- **Expediente N.º: PS/00281/2022**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: Con fecha 23 y 24/03/2021, se recibe reclamación de ***A.A.A.,*** en adelante, la parte reclamante) contra **SECURITAS DIREC ESPAÑA, S.A.** con NIF ***A26106013*** (en adelante, la parte reclamada).

En ella, indica que en el procedimiento TD/01593/2017, la Agencia dictó una resolución del siguiente tenor: "*Securitas deberá facilitar el acceso al recurrente la información obrante en los servidores (...) relativa a los registros y señales enviados por el equipo de alarma (...), así como las copias existentes de los registros contenidos en la memoria interna de la alarma entre los días 26/11 y 13/12 del año 2015*". Esta resolución fue recurrida por Securitas Direct S.A. y confirmada por la Audiencia Nacional.

Ese procedimiento de ejercicio de derechos se produce como consecuencia de que el reclamante había ejercitado previamente su derecho acceso ante la reclamada el 7/04/2017: "*respecto a toda la información obrante en los servidores de Securitas Direct relativa a los registros y señales enviadas por el equipo de alarma instalado en" su propiedad, "así como las copias existentes de los registros contenidos en la memoria interna de la alarma entre los días 26 de noviembre y 18 de diciembre del año 2015 (antes y después del robo hubo otros incidentes de seguridad que conviene aclarar igualmente)",* "*habida cuenta de que tienen la calificación inequívoca de datos personales". "La información cuyo acceso se solicita hace referencia directa o indirectamente a sucesos y acontecimientos (entradas, salidas, movimientos, saltos de alarma, activación y desactivación de la alarma por determinado usuario, etc.) acaecidos en el interior de mi hogar, de los cuales puede inferirse, directa o indirectamente, actos o comportamientos relacionados con mi persona, otras personas de mi familia o incluso terceros autorizados al acceso a la vivienda".*

En relación con ese derecho de acceso, la reclamada le respondió el 11/05/2017 que "*los registros contenidos en la alarma no entran dentro de la categoría de datos personales*", según copia de documento 5 que aporta.

Al no estar de acuerdo con la respuesta dada por la empresa de seguridad, el reclamante presenta una reclamación ante la Agencia el 28/06/2017, en la que, entre otras cuestiones, indica que el 4/12/2015 por la tarde, descubrió, al acceder a su vivienda, que había sufrido un robo y encontró "*la central de alarma"* destrozada, sin haber sido avisado, recibiendo solo una llamada de la compañía de seguridad de esa misma mañana en la que le indicaban que existían problemas de conexión. En el texto de la reclamación presentada ante la Agencia el reclamante manifiesta que la reclamada "*se ha negado a esclarecer las circunstancias de la intromisión en nuestra vivienda o a desvelar la causa de que el sistema de alarma funcionara defectuosamente, asegurando que el sistema funcionó correctamente",* siendo los clientes los que tuvieron que

telefonear a la compañía de seguridad para informarles que la central de alarma que habían instalado *había sido destruida por los ladrones*.

La citada reclamación se resolvió el 2/01/2018 en el recurso de reposición del procedimiento de ejercicio de derechos TD/01593/2017, estimando el recurso y requiriendo en un plazo que se atendiera el derecho.

La reclamada recurrió la resolución ante la Audiencia Nacional (AN), que en la sentencia de la sala de lo Contencioso administrativo, sección primera, de 23/07/2019, recurso 146/2018, desestimó su pretensión.

La sentencia de la Audiencia Nacional fue recurrida ante el Tribunal Supremo en casación, admitida a trámite el 29/05/2020, recurso 78/2020, sin embargo, la reclamada desistió del mismo.

Alude el reclamante en su nueva reclamación, que ha vuelto a solicitar el acceso el 2/02/2021 y recibió respuesta de la reclamada de 23/02/2021, en la que destaca:

1) Responde: "*en cumplimiento, primero de la resolución del recurso de reposición RR 779/2017 de la AEPD y la sentencia de la Audiencia Nacional.", "adjuntando como documento 1, un listado de* "*logs asociados a dicho sistema de alarma que son datos de carácter personal*".

El documento 1, inicia:

"*Para poder entender la configuración de la tabla que hemos preparado con los logs que son datos personales…*", y explica los significados de las tres columnas.

La tabla Excel de logs proporcionada contiene en la primera columna la fecha/s y hora/ s en que se genera/ el log, o los logs. No aparecen ordenados de forma cronológica, comenzando por 5/12/2015. Solo un log aparece definido cronológicamente entre dos fechas, el de 5/12/2015 18:38: 10 y las 20:15:17. Comprende un total de 94 líneas de logs, más la del período, por lo que se desconoce cuántos serían en total.

La fecha o fechas de generación de los logs se correlacionan o agrupan con la "*denominación/nomenclatura del log*", y con una descripción básica como "*Señal informativa*", "*Actuación CRA"* (central receptora de alarmas), "*pruebas y verificaciones obligatorias como parte del mantenimiento de la instalación*".

En la última columna, con "*descripción extendida del log*", que según el reclamado contiene una descripción del significado del log, figura en algunos casos la clave N/A, asociada a una nomenclatura, por ejemplo de "*actuación CRA Salta buzón de voz*", "*operador consigue hablar con contacto*", o "*los contactos a los que el operador de Securitas trata de localizar no contestan*".

En otros tampoco se concreta al indicar: "*se deja mensaje en buzón de voz*".

En algún log se refiere a "*contacto*", sin identificar o especificar a que contacto se refiere, como "*contacto no recuerda la palabra clave para acreditar la identidad y*

cerrar la incidencia", o "*los contactos a los que el operador de Securitas trata de localizar no contestan*", "*operador consigue hablar con contacto*".

Se observa que figuran logs en los que consta: "*código generado automática y aleatoriamente por el sistema para que el vigilante desactive la alarma"*-, denominación: "*Central prioridad alta*", u otra denominación de log: "*pruebas y verificaciones obligatorias como parte del mantenimiento de la instalación*" conectado con "*denominación extendida*: "*el técnico realiza comprobaciones reglamentarias para asegurar el funcionamiento correcto del sistema. A petición del cliente puede modificar algún parámetro del propio sistema*".

Señala la reclamada que: "*Para simplificar la información hay diferentes fechas y horas asociados a un log, y ello es porque hemos agrupado por logs las fechas y horas en las que se generaron en el sistema del Sr*."

Considera el reclamante que no se ha contestado satisfactoriamente, debido a que:

-El acceso a la información obrante en los servidores ha sido filtrado/reducido por Securitas a los logs que ellos consideran datos personales, cuestión ésta que no le corresponde hacer.

-"La tabla proporcionada con información esquemática no satisface el derecho de acceso ejercitado. Por ejemplo, en la página uno, en la columna de nomenclatura "Actuación CRA", se hace constar "distintas actuaciones genéricas del operador humano de Securitas ante una incidencia concreta (e.g. habilitación del habla/escucha; llamada a los distintos contactos listados; comentarios internos en relación a la información que le transmite los contactos)" pero sin indicación alguna de que clase de actuación/información se ha registrado respecto a las incidencias listadas, lo cual impide al solicitante del derecho de acceso, entender y analizar dichos logs, que es el objetivo último de esta solicitud de acceso."

