman parte de los 27.400 exclientes regularizados mencionados en la acción anterior*".

- Envíos de correo electrónico. *"En el mes de noviembre de 2019 se envió un correo electrónico informativo a 196.000 exclientes, donde directamente se requería la posibilidad de otorgar su consentimiento con fines comerciales mediante una acción proactiva sobre el propio correo electrónico. De todos los exclientes que recibieron el correo electrónico: 1.192 clientes dieron su consentimiento positivo. 13.886 abrieron el email pero no dieron el consentimiento. 183.050 no abrieron el correo electrónico".* Sobre los últimos, la investigada señala que *"en febrero de 2020, hemos contactado de nuevo con 48.400 exclientes repitiendo esa acción. Además, algunos exclientes optaron por enviar directamente un correo electrónico a dpo@securitasdirect.es, para solicitar no ser contactados más."*

- Por último, sobre este tema la investigada manifiesta en el escrito 19512/2020 que *"estos exclientes sin perjuicio del que estén regularizados o no o tengamos consentimientos negativos, se verán afectados directamente por la ejecución*

del proyecto de conservación de datos, siendo sus datos ofuscados si cumplen con los requisitos de temporalidad definidos en nuestras políticas internas de conservación de datos".

Según señala la investigada, las personas (clientes o exclientes) que no han dado su consentimiento expreso al tratamiento de sus datos con fines comerciales (o lo han retirado o ejercido el derecho de oposición) no se incluyen en las campañas comerciales. No se realiza un filtrado basado en la lista Robinson de ADigital ya que, según manifiesta la investigada, se trata de clientes o exclientes. En el caso de las acciones orientadas a la fidelización, de forma general, se realiza el mismo filtrado -a excepción de casos puntuales como la llamada de bienvenida (acciones que, según señala la investigada, no tienen la consideración de comerciales sino de servicio al cliente)-. El documento *E_10418_2018_I01_DOC32 Decálogo General de la Política de Privacidad de SD* facilitado en el marco de la inspección E/10418/2018/I-01, incluye en su punto quinto: "*no te pongas en contacto con los clientes o potenciales clientes que nos han pedido que no se les moleste*".

El resultado de la selección de las personas objeto de campaña se vuelca en un fichero que se almacena en la intranet de la investigada.

Para la ejecución de estas acciones comerciales o de fidelización, la investigada hace uso de un *contact center* interno, y de dos *contact center* externos provistos por Atento y TELECYL. S.A. (en adelante, Madison).

El documento *E_10418_2018_I01_DOC2* facilitado en el marco de la inspección E/10418/2018/I-01, copia del contrato suscrito entre la investigada y Madison, contiene la información correspondiente al tratamiento de datos personales en un anexo denominado *Acuerdo de tratamiento de datos de carácter personal,* de fecha 23 de mayo de 2018. Señala que Madison actúa en calidad de encargado de tratamiento.

El documento *E_10418_2018_I01_DOC3* facilitado en el marco de la inspección E/10418/2018/I-01, copia del contrato suscrito entre la investigada y Atento, contiene la información correspondiente al tratamiento de datos personales en el Anexo III. Igualmente especifica que Atento actúa en calidad de encargado de tratamiento.

La determinación de qué *contact center* actúa en cada campaña se basa en criterios de rentabilidad económica. El documento E_10418_2018_I01_DOC27 facilitado en el marco de la inspección E/10418/2018/I-01 (tipificado de carácter confidencial), incluye las directrices facilitadas a los *contact center* externos antes de la ejecución de las campañas.

El acceso de los usuarios de Atento y Madison a los datos de clientes y exclientes se realiza de forma remota a través de una conexión *SFTP* (protocolo seguro de transferencia de ficheros que permite enviar documentos cifrados a través de una red de telecomunicaciones) con el archivo de la campaña en cuestión alojado en los servidores de la investigada. Estos datos se descargan a los sistemas de Atento y

Madison. La devolución del fichero con las modificaciones correspondiente se realiza igualmente a través de una conexión *SFTP* a la misma ruta de recogida del fichero.

Las llamadas de los *contact center* (tanto internos como externos) se graban y se auditan con base en distintos parámetros (KPIs), que incluyen si se ha realizado correctamente o no la parte del argumentario correspondiente a la protección de datos personales.

5. VOLUMEN DE DATOS PERSONALES ALMACENADOS

Se facilita, juntamente con el escrito 6084/2019, la siguiente información relevante sobre el volumen de datos tratados:

- En el periodo junio – noviembre de 2018, los agentes comerciales recogieron 482.761 números de teléfono y direcciones sin número (esta cantidad incluye tanto los teléfonos facilitados directamente por los interesados como los referidos por éstos).

- En este mismo periodo se gestionaron 7501 derechos de oposición y 1548 derechos de cancelación (los datos, según manifiesta, engloban peticiones realizadas por clientes y potenciales clientes).

Se realizan, en el marco de la inspección E/10418/2018/I-01 concluida el pasado 7 de noviembre de 2019, las siguientes consultas a la base de datos *CRM41* (plasmadas en el documento *E_10418_2018_I01_DOC23*):

- Hay 1.370.000 números de teléfono distintos de potenciales clientes en la base de datos *CRM41* de la investigada.

- Hay 175.000 números de teléfono distintos de potenciales clientes en la base de datos *CRM41* de la investigada con consentimiento positivo para comunicaciones comerciales.

- Hay 42.000 números de teléfono distintos de potenciales clientes en la base de datos *CRM41* de la investigada con consentimiento negativo para comunicaciones comerciales.

- Hay datos relativos a 585.000 teléfonos distintos introducidos por la fuerza de ventas cuyos nombres asociados no están ofuscados y de los cuales no existe registro asociado de consentimiento (ni negativo ni positivo).

  Con respecto a este resultado, la investigada facilitó nueva información a la AEPD en marco del escrito 19512/2020 registrado de entrada en la AEPD el pasado 11 de junio de 2020. Así, manifiesta que en el documento que se adjunta como número 1, hay 4 pestañas: *“dos pestañas "query 585585" y "585585", que se corresponden con el ejercicio realizado por parte de los*

inspectores y su resultado, y otras dos "585585 modificado" y "query 585585 modificado" que es otra búsqueda realizada a partir de otros parámetros". Según explica, la consulta realizada en el ámbito de la investigación no era correcta del todo, pues se estarían mezclando consentimientos de varios tipos de usuarios. Por ello, la investigada facilita la consulta corregida y su resultado, en la que los campos *"NOMBRE", "APELLIDO1", "APELLIDO2", "TIPOVIA", "NOMBREVIA", "NUMVIA", "RESTOVIA", "POBLACION", y "CODPOBLA"* aparecen ofuscados (vacíos). Sí tienen valor asociado los campos *"TFNOCONTACTO1", "IDPROVINCIA", y "CODPOST".*

- Hay datos relativos a 299.224 teléfonos distintos insertados tras el 1 de junio de 2018 cuyos nombres asociados no están ofuscados y de los cuales no existe registro asociado de consentimiento (ni negativo ni positivo).

- Hay 5.841 potenciales clientes referidos en total en la base de datos.

- Hay 897 potenciales clientes referidos con consentimiento afirmativo para la realización de comunicaciones comerciales.

- Hay 177 potenciales clientes referidos con consentimiento negativo para la realización de comunicaciones comerciales.

  Con respecto a este resultado, la investigada facilitó nueva información a la AEPD en marco del escrito 19512/2020 registrado de entrada en la AEPD el pasado 11 de junio de 2020. Así, manifiesta que en el documento que se adjunta como número 1, la pestaña denominada *"query 177"* refleja la consulta a la base de datos realizada en el marco de la inspección, en tanto que la pestaña *"177*" refleja el resultado actual de la misma. Según señala, *"sólo se conserva el número de teléfono de esos leads ya que es la única manera de excluidos de cualquier campaña. El resto de información, no son datos personales y se mantienen a efectos analíticos internos"*. Se constata que los campos *NOMBRE*, *APELLIDO1*, *APELLIDO2*, *TIPOVIA*, *NOMBREVIA*, *NUMVIA* y *RESTOVIA* se encuentran vacíos, mientras que el campo *TFNOCONTACTO1* sí contiene información para los registros consignados en la pestaña *"177"*.

  Hay datos relativos a 350 teléfonos distintos de potenciales clientes referidos cuyos nombres asociados no están ofuscados y de los cuales no existe registro asociado de consentimiento (ni negativo ni positivo). Las fechas de creación de dichos registros oscilan entre el 5 de septiembre de 2018 y el 5 de octubre de 2019.

  Con respecto a este resultado, la investigada facilitó nueva información a la AEPD en marco del escrito 19512/2020 registrado de entrada en la AEPD el

pasado 11 de junio de 2020. Así, manifiesta que en el documento adjunto número 1 la pestaña denominada *"query 350"* refleja la consulta a la base de datos realizada en el marco de la inspección, en tanto que la pestaña *"350*" refleja *"el resultado actual de dicha query una vez realizados los procesos de ofuscación mencionados a lo largo de este escrito"*. Según señala los 19 registros que ofrece ahora la consulta como resultado se corresponde con los *"potenciales clientes referidos de los que la compañía ha recabado consentimiento expreso"*.

En cuanto a la información recabada de *Altitude*, se recoge, en el marco de la inspección E/10418/2018/I-01, la siguiente información (plasmada en el documento *E_10418_2018_I01_DOC24*):

- Se recoge de *Altitude* versión 8 información relativa a una campaña. Según indican existen once campañas activas. Con respecto a la campaña consultada, existen:

    - 152.867 registros de potenciales clientes cuyo estado es terminado (ya se realizó la gestión comercial con ellos).

    - 23.477 registros de potenciales clientes cuyo estado es terminado y que han comunicado su negativa a facilitar consentimiento para comunicaciones comerciales.

    - 74.303 registros de potenciales clientes cuyo estado es terminado y para los cuales no existe consentimiento para la realización de comunicaciones comerciales, ni positivo ni negativo. Según indican, en todos estos casos no se ha podido contactar con el titular de la línea.

- En *Altitude* versión 7, se recoge información correspondiente a la campaña más antigua (datos de septiembre de 2011). Como se ha dicho, no existe información relativa al consentimiento. Hay 40.911 registros de teléfonos categorizados como *Robinson.*

En relación con el *Programa Amigo* a través del sitio de internet de la investigada, se recoge, en el marco de la inspección E/10418/2018/I-01, la siguiente información (plasmada en el documento *E_10418_2018_I01_DOC25*):

- Evolución del número de solicitudes introducidas a través de la página de internet del *Programa Amigo*. En septiembre de 2019 se produjeron ocho y en ningún mes, desde septiembre de 2011, se superaron las 80. A efectos comparativos, la investigada traslada que el promedio mensual de números de teléfono introducidos a través del sitio de internet de la investigada es, aproximadamente, 42.000.

En relación con los volúmenes de datos de clientes y exclientes, la investigada facilita la siguiente información extraída del sistema *SBN* a fecha 7 de noviembre de 2019 (plasmada en el documento *E_10418_2018_I01_DOC31* facilitado en el marco de la inspección E/10418/2018/I-01):

- Hay más de 1.300.000 instalaciones operativas (en funcionamiento). El valor del campo estado (*mon_stat*) en *SBN* en estos casos es *OP*.