-"Por último, la respuesta de Securitas es inexistente respecto a la segunda parte de la petición de acceso recogida en la resolución: "las copias existentes de los registros contenidos en la memoria interna de la alarma", "no habiéndose indicado en ningún momento si es que esas copias no existen o no se da acceso por no considerar que no son "logs de datos personales".

Con la presentación de la reclamación por el reclamante manifiesta que no se ha atendido correctamente su derecho y con el tiempo transcurrido se le ocasiona indefensión.

SEGUNDO: La reclamación dio lugar a que la AEPD resolviera el 17/09/2021 un procedimiento por falta de atención de ejercicio de derechos (arts. 15 a 22 del RGPD), TD/00167/2021, en el que en el trámite de traslado de la reclamación para su resolución (E/4382/2021), la reclamada, manifestó con fecha 19/05/2021:

-"*El reclamante del derecho de acceso no solicitó en ningún momento tras la firmeza de la sentencia su ejecución o que cautelarmente se cumpliera la*

resolución de la Agencia que se recurrió en la misma".

Confirma la recepción del escrito del reclamante solicitando el ejercicio del derecho de acceso, al que "*dio respuesta con recepción de 3/03/2021*."

-Considera que no todos los logs que registran las señales de los equipos de alarmas, así como los contenidos en la memoria interna de la misma se pueden considerar que contienen datos de carácter personal, y que se desprendía del literal de la sentencia: "*Dentro de la información obrante en los servidores…, si figuran datos de carácter personal del titular de tal alarma contratada*". Por ello, encargó en 2020 un informe a un despacho jurídico que así lo establecía, para diferenciarlos, que no aporta, pero "*pone a disposición de la AEPD*".

Indica que, como resultado de ese ejercicio y ese informe, cuenta en la actualidad con un "*protocolo para su gestión*".

Explica su posición con base a dicho Informe que se resume a continuación.

Partiendo del concepto legal de datos de carácter personal, para poder determinar si la información tiene la condición de dato personal por versar sobre una persona física identificada o identificable, será preciso analizar la afectación que la información produce en la misma.

"*En cuanto a su contenido, la información debe suponer un atributo de cualquier índole predicable directamente del interesado en cuestión, existiendo una relación directa entre atributo y persona.*

En cuanto a su finalidad, el tratamiento de la información debe tener por objeto el conocimiento del mencionado atributo de esa persona.

En cuanto a sus efectos. la información debe referirse a aspectos que afecten al interesado como consecuencia del citado atributo."

En el término explicativo de qué es un dato personal, queda definido por "*toda información sobre una persona física*", se parte de cuando se refiera a ella, "*y como consecuencia, en el momento en que la información proporcionada no derive o se vincule directamente a la persona física, sino a objetos que le pertenecen o están bajo su influencia, solo indirectamente podrá considerarse que la información se refiere a esa persona y siempre que la misma permita inferir datos referidos a esa persona física y no al propio objeto". "Por tanto, la información sobre un objeto únicamente tendrá la consideración de dato personal cuando se establezca una conexión o vínculo entre el objeto y el afectado con el objetivo de generar información sobre dicha persona".*

La reclamada ha diferenciado dos categorías en las que se podrían encontrar los distintos logs.

En una primera categoría se encontrarían los logs que <u>consideran que no implican tratamiento de datos personales, que pueden comprender:</u>

"- aquellos en los que *no se recoge información sobre un interesado a través de dichos logs que lo individualicen frente al resto de la población,*

-no se pretende el conocimiento de dicha información con el fin de llevar a cabo un análisis del comportamiento o influir en el mismo, y

- no se ven afectados sus derechos y libertades.“

Enumera las categorías de los logs que se encontrarían en este supuesto:

1) “Emisión de señales de carácter puramente técnico de comunicación entre los dispositivos como parte del protocolo de verificación de su correcto funcionamiento o para el registro de algún fallo técnico.

2) Registro de señales informativas en relación con, entre otras, la versión del sistema, modelo o categoría del dispositivo instalado.

3) Registro descriptivo de procedimientos internos y técnicos ante un evento concreto.

4) Registro de señales técnicas en relación con las configuraciones de los dispositivos que no proporcionan información sobre el interesado o sus hábitos sino que simplemente refleja en calibraciones de los sistemas de Securitas para su correcto funcionamiento.

5) Información estadística acerca de los dispositivos.“

Alude además, que “*dichos logs*” podrían contener información sobre procesos técnicos internos de la reclamada cuya revelación a terceros podría implicar difusión de secretos comerciales. Menciona a tal efecto, el considerando 63 del RGPD, como legitimador de “*discriminar la información que puede proporcionar a la persona que ejerce el acceso.*”

En una segunda categoría estarían los logs que consideran **sí que implican tratamiento de datos personales**, en la medida que:

- “*Recogen la información sobre un interesado y sus características intrínsecas,*

-Se busca el conocimiento de dicha información para analizarlo o influir en su comportamiento,

-Se ven afectados sus derechos y libertades.”

Añadiendo o especificando que “*no todos los logs de esta categoría implicarían el tratamiento de datos de los titulares de los contratos*”, sino que “*podrían implicar el tratamiento de datos personales de terceras personas*”. **“**En esta categoría, *se incluirían los siguientes logs*.”

1) “*Procesos llevados a cabo por operadores o técnicos de Securitas , que en ocasiones pueden ser considerados dato personal de un tercero distinto al cliente de Securitas*”

2) “*Las interacciones activas del propio usuario -o terceros- con los sistemas en físico o a través de la aplicación móvil*.”

3) “*Interacciones pasivas del usuario o de terceros que puedan proporcionar información en relación con su forma de actuar en un determinado instante o su disponibilidad frente a un evento*.-

4) *Registros de identificadores de los interesados que se contienen en los logs, tales como por ejemplo nombre y apellidos o direcciones de correo electrónico*."

5) *Imágenes o datos en relación con una intrusión o sabotaje. En este sentido, es preciso indicar que si el intruso es captado por la cámara de seguridad, en la medida en que dicha persona sea identificable a raíz de la imagen obtenida, nos encontraríamos ante un dato personal del mismo*."

6) *Pulsaciones introducción de códigos que determinan una situación particular del interesado*.

7) *Configuraciones del propio usuario que determinan un conocimiento de sus gustos o patrones de conducta".*

Manifiesta que la respuesta del acceso proporcionada al reclamante contenía los logs que son datos de carácter personal que afectan al cliente, quedando "*excluidos los técnicos o que afectan a terceros*".

-Añaden que han enviado el 18/05/2021 un e mail al reclamante, aportan copia de documento 4 en el que se remiten a lo ya enviado el 26/02/2021, recibido por el reclamante el 3/03/2021.

-Manifiestan que las causas que han motivado la incidencia original de la reclamación se deben a que "*no todos los logs generados por un sistema de alarma son datos de carácter personal*".

-Con fecha 7/06/2021**,** se acuerda por la Directora de la AEPD "*el acuerdo de admisión a trámite, y el inicio de un procedimiento de ejercicio de derechos de los artículos 15 a 22 RGPD*", procedimiento TD/00167/2021.