- Hay 1.045.851 instalaciones correspondientes a exclientes. De las cuales:

    - 1.007.597 tienen el campo *class14* vacío (el consentimiento ha sido facilitado, bien sea tácitamente en el caso de los anteriores a la implantación del RGPD, o expresamente con posterioridad).

    - 30.216 tienen consignado el valor “T” en el campo *class14* (no han dado su consentimiento para ningún tipo de comunicación comercial).

    - 6.379 tienen consignado el valor “E” en el campo *class14* (no han dado su consentimiento para comunicaciones comerciales por correo electrónico)

    - 1.303 tienen consignado el valor “L” en el campo *class14* (no han dado su consentimiento para comunicaciones comerciales por teléfono)

    - 347 tienen consignado el valor “C” en el campo *class14* (no han dado su consentimiento para comunicaciones comerciales por correo postal)

    - 9 tienen consignado el valor “F” en el campo *class14* (no han dado su consentimiento para comunicaciones comerciales por fax)

- Hay 51.739 instalaciones cuyo valor del campo estado (*mon_stat*) en *SBN* es *NI*. Este estado representa a clientes cuya instalación está pendiente. No obstante, existen instalaciones en este estado desde el día 5 de marzo de 1996. Se toma una muestra de 14 instalaciones correspondientes a los años 1996 y 1997 que tienen asociados nombres, apellidos y direcciones.

6. PROYECTOS DE LA INVESTIGADA SOBRE SUS TRATAMIENTOS

Durante el procedimiento de inspección E/10418/2018/I-01, la investigada informa de que tienen en marcha (con distinto grado de avance) varios proyectos que supondrán una modificación de distintos aspectos relacionados con el tratamiento de los datos personales.

En relación con el proyecto de ofuscación de la base de datos, el documento *E_10418_2018_I01_DOC17, Análisis Funcional – Casos de Uso. GDPR – Captación y Ventas Versión 1.1* de fecha 6 de marzo de 2018 *(calificado de carácter confidencial),* contiene la siguiente información de utilidad al objeto de este informe:

- El apartado 3.8.1 del documento refiere el caso de uso relativo al proceso de ofuscación de información de *preprospectos* y *prospectos*. Describe el caso especificando que "*se ofuscará (ocultará) la información personal de los preprospectos y prospectos de los que no se tenga el consentimiento de comunicaciones comerciales que hayan sido creados antes de X días (parametrizable en el SSIS)".*

  Como precondición del caso de uso señala que "*existen prospectos creados antes de X días sin consentimiento comercial".*

  Y como postcondición (salida del caso de uso) indica que "*se ha ofuscado la información personal de los prospectos creados antes de X días sin consentimiento comercial (no anteriores al 25 de Mayo de 2018)".*

- Además, como parte del *E_10418_2018_I01_DOC17,* se incluye un correo electrónico de fecha 4 de octubre de 2019 en el que se especifica la necesidad de ofuscar "*determinados campos de información como pueden ser el Nombre, DNI o parte de la Dirección"* correspondientes a:

  - Los potenciales clientes que llevan 90 días en situación de origen *CALL RP – Visita Concertada* y no se ha conseguido recabar su consentimiento.

  - Los potenciales clientes que llevan 90 días en situación de origen *CALL RP – Prospecto* sin convertirse en clientes (no se ha recabado aún su consentimiento).

El documento *E_10418_2018_I01_DOC19* describe otros dos proyectos que tiene en marcha la investigada. Son los proyectos siguientes:

- *Data Retention Project.*

  Según manifiesta, es un proyecto del grupo Verisure liderado por la investigada (el desarrollo lo está realizando la investigada si bien el resultado se implantará en varias sociedades del grupo erradicadas en distintos países de Europa). Este proyecto afecta a los períodos de conservación de los datos personales, previendo la ejecución de tratamientos de cifrado y ofuscación de los datos con base en distintos parámetros. Según manifiesta la investigada en el escrito 19512/2020, la inversión en este proyecto, durante los años 2019 y 2020 asciende a 389.000 euros.

Asimismo, el documento 2 adjunto al escrito 19512/2020 elaborado por la auditora, fechado el 8 de junio de 2020, y titulado "*Informe de análisis de los procesos de regularización de prospecto y exclientes"*, señala que *"se ha comprobado que la Compañía cuenta con un proyecto de retención de datos (en adelante, Proyecto de Retención) que consiste en la ofuscación de las bases de datos de los principales sistemas de Securitas Direct"*. Este mismo documento define el Proyecto de retención en los siguientes términos:

"El objetivo del Proyecto de Retención de Securitas Direct es adecuar los sistemas de la Compañía que tratan datos personales para la correcta aplicación de los plazos de conservación establecidos en la Compañía, dando así cumplimiento a los principios y requerimientos establecidos en el RGPD. Esta adecuación consiste en la implementación de un algoritmo que, cumpliendo los plazos de conservación establecidos en la Compañía, ofusque o cifre los datos personales tratados en los sistemas de Securitas Direct.

La principal diferencia entre la ofuscación y el cifrado es que, en el primer caso, una vez aplicado, no se puede obtener el dato real, es decir, no se puede revocar el proceso, mientras que, en el segundo caso, se podría acceder al dato real mediante una "llave o clave de cifrado".

La auditora ha evaluado la documentación e información facilitada por los responsables de la Compañía relativa a las distintas fases que componen el Proyecto de Retención. Se ha comprobado que el Proyecto se encuentra alineado con los principios de privacidad establecidos en la normativa de referencia, RGPD. Cabe destacar que los principios de confidencialidad, integridad y disponibilidad de la información se han establecido como pilares fundamentales en todas las fases del Proyecto.