-En el seno de dicho procedimiento, la reclamada, **(…),** manifiesta:

a) En relación con el contenido de la *"memoria interna de la alarma instalada en el domicilio del reclamante",* esta generó logs hasta el 27/11/2021, 20:09, hora y fecha en la que se produjo la intrusión en el domicilio-como este ya conoce- durante la cual dicho sistema de alarma quedó completamente inutilizado. A partir de esa fecha, no pudo generar más logs de ningún tipo. Por tanto, en el marco temporal entre el 26/11 y 18/12/2015, la memoria interna solo pudo generar logs los días 26 y 27/11/2015, y tras el análisis de los logs generados en la memoria interna de la alarma, solo constaba un log generado en ese marco temporal, el cual constaba *en la respuesta dada al reclamante el 23/02/2021.* Aportan documento 1, que es el cuadro con columnas del acceso que se le dio al reclamante en esa fecha, en el que aparece marcado en verde fluorescente ese log, y en el que se puede leer:

"*27/11/2015 20:09:47/CENTRAL PRIORIDAD ALTA/Código generado automática y aleatoriamente por el sistema para que el vigilante desactive la alarma*".

Consideran que han dado cumplimiento al derecho de acceso.

Ya en el seno de la tramitación de la TD/00167/2021, el 23/06/2021, se envió al reclamante la copia de la respuesta dada por la reclamada, y con fecha 16/07/2021, el reclamante manifestó:

-Por un lado que la información ha de proporcionarse de manera transparente e inteligible. "*El listado incompleto de logs proporcionado por Securitas Direct no permite a esta parte entender de manera transparente e inteligible la información obrante en sus servidores relativo al funcionamiento del sistema de alarma existente en mi domicilio".*

Por otro lado, señala que lo que ha hecho la reclamada ha sido confeccionar un listado de logs filtrado por el despacho de abogados que contrató, diferenciando los que puedan considerarse que contienen datos personales de aquellos otros que no. Añade que esta diferenciación no le corresponde a la reclamada y señala que "*la Audiencia Nacional consideró que todos los logs son datos de carácter personal y de ello deduce que el acceso ha sido incompleto*."

-Considera que no se cumple con dar el acceso al log, sino *a "la información obrante en los servidores relativa a los registros y señales del equipo de alarma instalado en su propiedad".* Consideraría que se cumple la resolución cuando se *"haya dado acceso a toda la información existente en los servidores en relación al funcionamiento de la alarma instalada en mi domicilio". "La información obrante en los servidores en relación al funcionamiento de la alarma instalada en mi domicilio va mucho más allá de estos logs a los que se pretende ceñir el derecho de acceso Securitas Direct, e incluye cualquier información en forma de texto, imágenes, alfanumérica etc. existente en sus servidores que guarde relación con los registros y señales del equipo de alarma instalado en mi vivienda".*

-Considera que la negativa de la reclamada a proporcionar acceso a la información obrante en sus servidores puede deberse a que pretende eludir sus responsabilidades particulares en relación a los daños y perjuicios ocasionados en este robo y "*dilatar y dificultar en la medida de lo posible la debida investigación de las razones de deficiente funcionamiento del sistema de alarma instalado en mi vivienda*".

-Sobre la respuesta proporcionada al log de la memoria interna de la alarma, considera no plausible la afirmación de que la central de alarma generó logs hasta las 20:09 del 27/11/2015, en que se produjo la intrusión y dicho sistema quedó inutilizado, ya que esa supuesta intrusión se refiere en realidad a un salto de la alarma del detector perimetral de la puerta del garaje, estancia que se encuentra físicamente separada de la vivienda y que no resultó afectada por el robo y estima que la intromisión en el domicilio se produjo en fecha posterior al 27/11, ya que "*si la central de la alarma quedó*" destruida, difícilmente podría Securitas haber desconectado remotamente la misma.

Subraya que la solicitud de acceso a los registros contenidos en la memoria se refieren tanto a "*la central de alarma destruida como a la que se instaló en mi vivienda el 5/12/2015 y que siguió generando señales y registros*".

Con fecha 17/09/2021 se resolvió el procedimiento de ejercicio de derechos, acordando estimar la reclamación y otorgando un plazo para atender el derecho. La resolución fue recurrida en reposición el 18/10/2021, resolviéndose el 27/10/2021 su desestimación, y figurando notificado electrónicamente a la reclamada el 28/10/2021.

Interesa destacar del mismo, que la reclamada, recurrente, manifestaba:

-La resolución del procedimiento de ejercicio de derechos estima atender el derecho, pero no determina la información que debe tener la consideración de dato personal, no argumenta los motivos que fundamenta su conclusión. Tampoco fundamenta "*que la totalidad de los logs generados por el sistema de alarma instalado tienen efectivamente la consideración de dato personal*". Solo detalla lo que reproduce el reclamado, de que "*no atiende la totalidad de lo solicitado puntualizado el motivo*", "*sin determinar si esa totalidad incorporará informaciones que nada tenga que ver con la normativa de protección de datos*".

"*Tampoco resulta cierta la afirmación del reclamante de que la SAN de 23/07/2019 indicara que toda la información o todos los logs generados por el sistema de alarma hayan de ser considerados datos personales*.", ya que la sentencia en su fundamento de derecho cuarto, indica que "*dentro de los logs se encuentran datos personales*", lo que permite concluir que "*no todos ellos deberán ser considerados como tales*". Estima que "*no es posible ejercitar el derecho de acceso a los datos personales respecto de información que en ningún momento pueda ser considerada dato personal*", y añade que la AEPD en las distintas resoluciones recaídas en este, caso no ha delimitado que información contiene datos que deban sujetarse a la normativa de protección de datos, "*es evidente que "la reclamada pueda delimitar que información tendrá el mencionado carácter*".

"*Ni la sentencia de la AN ni la resolución han delimitado que información contiene datos que deban considerarse sujetos a la normativa de protección de datos*", por lo que serán ellos los que lo tienen que delimitar.

Reproduce parte del dictamen 4/2017 sobre el concepto de datos personales adoptado el 20/06, WP 136:

"*En algunas ocasiones, la información que proporcionan los datos se refiere no tanto a personas como a objetos. Esos objetos suelen pertenecer a alguien, o pueden estar bajo la influencia de una persona o ejercer una influencia sobre ella o pueden tener una cierta proximidad física o geográfica con personas o con otros objetos. En esos casos, sólo indirectamente puede considerarse que la información se refiere a esas personas u objetos.*

Un análisis similar puede aplicarse cuando los datos se refieren en primera instancia a procesos o hechos, como por ejemplo el funcionamiento de una máquina cuando es necesaria la intervención humana. Bajo determinadas circunstancias, esta información también puede considerarse información «sobre» una persona."

Muestra su desacuerdo con el contenido de la resolución, que indica "*dado que el reclamante es el titular del contrato de la alarma, le es de aplicación la normativa sobre Protección de Datos en cuanto al derecho a acceder a los logs sobre el*

funcionamiento de la alarma instalada en su propiedad".

"*Además de los considerandos 26 a 28 para la conceptualización de los datos personales, no solo tienen esta condición la información que permita la identificación del interesado, sino también la que permita su singularización.*

A estos efectos la memoria explicativa del convenio 223 del Consejo de Europa de 10/10/2018 trata de matizar el contenido de individualización o singularización en estos términos:

"Esta individualización podría realizarse por ejemplo refiriéndose a él o a ella específicamente, o a un dispositivo o una combinación de dispositivos (computadora, teléfono móvil, cámara, dispositivos de juegos etcétera) sobre la base de un número de identificación, un seudónimo, datos biométricos o genéticos, datos de ubicación, una dirección IP u otro identificador. El uso de un seudónimo o de cualquier identificador digital/identidad digital no da lugar a la anonimización de los datos, ya que el interesado aún puede ser identificable o individualizado. Por tanto, los datos seudónimos deben considerarse datos personales y están cubiertos por las disposiciones del convenio."

"*Considera la reclamada que la información incluida en el sistema de alarma puede no referirse a un interesado, ni a sus características atributos o comportamientos, ni aun menos afectarlo de cualquier otro modo o permitir la inferencia de información relativa al mismo. En efecto, con carácter general esos logs consistirían en informaciones que únicamente hacen referencia a la comunicación entre sistemas de datos meramente operativos y técnicos que nada tienen que ver con un interesado ni se vinculan a el de ningún modo, y únicamente algunos de estos logs podrían permitir obtener información sobre la persona física titular de la alarma*". Pone tres ejemplos relacionados en los cinco casos en los que en su informe consideraba "*no datos personales*", en concreto:

En el 1), "*el nivel de batería del dispositivo, desconexión de la red, inhibición, etcétera*". Se trataba de la "*Emisión de señales de carácter puramente técnico de comunicación entre los dispositivos como parte del protocolo de verificación de su correcto funcionamiento o para el registro de algún fallo técnico".*

En el 3), "*tiempos de espera procedimentados ante un evento, recogida y descripción del evento, proceso de captura y puesta a disposición de los operadores de la imágenes o sonidos, modificación de parámetros internos, traslado del evento a un operador etcétera*". Se refería a "*Registro descriptivo de procedimientos internos y técnicos ante un evento concreto".*

En el 5) "*número de fotos captadas, dispositivos activados, calidad de las respuestas de los dispositivos, número de desconexiones, etc*.). Se refería a "*Información estadística acerca de los dispositivos*".

También pone ejemplos a los que anteriormente ha clasificado como "*datos de carácter personal*", como:

En el 1), "*el personal de Securitas Direct cuya actividad quede registrada en los propios logs". Se refería a:* "*Procesos llevados a cabo por operadores o técnicos de Securitas , que en ocasiones pueden ser considerados dato personal de un tercero distinto al cliente de Securitas*"

En el 3), "*el operador de Securitas Direct inicia una llamada y esta es contestada, o no por el usuario, se le solicita el código de seguridad y el usuario lo incluye correctamente o no, no se registran movimientos durante un período de tiempo determinado en la zona vigilada etcétera*". Se refería a: "*Interacciones pasivas del usuario o de terceros que puedan proporcionar información en relación con su forma de actuar en un determinado instante o su disponibilidad frente a un evento*."

En el 6) "*pulsador de pánico o inclusión del código de desactivación de alarmas bajo coacción", se refería a: Imágenes o datos en relación con una intrusión o sabotaje. En este sentido es preciso indicar que si el intruso es captado por la cámara de seguridad, en la medida en que dicha persona sea identificable a raíz de la imagen obtenida, nos encontraríamos ante un dato personal del mismo*."

En el punto 76 "*los distintos (...)s que utiliza, tiempos de dichos (...)s, configuraciones personales sobre volumen de los dispositivos, lenguaje, parámetros seleccionados sobre la calidad del aire o designación de nombres de usuarios y zonas etc*.", que relaciona con: "*Configuraciones del propio usuario que determinan un conocimiento de sus gustos o patrones de conducta".*

Si se diera acceso a todos los logs generados, cualquier persona tendría derecho a dicho tipo de acceso por el hecho de haber contratado la instalación de un sistema de alarma, siendo "públicamente accesibles" las operaciones técnicas de carácter interno desvinculadas de una persona y que revelan información sustancial sobre la eficacia y funcionamiento de los sistemas comercializados, pudiendo violarse la ley de secretos empresariales 1/2019 de 20/02 y lo relaciona con el considerando 63 del RGPD."

Sobre la expresión del reclamante de que no es posible entender los logs (actuación CRA…) señala que el formato para satisfacer el derecho de acceso lo fue para cumplir con lo establecido en el artículo 12 del RGPD "*en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo*" y que "*la información se encuentra listada en la tabla adjunta al escrito de 23/02/2021"*, y que "*incluso aquellos datos son registrados de forma técnica y poco inteligible para cualquier persona no versada en la terminología de sistemas de alarmas, e incluso en la propia terminología interna de Securitas, de forma que su lectura no revelaría la información que si incorpora en el formato remitido al interesado*". Manifiesta que "*llevó a cabo una adaptación de los logs a un lenguaje claro y sencillo para atender el derecho*". Indica que no tienen inconveniente en entregar la información en "*formatos líneas de código*", aunque satisfaría el derecho en menor medida el cumplimiento de los requisitos exigidos por el RGPD.

TERCERO: Con fecha 4/11/2021, el reclamante presenta un escrito en el que manifiesta que se sigue sin cumplir lo dispuesto en la resolución TD/00167/2021.

Con fecha 2/12/2021, la AEPD remite escrito a la reclamada, reiterando la petición del

cumplimiento de lo resuelto, otorgando plazo y advirtiendo de las consecuencias de su incumplimiento.

Con fecha 21/12/2021, la reclamada presenta escrito en el que manifiesta "*satisfacer el cumplimiento de la resolució*n" y aporta copia de escrito de 14/12/2021 y documentación que envía al reclamante. Manifiesta:*" Se ha llevado a cabo de nuevo un trabajo exhaustivo para proporcionar a D. xxx cualesquiera registros y señales enviados por el equipo de alarma que pudieran llegar a vincularse con la actuación, comportamiento o características del mismo excluyendo aquella información que no tiene la consideración de dato personal al tratarse de información exclusivamente técnica que además afecta al legítimo interés de Securitas Direct en la confidencialidad de sus secretos empresariales."*

En relación con los *registros contenidos en la memoria interna de la alarma entre los días 26 de noviembre y 18 de diciembre de 2015, la (micro tarjeta o chip) de los sistemas de alarma de Securitas Direct registran y almacenan la información procedente de los eventos con origen técnico y de los eventos con origen en la interacción de los dispositivos instalados en el domicilio de los clientes. En el caso del equipo instalado a D. xxx los registros de la memoria interna llegan hasta el momento en el que la misma quedó inutilizada y todos los registros recogidos antes de ese momento, son eventos de carácter técnico por lo que no es información personal*."

Acompaña los registros en hojas "*excel*" con la ordenación cronológica de logs por fecha y hora y más columnas informativas como event", "*event (...)*" "*Zone*", "******COLUMNA.3***", "****COLUMNA.4*". "****COLUMNA.1*""*área*", "*tiempo de* ***(...)***" por nombrar solo varias.

En la columna de descripción figuran términos descriptivos breves que no son comprensibles, por ejemplo, EVENT: palabra que su sentido especifico no es comprensible , igual que en "*event (...)*", y en general en todas las columnas.