De acuerdo con lo indicado por los responsables de la Compañía, el Proyecto se encuentra en sus primeras fases de desarrollo y tiene como alcance los principales sistemas que tratan datos de empleados y clientes de Securitas Direct. Si bien, se ha contemplado incluir, en próximas fases, otros sistemas que tratan esta categoría de datos personales como, entre otros, sistemas externos y otras plataformas que tratan datos personales de empleados; así como interfaces, procesos y sistemas secundarios conectados a los sistemas principales que tratan datos personales de clientes.

Adicionalmente, dada la volumetría de casuísticas de servicios contratados por los clientes de la Compañía, el alcance del Proyecto de Retención contempla únicamente las instalaciones simples. Si bien, una vez adecuada esta tipología de instalaciones, se ampliará el alcance del Proyecto con el objetivo de integrar en el mismo la totalidad de instalaciones registradas en los sistemas de Securitas Direct.

A fecha de emisión del presente Informe, las áreas involucradas en el Proyecto de Retención de la Compañía han llevado a cabo un análisis de las fuentes de datos, así como de las reglas o excepciones, impuestas desde las distintas

áreas de Securitas Direct, que afectan a los plazos de conservación y que deben ser tenidas en cuenta en la implementación del Proyecto.

Con el objetivo de desarrollar el algoritmo de ofuscación a ejecutar, la Compañía ha identificado los campos, susceptibles a almacenar datos personales, de las bases de datos de los sistemas en alcance. De este modo, los responsables de las áreas involucradas han identificado los campos a ofuscar y cifrar, así como aquellos que no se verán afectados por dicho algoritmo. De igual forma, la Oficina DPO, debe validar y, en su caso, determinar, el alcance del algoritmo de ofuscación sobre los campos que componen las bases de los sistemas en alcance del Proyecto.

A fecha de emisión del presente Informe, se ha obtenido evidencia de que la Compañía ha realizado un gran avance en la identificación de los campos, así como en la determinación de aquellos que deberán ser ofuscados y cifrados. De este modo, se considera que la obtención de tal detalle de información permitirá a la Compañía dar cumplimiento a los principios establecidos en el RGPD, y, especialmente, a los principios de exactitud, minimización de los datos y limitación del plazo de conservación, desde las fases más tempranas del Proyecto".

Durante el procedimiento de inspección E/10418/2018/I-01, concluido el pasado 7 de noviembre de 2019, la investigada informa de que, la primera fase de este proyecto se centraría en los datos relativos a exclientes y exempleados. Posteriormente, en el marco del escrito 19512/2020 registrado de entrada en la AEPD el 11 de junio de 2020, añade que, *"si bien se pensaba abordar en una fase posterior, se ha abordado la ofuscación de datos de Prospectos"*. Según señalan, estiman la ejecución siguiente:

- Sobre los datos de exclientes: una primera ejecución seis años después de la extinción del contrato sobre un conjunto de datos y, una segunda, diez años después de la extinción, sobre el resto. Según señala en el escrito 19512/2020, el sistema impactado por este proceso de ofuscación sería *SBN.*

  El documento *E_10418_2018_I01_DOC19* que refiere los periodos de conservación de datos acordados por la investigada, especifica que el período de seis años tiene su fundamento en la normativa de consumidores y el código civil, en relación con los plazos de prescripción. Mientras que señala también que fijar los diez años para el resto de los datos se motiva en las necesidades del negocio.

  Asimismo, en el escrito 19512/2020 facilita información sobre el estado de situación de este proyecto para los exclientes. Así, señala que durante el año 2020 está previsto realizar la ofuscación de *"aproximadamente 155000 instalaciones de un total de 320519 instalaciones dadas de baja antes de 2011".* Según señala se trata de

instalaciones que *“tienen unas particularidades específicas como por ejemplo, no tienen deuda/pleito/litigio/contencioso administrativo con la compañía, no poseen vinculación con otras instalaciones, no han sido trasladadas, etc.”.*

- Sobre los datos de exempleados: una primera ejecución, cuatro años después de la extinción del contrato sobre un conjunto de datos y, una segunda, ocho años después de la extinción, sobre el resto. Según señala en el escrito 19512/2020, los sistemas impactados por este proceso de ofuscación serían *META4, Workday* y *NavFrontal.*

  El documento *E_10418_2018_I01_DOC19* que refiere los periodos de conservación de datos acordados por la investigada, señala, sobre los datos de los exempleados los siguientes períodos de conservación: un conjunto de datos se mantienen durante cuatro años con base en la normativa laboral (artículo 4.1 y 4.2 del RDL 5/2000) y a la ley de infracciones y sanciones del orden social; otros datos se conservan durante seis años con base en la normativa laboral (artículo 4.3 del RDL 5/2000) y a la ley de infracciones y sanciones del orden social; un tercer conjunto de datos se mantienen durante diez años a efectos de análisis estadísticos; y un último conjunto de datos (que incluye DNI, nombre y apellidos, motivo de salida de la compañía, fecha de salida, etc.) se mantienen sin límite de tiempo por *motivos de seguridad y análisis históricos (negocio).* Con respecto a este último dato, la investigada, en el escrito 19512/2020 registrado de entrada en la AEPD el pasado 11 de junio de 2020, señala que ha decidido que los datos personales tanto de exclientes como de exempleados se ofuscarán a través de un proceso no reversible “*cuando estemos en disposición de hacerlo”*.

  Asimismo, en el escrito 19512/2020 facilita información sobre el estado de situación de este proyecto para el bloque de los exclientes. Así, señala que durante el año 2020 está previsto *“al tratarse de sistemas soportados por terceros (Meta4 y Workday) y cada uno con un proceso de ofuscación diferente, realizar un análisis de los sistemas involucrados Meta4 + Workday + NAVFrontal (sistema intermedio) para determinar, en cuál de ellos es conveniente realizar el proceso de 0fuscacíón, dejando para el año próximo la implementación de los desarrollos”*.

- Sobre los datos de *prospectos.* Según indica en el escrito 19512/2020, la funcionalidad de ofuscación de los datos de *prospectos* comenzó a ejecutarse sobre los sistemas de la investigada el día 28 de enero de 2020. Según manifiesta la investigada en el escrito 19512/2020, los sistemas impactados por este proceso de ofuscación serían *CRM41* y *ForceManager.* Tal y como se ha visto anteriormente, la investigada

señala que este proceso ha conllevado la ofuscación de los datos personales correspondientes a 2.033.467 *prospectos* cargados en el sistema antes del 1 de enero de 2015. Añade además que se ha ofuscado el DNI de todos los prospectos cuya antigüedad sea superior a tres meses.

- *USB Consents.*

  Según manifiesta la investigada, este proyecto, orientado a generar una base de datos única de consentimientos, se encuentra actualmente en fase de definición. Su objetivo es tratar de forma unificada información que actualmente se encuentra dispersa en relación con los consentimientos y los derechos de protección de datos personales.

  La planificación consignada en el documento señala que esta primera fase estaría lista para entrar en producción (ejecutarse sobre datos reales) en el tercer trimestre de 2020.

  El documento *E_10418_2018_I01_DOC18* refleja la situación del este proyecto a fecha 9 de octubre de 2019.

1. AUDITORÍAS DE PROTECCIÓN DE DATOS

Como parte del escrito 19512/2020 registrado de entrada en la AEPD el pasado 11 de junio de 2020, la investigada informa de que una de las primeras decisiones que tomó tras la entrada en vigor del RGPD con el fin de cumplir con el principio de responsabilidad proactiva y evidenciar su compromiso con el cumplimiento de la normativa de protección de datos fue la realización periódica de auditorías de protección de datos. Así, la investigada contrató a la auditora para ejecutar un proceso de auditoría dividido en tres fases (2019, 2020, y 2021). No obstante, la investigada manifiesta que *"este año (2020) estaba previsto ejecutar la fase 2 de la auditoría, pero en las condiciones actuales se ha suspendido hasta que planifiquemos el año 2021"*.

Según señalan, el informe final de la primera fase *"se cerró a primeros de 2020".* Añade que se adjunta al escrito 19512/2020 como documento número 2*.* No obstante, el documento facilitado, fechado el 8 de junio de 2020, se titula "*Informe de análisis de los procesos de regularización de prospecto y exclientes"* y según él mismo describe se trataría de *"un entregable añadido a la evaluación y revisión de cumplimiento del Reglamento General de Protección de Datos (en adelante, RGPD) llevada a cabo por la auditora en 2019".* No obstante, este documento cuenta con un apartado (3.1) en el que *"se detallan las principales acciones, a nivel organizativo, identificadas durante la revisión de cumplimiento del proceso de adecuación al RGPD llevado a cabo por Securitas Direct*". Este apartado incluye las siguientes consideraciones:

- *Se ha comprobado que la Compañía dispone de un modelo de gobierno de protección de datos que incluye las principales medidas técnicas y organizativas, basadas en las estipulaciones de la legislación vigente, que*

deben ser cumplidas y observadas por todo el personal con acceso a los datos de personales de Securitas Direct.

- *Se ha verificado que el grupo Securitas Direct Verisure (en adelante, el Grupo), del que forma parte Securitas Direct, con motivo de la entrada en vigor del RGPD, ha elaborado y desarrollado documentación en materia de protección de datos, teniendo en cuenta las normativas europeas de privacidad aplicables.*

  De este modo, cabe destacar que, la gestión y coordinación de los procesos de privacidad de la Compañía, así como la operativa seguida para el tratamiento de datos personales, se realiza de manera homogénea y global a todas las compañías del Grupo, permitiendo así compartir prácticas y lecciones aprendidas.

- *Se ha evidenciado que la Compañía ha desarrollado, aprobado y puesto a disposición de sus empleados una política de protección de datos. El objetivo principal de esta política es establecer los principios y reglas a seguir en la recogida, almacenamiento y tratamiento de los datos personales de los clientes, potenciales clientes, proveedores y empleados del Grupo, así como de todas las sociedades que forman parte de dicho Grupo.*

- *Se ha comprobado que Securitas Direct, entidad de seguridad privada, ha designado un Delegado de Protección de Datos de acuerdo con lo estipulado en el artículo 34 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD). Adicionalmente, se ha comprobado que el Delegado de Protección de Datos de Securitas Direct cuenta con la certificación Certified Data Privacy Professional (CDPP), que acredita un alto nivel de especialización en la normativa de protección de datos, tanto en un contexto local, como en un contexto europeo e internacional.*

  De igual forma, se ha evidenciado que la Compañía ha comunicado dicho nombramiento a sus empleados, así como a la Agencia Española de Protección de Datos (en adelante, AEPD). De igual forma, la Compañía ha establecido las funciones de dicha figura, así como las razones que justifican su designación, en el modelo de gobierno mencionado con anterioridad.

- *La Compañía cuenta con un Comité de Privacidad (PSC, por sus siglas en inglés), celebrado periódicamente cada dos meses, formado por los representantes de las principales áreas que tratan datos personales de Securitas Direct.*

- *Se ha comprobado que la Compañía se encuentra inmersa en las fases finales del proceso de regularización de contratos, u otros documentos jurídicos, que regulan los servicios prestados entre las distintas sociedades del Grupo.*

  Adicionalmente, se ha evidenciado que la Compañía ha establecido un plan de acción con el objetivo de regularizar los servicios prestados por los proveedores. Con este fin, en base a unos criterios como, por ejemplo, la criticidad del servicio, en términos de privacidad, o el tipo de datos tratados por el proveedor, Securitas Direct ha desarrollado una planificación para regularizar los contratos, u otros documentos jurídicos, que regulan los servicios prestados por dichos proveedores.