Según la reclamada, es la "*transcripción literal, en el formato en que se recoge en los sistemas de SD de los registros y señales enviados por el equipo de alarma*."

CUARTO: Con fecha 7/05/2022, el reclamante presenta escrito en el que manifiesta que la respuesta de la reclamada persiste en clasificar los logs que son datos personales de los que no, cuando no le corresponde, reiterando que la cuestión ya fue dirimida por la AN. Señala que sigue sin atenderse el derecho durante años, volviendo a los orígenes de la sentencia de la AN. El cuadro es ininteligible, la expresión de la descripción es imprecisa, la letra muy pequeña, la mayoría de los logs corresponden a la intervención técnica de sustitución de la alarma destruida al día siguiente del robo: 5/12/2015, por lo tanto "*completamente inútiles e irrelevantes*". *"Siguen sin proporcionar la información que motiva el ejercicio del derecho de acceso, que no es otro que esclarecer las circunstancias del robo en mi vivienda y dirimir posibles responsabilidades*", y que "*necesita conocer que pasó con la alarma*".

Solicita, se "*acuerde la ejecución forzosa de su resolución…",* sin perjuicio de la "*apertura de un procedimiento sancionador*".

QUINTO: Con fecha 8/06/2022, la Directora de la AEPD acordó:

"*INICIAR PROCEDIMIENTO SANCIONADOR a* **SECURITAS DIRECT ESPAÑA, S.A.**, *con NIF* ***A26106013****, por la infracción del artículo 58.2 c) del RGPD, tipificada en el art. 83.6 del citado RGPD y 72.1.m) de la LOPDGDD*."

"*a los efectos previstos en el art. 64.2 b) de la ley 39/2015, de 1/10, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP, en adelante), la sanción que pudiera corresponder sería de 50.000 euros, sin perjuicio de lo que resulte de la instrucción*."

Dicho acuerdo de inicio fue debidamente notificado, otorgando a la reclamada plazo para efectuar alegaciones

SEXTO: Con fecha, 6/07/2022, la reclamada efectúa las siguientes alegaciones:

1) Reitera que durante el año 2020, encargaron a un despacho de abogados un informe, del que aportan copia en DOCUMENTO 1 (fecha firma **29/01/2021**) (ya se menciona antes el mismo en la respuesta al traslado de la reclamación de 19/05/2021, contenido supra en cuanto a la TD/00167/2021), sobre la "*aplicación del concepto de dato personal a los señales o logs generados por los sistemas de alarma",* con el objeto de si todos o parte de los mismos tienen la condición de dato personal a los efectos de la aplicación de la normativa sustantiva, y subsidiariamente como

2) Documento que para el futuro permita atender las solicitudes de ejercicio de derechos.

El informe lleva en portada: *"confidencia*l", desconociendo si alcanzaría a todo su contenido.

El informe partiendo de las definiciones históricas en la legislación del dato personal, considera que el RGPD introduce un concepto extensivo, al considerar que "*no sólo tendrá esta condición la información que permita la identificación del interesado, sino también la que permita su "singularización", aun cuando no fuera posible conocer directa o indirectamente a la persona a la que los datos se refieren*."

Alude el Convenio 108 del Consejo de Europa, de 28/01/1981, sobre la protección de las personas en relación con el tratamiento automatizado de sus datos personales, en la redacción resultante de la reforma operada por el Convenio 223, del Consejo de Europa, de 10 de octubre de 2018 (en adelante, por la denominación comúnmente aceptada "*Convenio 108+*") establece en su artículo 2 a) que a los efectos del propio Convenio, dato personal significa "*cualquier información sobre una persona física identificada o identificable*" y en relación con el concepto de persona identificable, siguiendo la misma línea establecida en el considerando 26 del RGPD, indica el párrafo §18 de su memoria explicativa:" *La noción de "identificable*" se refiere no solo a la identidad civil o jurídica del individuo como tal, sino también a lo que puede permitir "*individualizar*" o singularizar (y por tanto permitir tratar de manera diferente) a una persona de las demás. Esta "*individualización*" podría realizarse, por ejemplo, refiriéndose a él o ella específicamente, o a un dispositivo o una combinación de dispositivos (computadora, teléfono móvil, cámara, dispositivos de juego, etc.) sobre la base de un número de identificación, un seudónimo, datos biométricos o genéticos,

datos de ubicación, una dirección IP u otro identificador. El uso de un seudónimo o de cualquier identificador digital / identidad digital no da lugar a la anonimización de los datos, ya que el interesado aún puede ser identificable o individualizado. Por tanto, los datos seudónimos deben considerarse datos personales y están cubiertos por las disposiciones del Convenio. La calidad de las técnicas de seudonimización aplicadas debe tenerse debidamente en cuenta al evaluar la idoneidad de las salvaguardias implementadas para mitigar los riesgos para los interesados."

"*Se desprende que dicho concepto se caracteriza por la necesaria concurrencia de cuatro elementos esenciales*:

-El dato personal es en todo caso una información.

-Esa información debe referirse una persona determinada dado que debe ser sobre la misma.

-La persona a la que se refiere la información debe ser una persona física, quedando excluidas del concepto de dato personal las personas jurídicas o entidades sin personalidad jurídica.

-La persona debe ser identificada o identificable en el amplio sentido establecido por el considerando 26 del RGPD y el parágrafo 18 del convenio 108 + que identifican los conceptos "que identifique" e identificabilidad, singularización e individualización."

Menciona diversa jurisprudencia de los casos más reseñables sobre el concepto de datos de carácter personal de la Unión Europea.

Estima que para poder determinar, conforme a la jurisprudencia del TJUE si una información tiene la condición de dato personal por referirse a (o versar "*sobre*") una persona física identificada o identificables, será preciso analizar la afectación que la información produce en la misma:

·En cuanto a su contenido, es decir, la información debe suponer un atributo, de cualquier índole, predicable directamente del interesado en cuestión, existiendo una relación directa entre el citado atributo y dicha persona. De este modo, la información debe aparecer vinculada al interesado, excluyéndose del concepto de dato personal aquella información que no se vincule a una característica o actividad de aquél.

En cuanto a su finalidad, es decir, el tratamiento de la información debe tener por objeto el conocimiento del mencionado atributo predicable directamente de esa persona, quedando vinculado la finalidad del tratamiento al análisis de dicho atributo.

En cuanto a sus efectos, es decir, la información debe referirse a aspectos que afecten al interesado precisamente como consecuencia del citado atributo. Estas medidas pueden variar en cuanto a su intensidad (e.g. desde el mero hecho de contactar con él hasta la realización de un perfilado y la adopción de decisiones que le afecten significativamente)."·

También analiza varias sentencias recaídas en España sobre el concepto y alcance del dato personal y el análisis del concepto de dato personal del Dictamen 4/2007

sobre el concepto de datos personales, adoptado por el GT29 (documento WP136, de 20/06/2007).

Se indica en el Dictamen: "*un dato se refiere a una persona si hace referencia a su identidad, sus características o su comportamiento o si esa información se utiliza para determinar o influir en la manera en que se la trata o se la evalúa*".

"*Consecuencia de lo anterior será que en el momento en que la información proporcionada no derive o se vincule directamente a la persona física sino a objetos que le pertenecen o están bajo su influencia, sólo indirectamente podrá considerarse que la información se refiere a esa persona y siempre que la misma permita inferir datos referidos a esa persona física y no al propio objeto.",* cita el ejemplo 5 "*valor de una vivienda*" que refiere la aplicación de la normativa de protección de datos según el uso de esa información.

"El valor de una vivienda es información sobre un objeto. A todas luces, las normas sobre protección de datos no se aplicarán cuando esa información se utilice únicamente para ilustrar el nivel de precios de la vivienda en una determinada zona. Sin embargo, si se dan determinadas circunstancias esa información también debe considerarse como un dato personal. En efecto, la vivienda es un activo de su propietario y, como tal, se tendrá en cuenta, por ejemplo, a la hora de calcular los impuestos que deberá pagar esa persona. En este contexto, es incuestionable que tal información debe considerarse como datos personales".

"*El Grupo de trabajo ya se ocupó anteriormente de la cuestión de cuándo puede considerarse que una información versa «sobre» una persona. En el marco de sus debates sobre los problemas de protección de datos planteados por las etiquetas RFID, el Grupo de trabajo señaló que un «dato se refiere a una persona si hace referencia a su identidad, sus características o su comportamiento o si esa información se utiliza para determinar o influir en la manera en que se la trata o se la evalúa» . Teniendo en cuenta los casos mencionados anteriormente, y siguiendo la misma línea de razonamiento, podría afirmarse que para considerar que los datos versan «sobre» una persona debe haber un elemento «contenido» o un elemento «finalidad», o un elemento «resultado»*.

El elemento «contenido» está presente en aquellos casos en que - de acuerdo con lo que una sociedad suele general y vulgarmente entender por la palabra «sobre» - se proporciona información sobre una persona concreta, independientemente de cualquier propósito que puedan abrigar el responsable del tratamiento de los datos o un tercero, o de la repercusión de esa información en el interesado. La información versa «sobre» una persona cuando «se refiere» a esa persona, lo que debe ser evaluado teniendo en cuenta todas las circunstancias que rodean el caso. Por ejemplo, los resultados de un análisis médico se refieren claramente al paciente, o la información contenida en el expediente de una empresa bajo el nombre de determinado cliente se refiere claramente a él: De la misma manera, la información contenida en una etiqueta RFID o en un código de barras incorporados al documento de identidad de una determinada persona se refiere a esa persona, como en los futuros pasaportes que llevarán incorporados un microprocesador RFID.

También la presencia de un elemento «finalidad» puede ser lo que determine que la información verse «sobre» determinada persona. Se puede considerar que ese elemento «finalidad» existe cuando los datos se utilizan o es probable que se utilicen, teniendo en cuenta todas las circunstancias que rodean el caso concreto, con la finalidad de evaluar, tratar de determinada manera o influir en la situación o el comportamiento de una persona."

En base a ello, considera la reclamada que "*para considerar que "una información trata "sobre" una persona debe encontrarse, al menos, en uno de los siguientes tres supuestos o circunstancias:*

1. "Contenido": es decir, que la información se refiera de forma directa a una persona física concreta. Si concurre esta circunstancia será irrelevante cuál sea el propósito del responsable del tratamiento o de un tercero destinatario de la información o que repercusión tendrá el tratamiento de esa información en el interesado.

2. "Finalidad": la información recabada, si bien no se refiere de forma directa a una persona física, se utiliza o es probable que se utilice con la finalidad de evaluar, tratar de determinada manera o influir en la situación o el comportamiento de una persona.

3. "Resultado": aún en el supuesto de que no concurrir ninguna de las situaciones anteriores, una información versará "sobre" una persona cuando su uso repercuta en los derechos y los intereses de la misma, al poder ser tratado de forma diferente a otras personas como consecuencia del tratamiento de tal información."

Manifiesta la reclamada que:

- "*por lo tanto, la información sobre un objeto únicamente tendrá la consideración de dato personal cuando se establezca una conexión o vínculo entre el objeto y el afectado (particularmente pero no necesariamente, su dueño) con el objetivo de generar información sobre dicha persona o fomentar una actuación por su parte*"

Manifiesta la reclamada que: "Una vez analizado el concepto de *dato personal desde las perspectivas legal, doctrinal y jurisprudencial, procede ahora analizar la aplicación del mencionado concepto a los logs generados por los sistemas de alarma de Securitas Direct, a fin de determinar cuáles de ellos tendrán la condición de "dato personal", con la consiguiente aplicación en relación con los mismos de la normativa de protección de datos*."

"*Para llevar a cabo el análisis y calificación de los logs facilitados por Securitas Direct como dato personal se han tenido en consideración los siguientes aspectos:*

a*. Debe tratarse de información, en cualquier formato o forma conocida que de efectivamente implique la existencia real de datos.*

b*. Dicha información debe referirse a una persona* física específica, por lo que la información contenida en los logs deberá, como mínimo, encontrarse en una de las siguientes situaciones:

- Esté vinculada directamente con un individuo determinado, de tal manera que proporcione información directa sobre su forma de actuar, sus características mentales o físicas, sus preferencias, sus habilidades o cualquier otro patrón de conducta que pueda atribuirse directamente a la misma; o

- Pueda utilizarse para evaluar o influir de cualquier forma en un individuo determinado o en su conducta; o

- Pueda repercutir directamente en los derechos e intereses de un individuo determinado.

-"*La información incluida en un sistema de alarma puede no referirse a un interesado ni a sus características atributos o comportamientos, ni aún menos afectarlo de cualquier otro modo o permitir la inferencia de información relativa al mismo. En efecto, con carácter general los citados logs consistirán en informaciones que únicamente hacen referencia a la comunicación entre sistemas de datos meramente operativos y técnicos que nada tienen que ver con un interesado, ni se vinculan a él de ningún modo y únicamente algunos de estos logs podrían permitir obtener información sobre la persona física titular de la alarma*."

Partiendo de estos elementos, se han diferenciado dos categorías fundamentales en las que podrían encontrarse los distintos logs proporcionados por Securitas Direct,

a. "*Logs que no implican tratamiento de datos personales".* Reitera los motivos y las categorías que expuso en 19/05/2021.

-Aporta la diferenciación en el mismo documento 1:

Un Anexo I, que recoge el "*estudio*" específico de los distintos logs que los sistemas de Securitas generaron en relación con la prestación de sus servicios al reclamante. Dicho Anexo I contiene, a su vez, dos tablas distintas, agrupando aquellas líneas de log pertenecientes al reclamante no consideradas como dato personal (tabla I) (pág. 23 a 30/105) y aquéllas que sí tendrían esa consideración, a la vista del análisis llevado a cabo a lo largo del Informe (tabla II), (pág. 30/105).

En Anexo II, se adjunta el "*análisis general y sin aplicación específica a un interesado concreto, de la consideración como dato personal de las líneas de log genéricas que normalmente pueden ser utilizadas en los sistemas de Securitas Direct durante el desarrollo de su actividad*."