  De igual forma, se ha verificado que, en el proceso de homologación o contratación de nuevos proveedores o servicios seguido por la Compañía, desde la Oficina DPO se ha incluido una validación, en términos de privacidad, con el objetivo de regular el servicio de forma adecuada y correcta de acuerdo con su naturaleza.

- *Se ha verificado que la Compañía, con el objetivo de concienciar en materia de privacidad y seguridad a sus empleados, ha elaborado iniciativas de formación, en términos de protección de datos y, en particular, del RGPD, así como de seguridad de la información. Adicionalmente, estas iniciativas de formación resultan de igual aplicación para los nuevos empleados, debiendo éstos completarlas en su proceso de incorporación a Securitas Direct.*

- *De igual forma, siguiendo el principio de responsabilidad proactiva establecido en el RGPD, se ha comprobado que el área de Seguridad IT de la Compañía lleva a cabo un control y seguimiento de los sistemas de Securitas Direct, que tratan datos personales, a través del inventariado de los mismos, así como de revisiones de seguridad periódicas.*

  Como consecuencia, la capacidad de gestión, control y acción frente a una circunstancia sobrevenida, como, por ejemplo, la materialización de una amenaza o un incidente de seguridad aumenta de forma considerada.

Asimismo, el informe concluye con las siguientes consideraciones de la auditora:

“En nuestra opinión, Securitas Direct cuenta con un nivel de cumplimiento respecto a los principios, obligaciones y responsabilidades de obligada aplicación, exigidos por la normativa de referencia, favorable con perspectiva de mejora. Adicionalmente, se ha podido constatar que la Compañía, y su alta Dirección, presentan un compromiso y una responsabilidad proactiva frente a la privacidad.

Si bien, cabe destacar que, la finalización de los diferentes proyectos y acciones que la Compañía tiene en proceso, incluido el Proyecto de Retención detallado en el

presente Informe, permitirán obtener a Securitas Direct un avance óptimo en términos de garantía y confiabilidad de cumplimiento en el tratamiento de los datos personales".

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

II

El presente procedimiento trae causa las reclamaciones recibidas y tramitadas con los números de referencia E/03484/2018, de fecha de entrada en esta AEPD el 4/6/2018 (reclamante 1) y E/06577/2018, de fecha de entrada en esta AEPD el 10/08/2018 (reclamante 2), contra la entidad investigada.

En ambas reclamaciones se manifiesta que el personal comercial de la investigada, durante la ejecución de acciones comerciales *"a puerta fría"*, recaba, en ocasiones, de las personas a las que visitan, datos personales de terceros que pudieran estar interesados en los servicios de la entidad. Estos datos de terceros son utilizados para contactar y ofrecer los servicios de la investigada. Así, los reclamantes afirman haber recibido llamadas comerciales de la investigada al tiempo que niegan cualquier relación previa con la entidad. Declaran asimismo desconocer cómo se han obtenido sus datos de contacto y afirman no haber otorgado su consentimiento.

Ambas reclamaciones fueron no admitidas a trámite por esta AEPD al resultar, una vez analizadas, que se atendieron debidamente por la investigada el 30/10/2018 y 2/11/2018.

III

Respecto al análisis de actuaciones de la investigada del presente procedimiento -la investigación de los procedimientos que la investigada sigue en relación con los tratamientos de datos personales que efectúa en el ámbito de la mercadotecnia directa a través de telefonía- se parte de la información y documentación generada durante las actuaciones previas de investigación y en la inspección presencial de referencia E/10418/2018/I-01 llevada a cabo en la sede central de la investigada finalizada el 7/11/2019 y el informe final de inspección de fecha 2/07/2020.

En primer lugar, se debe señalar que las actuaciones de la investigada de las que trae causa el presente procedimiento tiene su origen en hechos previos y posteriores a la entrada en aplicación del RGPD (25/05/2018) y, como ya se ha señalado, las

reclamaciones ante esta AEPD se atendieron debidamente por la investigada en fechas 30/10/2018 y 2/11/2018.

En segundo lugar, se procede a analizar los distintos procedimientos que sigue la investigada en relación con los tratamientos de datos personales que efectúa en el ámbito de la mercadotecnia directa a través de telefonía, estado de implantación de actualizaciones y futuros proyectos en curso, si bien, en aras a la simplificación, se hará referencia a menciones en páginas anteriores.

Consta como investigación previa tres accesos por el inspector actuante al sitio web de la investigada, introduciendo un número de teléfono al objeto de comprobar la respuesta por la investigada.

En el primer caso, la investigada devolvió el contacto al teléfono facilitado para responder al interés mostrado por potencial cliente.

En el segundo caso, el inspector actuante hizo uso de la pestaña “Calcula Online”, e introdujo número de teléfono, código postal y destino (vivienda/negocio) del sistema de alarma por el que se interesa. En este caso, la investigada también devolvió el contacto al teléfono facilitado para responder al interés mostrado por potencial cliente.

En el tercer caso, el inspector actuante accedió al “*Programa amigos*”, comprobando la existencia de un enlace en el que se describen los términos relativos a la protección de datos en relación con el uso de dicho programa. En dicho enlace se informa al usuario sobre los detalles en materia de protección de datos para el uso de esta funcionalidad, en concreto: que deberá informar con antelación al titular del número de teléfono facilitado sobre las finalidades del tratamiento, que la investigada contactará con él, que dicho número de teléfono se incluirá en los ficheros de la investigada, dirección de contacto de la investigada, que la conversación podrá ser grabada, de la posibilidad de cómo y dónde ejercer sus derechos, la dirección del DPD de la investigada y que podrá dirigirse a la AEPD si no ve satisfecho su ejercicio. Una vez que la investigada procede a realizar la primera comunicación al potencial cliente, le informa sobre lo restante dispuesto en el art 14.1 y 2 del RGPD.

Esta interacción del inspector actuante ha servido para posteriormente comprobar el almacenamiento de la información en el sistema de información de la investigada (ver páginas 13, 18 y 19).

En el apartado “Contexto” (página 5) constan las distintas categorías de datos en función de su relación con la investigada: Clientes, Exclientes, miembros de Planes de Acción, Prospectos, y Leads.

En cuanto a los datos de los clientes la licitud del tratamiento parte del art 6.1.b) del RGPD.

En cuanto a los datos de los exclientes que permanecen en el Sistema de información de la investigada, los hay previos y posteriores a la entrada en aplicación del RGPD, motivo por el cual la investigada está llevando a cabo un plan de actuación para recabar el consentimiento expreso para continuar con su tratamiento y de “ofuscación”

(supresión), que finalizará el último trimestre de 2020 al no poder haberlo finalizado a principios de año tal y como estaba previsto como consecuencia de la declaración del estado alarma y sus consecuencia directas sobre el personal de la entidad que han sido incluidos el 80% en Ertes de fuerza mayor.

En el apartado “Procedimiento del Área de Ventas” (página 6), consta que no se recaban datos personales ya que no identifican ni permiten la identificación de su titular. Estos datos se incluyen en una base de datos (CRM41) en la que posteriormente se puede complementar con el consentimiento expreso para su tratamiento en el caso de que así se requiera. Se debe añadir, que la gestión de este tipo de tratamientos se realiza a través de gestores externos en calidad de encargados de tratamiento. Estos encargados del tratamiento externos antes de ejecutar la llamada comercial cruzan el dato del potencial cliente con la lista de exclusión publicitaria que la investigada les suministra. Esta lista es un compendio consolidado de la lista de exclusión de Adigital y de aquellos que han manifestado a la investigada su negativa a recibir comunicaciones comerciales (derecho de oposición) como consecuencia del ejercicio del derecho de oposición del que se informa en la llamada telefónica. Esta forma de actuar del servicio externo lleva en activo desde 2017 y sólo cuando se procede a realizar el primer contacto con el potencial cliente es cuando se informa se sus derechos y tras obtener el consentimiento expreso se procede a recabar el resto de datos personales.

Las directrices de actuación están protocolizadas mediante argumentarios (ver página 10, 11 y 12). Además, estas llamadas se graban y auditan posteriormente analizando su correcta ejecución y, en su caso, instando las correcciones o mejoras que procedan.

El “Área de marketing-captación” (página 15) emite llamadas a potenciales clientes que han introducido su número de teléfono para interesarse por los servicios de la investigada, y se realizan desde un *contac center* propio de la investigada. También se tratan datos del *“Programa amigos”.* En este último caso, la investigada manifiesta que este Plan se creó en 2013 y ha sido suprimido den febrero de 2020 como consecuencia de las adaptaciones que se están llevando a cabo en la investigada. Los datos recabados y facilitados por los interesados a la investigada para recibir información sobre los servicios se gestionan en este caso (“Área de marketing-captación”) desde otro aplicativo denominado *Altitude* y en su caso se marcan como “Robinson” si así se ha solicitado. El traspaso de estos derechos de oposición se realiza manualmente a la lista consolidada de exclusión y se almacenan en la base de datos CRM41. Actualmente este traspaso de derechos de oposición de *Altitude* a CRM41 se está automatizando.

Desde la inspección de datos se ha constatado que los números de teléfono facilitados para contacto por el inspector actuante se encuentran debidamente codificados conforme señala el DOC22 del acta de la inspección presencial. En la actualidad, para los potenciales clientes, se está ejecutando una regularización del consentimiento (ver página 20), estando ya actualizados el 35% del 1.400.000 existentes. Los datos de los

potenciales clientes que han expresado su consentimiento expreso se mantienen y los que deniegan el consentimiento se ofuscan sin posibilidad de recuperación.

Este tratamiento de regularización cuenta con el informe favorable de una entidad Auditora independiente.

Se debe señalar que estos tratamientos de regularización del consentimiento para potenciales clientes previas a la entrada en aplicación del RGPD, también son objeto de auditoría posterior a fin de comprobar el protocolo de actuación de la investigada y en su caso establecer las correcciones oportunas.

Al "Área de Markting-Cliente" le corresponden las actividades de mercadotecnia directa enfocada a clientes y exclientes sobre fidelización y venta, respectivamente. La gestión de estos datos se realiza desde el sistema de gestión denominado SBN que hasta 2017 se realizaba por una entidad externa a la investigada. Desde esa fecha se realiza por el grupo *Verisure* -grupo empresarial al que pertenece la investigada- con sede en Madrid sin que haya posibilidad de acceso o cruce de datos con otros países.

Para la regularización del consentimiento de los clientes al nuevo marco regulador por extensión del mismo a diversas campañas, se enviaron correos electrónicos o SMS.

Para la regularización del consentimiento de los exclientes al nuevo marco regulador -más de medio millón- se mantiene su almacenamiento por imperativo de la normativa de seguridad privada que obliga a su conservación por cinco años (Ley 5/2014), cancelándose tras ese periodo. No obstante, el proyecto de supresión de estos datos sigue en curso y finalizará a finales de 2020 por la razón antes expuesta (declaración del estado de alarma). Si embargo, aquellos datos en proceso de supresión nunca son incluidos en campañas comerciales.

En cuanto al volumen de datos objeto de tratamiento y regularización de los consentimientos, bien para recabar el consentimiento expreso bien para ampliar el consentimiento a otras campañas comerciales, la investigada informa que desde junio-noviembre de 2018 se gestionaron más de 7.500 derechos de oposición y más de 1500 derechos de supresión (ver página 29 y siguientes).