-En cuanto al Anexo I, "*dada la cantidad de información proporcionada, en relación con los logs*", se ha procedido a identificarlos (tanto para tabla I como tabla II) mediante tres columnas:

1. En la primera de ellas*, "fecha de la línea del log", se recogen las "fechas y horas concretas de aparición".* Se aprecia que se pueden agrupar diversas fechas y horas

2. En la segunda, se incluye la *"denominación de la información."*

3. La siguiente es: "*descripción extendida*", *"conformada tanto por lo información facilitada por Securitas Direct durante las distintas reuniones mantenidas, así como de los documentos y tablas recibidas y del resto de columnas explicativas que se contienen en el propio log."*

Prosigue la reclamada que*: "A continuación, se ha llevado a cabo la "valoración del carácter de dato personal de cada uno de los logs" mediante la inclusión de dos columnas adicionales:*

b. *"En la cuarta columna, se procede a valorar si la información contenida en la línea de log concreta permite a Securitas Direct recabar información sobre el Reclamante o un tercero, o analizar y causar un impacto en su comportamiento",* bajo la denominación de: *"vinculación, de forma directa o mediante inferencia, a una conducta o información de una persona física".*

Se observa que contienen términos, como operador, cliente, usuario autorizado, contactos designados por este, interesados solicitante del derecho.

c. La última columna, concreta si la línea de log puede considerarse, partiendo de todo lo indicado, como dato personal o no, con el literal ¿Se considera dato personal? No, en todas las de la tabla I, mientras que la tabla II, en "*¿se considera dato personal?"* figura "*Si*", y se añade una columna de*: "Es susceptible de ser proporcionada como respuesta al ejercicio del derecho de acceso del interesado?,* figurando en algunos casos: si, y en otros anotaciones diferentes, ya que "*se han detectado líneas de log que sí podrían tener la consideración de dato personal pero que refieren a terceros interesados distintos del propio Reclamante y, cabe recordar, la petición de acceso permite exclusivamente que el Reclamante tenga acceso, a los datos personales que sobre su persona trate Securitas y no a aquéllos sobre otras personas físicas*."

En la tabla I, "*Información no considerada dato personal en relación con la petición de acceso analizada*" (23 a 30), destacan:

- En tres descriptores figura -"*Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física*":"*No se encuentra vinculación directa con información del interesado en la medida en que se trata de comunicaciones periódicas máquina-máquina de comprobación del estado de los dispositivos*", todos con: "*descripción extendida*: *Señales enviadas por la alarma que corresponden al estado de funcionamiento de los dispositivos*", que pueden responder en: "*denominación de información:*
En un caso: "*Superv Foto PIR RADIO, REPETIDOR RADIO, VOLUMETRICO RADIO*", otro: "*superv repetidor radio*" y " *superv volumétrico radio*"

-- -"*Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física*": "*No se encuentra vinculación directa con información del interesado en la medida en que esta línea de log no recaba información sobre el interesado ni pretende analizar o causar un impacto en su comportamiento, simplemente delimita un proceso interno de Securitas Direct en relación con una señal inicial de alarma*", y en "*descripción extendida*": "*Ante la señal inicial de alarma, se otorga un tiempo de margen por si se trata de un fallo u olvido por parte del usuario a la hora de no desactivar la alarma*.", "*denominació*n *de la información: confía espera 35 segundos para una posible desconexión*".

---"*Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física*": "*Información de carácter técnico de Securitas Direct. En la medida en la que no se traslada información directa sobre un atributo del interesado ni Securitas Direct pretende analizar un patrón de conducta o influir sobre él en modo al-*

guno, la información facilitada por la línea de log analizada no debería ser considerada como dato personal", "*descripción extendida: Detección de falta de corriente eléctrica en el dispositivo"*, "*denominación de la información: corriente eléctrica-auto*".

---"*Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física*": "*Se trata de un cambio de prioridad interna de la incidencia motivado por una señal de alarma no desconectada*" y en "*descripción extendida*": "*Cambia la prioridad porque se envía la incidencia a una cola manua*l.", "*denominación de la información" "PRIO 25---20*."

--"*Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física*": "*No se encuentra vinculación directa con información del cliente en la medida en que se trata de señales informativas de carácter técnico*". y en "*descripción extendida: nivel de cobertura del panel", "denominación de la información: señal informativa*".

--"*Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física*": "*Esta línea de log, si bien proporciona información sobre un salto de alarma en los sensores, en la medida en la que no se traslada información directa sobre un atributo del interesado ni Securitas Direct pretende analizar un patrón de conducta o influir sobre él en modo alguno, la información facilitada por la línea de log analizada no debería ser considerada como dato personal. En este sentido, se trataría de un descriptivo del proceso técnico e interno de Securitas Direct*", y en "*descripción extendida*": "*En estas líneas de log se describe el proceso del sistema y sensores en la detección de una intrusión"*. "*Denominación de la información:-"INTRUSION VOLUMETRICO RADIO, 27 11 2015, 20:09:47*

--"*Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física*": "*La señal, dada su relevancia, es transmitida a un operador máquina o humano para iniciar el proceso de gestión. No obstante, es un procedimiento interno del que no se puede inferir ningún dato personal del usuario*", "*descripción extendida*": "*Indicativo de que la incidencia se transmite a un operador humano o máquina*", "*denominación información (...): 0*".

-El único que comprende periodos de días y fechas indica: -"*Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física*": "*Sin perjuicio de que producto de alguna de estas señales pueda iniciarse algún tipo de actuación que sí implique el tratamiento de datos personales, los procedimientos y procesos internos de verificación son esencialmente técnicos y no es posible inferir ningún dato personal de los mismos"*, "*descripción extendida*": "*Describen periodos en los que se produce una pérdida de conexión entre los servidores de Securitas Direct y el dispositivo instalado en el domicilio del interesado. De esta forma, los dispositivos emiten una señal técnica periódica para confirmar que efectivamente se encuentra en conexión y en disposición de realizar su actividad. Asimismo, los logs describen las actuaciones internas y técnicas llevadas a cabo producto de esta desconexión*", "*denominación de la información: (...) TRASNFER*".

--"*Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física*": "*No existe vinculación con el usuario en la medida en la que se*

trata de un procedimiento interno que se debe seguir para prestar el servicio de forma correcta", y en "*descripción extendida*": Información técnica de que la incidencia es transferida a un operador humano para su gestión.", "*denominación : GTI: incidencia cancelada, cliente ya existe en cola manual 14*".

- -"*Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física*": "*Información de carácter procedimental e interno de Securitas Direct*", sin descripción extendida, "*denominación de la información: GTI: incidencia cancelada, pendiente de mantenimiento*".

--"*Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física*": "*Esta línea de log, si bien proporciona información sobre un salto de alarma en los sensores, en la medida en la que no se traslada información directa sobre un atributo del interesado ni Securitas Direct pretende analizar un patrón de conducta o influir sobre él en modo alguno, la información facilitada por la línea de log analizada no debería ser considerada como dato personal. En este sentido, se trataría de un descriptivo del proceso técnico e interno para la disposición de las imágenes de los detectores*", y en "*descripción extendida: En estas líneas de log se describen los distintos procesos de los sistemas y sensores desde que se detecta intrusión real: zona de detección, captura de las imágenes, disponibilidad de las mismas para el operador, etc*.", "*denominación : intrusión foto PIR Radio*", en se considera dato personal se añade: "*NO (no obstante lo anterior, las imágenes capturadas, en caso de que hubieran captado a algún sujeto, sí tendrían la consideración de datos personales y deberían ser facilitadas al interesado en caso de que lo hubiesen captado a él y no a un tercero*).