IV

Respecto de los proyectos y auditorias en curso que está llevando a cabo la investigada en el marco de regularización de los tratamientos a la nueva normativa, se constató en la citada inspección presencial, que se están ofuscando (suprimiendo) los datos de la información de prospectos y preprospectos en los que no se obtenga el consentimiento. También se están ofuscando los datos de los potenciales clientes que llevan más de 90 días en situación de "visita concertada".

Están en curso otros dos proyectos, denominados "Data Retention Proyect" y "USB Consents".

El primero afecta a periodos de conservación de los datos tratados, previendo la ofuscación o cifrado de los mismos con bases en distintos parámetros, con una inversión de 389.000 €. Respecto a este proyecto, la auditora ha evaluados la

información y certifica que las directrices se encuentran alineadas con los principios establecidos en el RGPD, si bien dada la volumetría de casuísticas de servicios contratados por la investigada, el alcance del proyecto contempla en principio a las instalaciones simples, con el objetivo de integrar en el mismo la totalidad de las instalaciones (ver página 34 y siguientes).

El segundo de los proyectos citados está orientado a generar una base de datos única de consentimientos, al encontrarse actualmente dispersa esta información.

En cuanto a la supresión de datos personales previos a 2015, la investigada manifiesta que se encuentra en curso un proyecto de aplicación de algoritmos de ofuscación de datos personales asociados a los prospectos sobre la base de datos CRM41. Durante el mes de mayo de 2020, se ofuscaron (sin posibilidad de recuperación) entre 8 y 14 millones de datos personales asociados a 2.000.000 prospectos anteriores a 2015 (nombre y apellidos, correo electrónico, dirección postal, DNI y números de teléfono), no quedando ningún dato de carácter personal asociado a dichos prospectos.

También se ofuscaron, sin posibilidad de recuperación, todos y cada uno de los DNIs o CIFs asociados a cualquier prospecto, no sólo los asociados a todos los prospectos anteriores al año 2015, sino también todos los asociados a los prospectos posteriores y hasta la actualidad, conservando los DNIs o CIFs asociados a los prospectos recabados durante los últimos tres meses, que se irán borrando una vez que tengan una antigüedad superior a tres meses. En total, se han ofuscado un total de más de 4 millones de DNIs o CIFs relacionados a prospectos posteriores a 2015.

V

La investigada informa de que una de las primeras decisiones que tomó tras la entrada en vigor del RGPD con el fin de cumplir con el principio de responsabilidad proactiva y su compromiso con el cumplimiento de la normativa de protección de datos fue la realización periódica de auditorías de protección de datos. Así, la investigada contrató a la auditora para ejecutar un proceso de auditoría dividido en tres fases (2019, 2020, y 2021).

La investigada manifiesta que el informe de auditoría final de la primera fase se cerró a primeros de 2020 en el que se detallan las principales acciones, a nivel organizativo, identificadas durante la revisión de cumplimiento del proceso de adecuación al RGPD (las consideraciones finales se encuentran recogidas en la página 37 y siguientes).

VI

Como conclusión, y al margen de los dos incidentes al principio mencionados que fueron atendidos debidamente por la investigada, se debe señalar que la investigada, dada la complejidad y volumen de datos del sistema de información y normativa aplicable al sector al que pertenece, consta que su conducta está siendo diligente al poner en marcha proyectos de auditoría y mejora en los tratamientos de los que es responsable basando su licitud en el consentimiento (art 6.1.a) RGPD), en el tratamiento necesario para la ejecución de un contrato (art 6.1b) RGPD) y otros en el interés legítimo (art 6.1.f) RGPD), toda vez que, en este último caso, se recaban datos

personales de terceros con la apariencia razonable de debido tratamiento, informando previa y adecuadamente sobre los aspectos básicos del tratamiento y las obligaciones que adquiere el cedente y facilitando al potencial cliente información sobre los aspectos básicos del tratamiento de sus datos (entre otros, origen y finalidad) y ejercicio de los derechos. No obstante lo anterior, consta que dicho tratamiento fue suprimido desde el mes de febrero de 2020. Respecto al derecho de oposición ejercido por los usuarios de los servicios y potenciales clientes, se debe señalar que la investigada mantiene actualizado un listado de exclusión publicitaria que denomina "listaExclConsolidada". Esta lista es un compendio consolidado de la lista de exclusión de Adigital y de aquellos que han manifestado a la investigada su negativa a recibir comunicaciones comerciales como consecuencia del ejercicio del derecho de oposición del que se informa en la llamada telefónica. Consta, asimismo, el proyecto de automatización que la investigada está llevando a cabo en la consolidación de esta lista de exclusión publicitaria consolidada en el ámbito del aplicativo Altitude que incluye también una *"Blacklist"* cuando se considera que el número es erróneo (bromas, descalificaciones, errores, etc.) para no atender ni emitir llamadas a esos números

No obstante, durante la implantación de los proyectos de mejora, actualmente en curso, la investigada se ha comprometido a evitar todo tratamiento de datos afectados por los proyectos inconclusos hasta su implantación definitiva en el cuarto trimestre de 2020.

VII

Por lo tanto, se considera que la actuación de la investigada como entidad responsable del tratamiento de los datos de carácter personal de los clientes, exclientes, potenciales clientes y empleados ha sido proporcional y diligente dado el volumen y la complejidad de los tratamientos y de las medias llevadas a cabo y que actualmente se encuentran en fase de finalización al último trimestre de 2020, resultando la actuación de la investigada proporcional con los principios rectores de la normativa sobre protección de datos personales analizada en los párrafos anteriores.

Por lo tanto, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a SECURITAS DIRECT ESPAÑA, S.A., con NIF A26106013 y domicilio postal a efectos de notificaciones en C/ Priégola 2, 28224 Pozuelo de Alarcón, Madrid.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora 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 de la referida Ley.

Mar España Martí
Directora de la Agencia Española de Protección de Datos