--"*Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física*": "*Información de carácter técnico de Securitas Direct en relación con las detecciones de movimientos a través de los distintos sensores del sistema*", y en "descripción extendida: Información del sistema en relación con una petición de fotografía o imagen", "denominación de la información: *Señal informativa*". Indica que no se considera dato personal, "*No obstante si estas detecciones pudieran implicar la recogida de algún tipo de información de un interesado, sí podrían tener la consideración de datos personales y deberían ser facilitadas al interesado en el caso de que lo hubiesen captado a él y no a un tercero*."

--"*Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física*": "*no se proporciona información en relación con ninguna característica patrón de conducta u otra información del usuario*", sin descripción extendida, "*denominación de la información: sin motivo*."

--"*Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física*": "*información de carácter técnico de Securitas Direct*", sin descripción extendida, "*denominación de la información: cortes de corriente: incidencia con restauración*."

En la tabla II, "*información considerada dato personal en relación con la petición de acceso analizada*" (pág. 31 a 48/105). En la columna de "¿es susceptible de ser proporcionada como respuesta al ejercicio del derecho de acceso del interesado?, suele

figurar Si, pero en algunas constan observaciones con salvedades y en una figura, NO.

informa el reclamado que "*determinados registros de las tablas del presente Anexo carecen de fecha concreta debido a que se trata de comentarios generales, independientes de una línea específica y con afectación transversal a todo el documento*."

-Figuran sin fecha:

-"*Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física*: "*De la información conjunta proporcionada por: (i) modo de alarma seleccionado por el usuario; (ii) fecha del log concreto y (iii) información derivada del "tiempo de **(...)**", podría derivarse el conocimiento de ciertos patrones de conducta de un usuario (e.g. a partir de cierta hora de la tarde los días de semana el interesado aplica un **(...)** determinado con lo que es posible que no se encuentre en su domicilio)", "descripción extendida: "modo de conexión de la alarma y tiempo que lleva la alarma conectada en dicho modo", "denominación de la información: **(...)** y tiempo de **(...)**."*

- "*Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física*: *Las prioridades más altas tienen relación directa con el usuario mientras que las prioridades bajas corresponden a logs de control y verificación técnico de los cuales no se puede inferir información del usuario"*, "*descripción extendida*: *Las distintas cifras incluidas a la columna "***COLUMNA.3" del log son prioridades asignadas según el tipo de señal que se recibe. A menor valor numérico, mayor prioridad (generalmente con actuaciones propias del interesado como llamada SOS); a mayor valor numérico, menor prioridad (generalmente relacionadas con incidencias de carácter técnico*). Figura la anotación añadida de: "*¿Es susceptible de ser proporcionada como respuesta al ejercicio del derecho de acceso del interesado?*": "*Únicamente aquellas prioridades calificadas como altas y conectadas con una actuación o situación particular del interesado (e.g prioridades unidas a situaciones de pánico o socorro)."*

--"*Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física*: estas denominaciones de las áreas, en tanto son áreas de la propiedad del usuario definidas por el mismo y conllevan información sobre elecciones del interesado, supondrían datos personales", "*descripción extendida: a lo largo del log se encuentran denominaciones, decididas por el interesado, para nombrar ciertas áreas de la propiedad, ejemplo perimetral, puerta del garaje etc*.", "*denominación de la información: nombres de las áreas definidas por el usuario en todos los blogs*"

-Ya con fecha de log, figuran, en todos ellos que sí se consideran datos personales, y entre otros:

-"*Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física*: en la medida en la que se trate de configuraciones llevadas a cabo por el interesado implicaría el conocimiento de características y preferencias del mismo por lo que tendrían la consideración de dato personal", en "*descripción extendida el dispositivo informa sobre distintas características relativas a su configuración y programación por ejemplo en tiempos de entrada, salida, volumen sirena entre otros", "denominación de la información señal informativa".*

-*"Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física*": *No se encuentra vinculación directa con información de un cliente*

en la medida en que se trata de señales informativas de carácter técnico y no se proporciona información en relación con ninguna característica, patrón de conducta u otra información de una persona física.", "*descripción extendida: Código generado automática y aleatoriamente por el sistema para que el vigilante desactive la alarma*", "*denominación de la información*: *Central prioridad alta*". *"Es susceptible de ser proporcionada como respuesta al ejercicio del derecho de acceso del interesado?*"": No. 27/11/2015

Se desconoce porque no figura clasificada en la tabla I.

- *"Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física: Actuación directa de un operador*". "*Descripción extendida"*: "*El operador comienza la gestión de la incidencia y realiza las llamadas de comprobación al usuario y otras personas indicadas por el mismo en caso de incidencia*." "*denominación de la información actuación Central Receptora Alarmas-llamada a H/E*"- *"¿Es susceptible de ser proporcionada como respuesta al ejercicio del derecho de acceso del interesado?"* "*En este sentido, sin perjuicio de que se trate de un dato personal, lo sería del operador y no del interesado que ejercita su derecho de acceso, por cuanto no es una información sobre dicho interesado."*

- "Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física: Las actuaciones de un operador, que incluye interacción con el usuario o los contactos designados por éste, suponen la obtención de información sobre dichos interesados", descripción extendida: "*Distintas actuaciones genéricas del operador humano de Securitas Direct ante una incidencia concreta (e.g. habilitación del habla/escucha llamada a los distintos contactos listados; comentarios internos en relación a la información que le transmite los contactos, etc.)." denominación de la información actuación CRA" "¿Es susceptible de ser proporcionada como respuesta al ejercicio del derecho de acceso del interesado? "Únicamente deberán facilitarse como parte del derecho de acceso los registros de las actuaciones relacionadas directamente con el solicitante del derecho y no así el resto de las comunicaciones con otros usuarios autorizados o contactos proporcionados por éste. Asimismo, tampoco deberá facilitarse al solicitante cualquier información o análisis sobre la actuación del operador, en la medida en la que se trata de un tercero distinto del propio interesado que hubiera ejercido el derecho de acceso"*

- Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física: Las actuaciones de un operador, que incluye interacción con el usuario o los contactos designados por éste, suponen la obtención de información sobre dichos interesados.", "*descripción extendida. Los contactos a los que el operador de Securitas Direct trata de localizar no contestan*", "*denominación de la información "actuación CRA-comunicando. ¿Es susceptible de ser proporcionada como respuesta al ejercicio del derecho de acceso del interesado*? No obstante, únicamente deberán facilitarse como parte del derecho de acceso los registros de las comunicaciones relacionadas con el solicitante del derecho y no así el resto de las comunicaciones con otros usuarios autorizados.

- *Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física*": *Las actuaciones de un operador, que incluye interacción con el usuario o los contactos designados por éste, suponen la obtención de información sobre dichos interesados*.", *denominación de la información*, "*actuación CRA-salta buzón de voz*" *Es susceptible de ser proporcionada como respuesta al ejercicio del derecho*

de acceso del interesado? No obstante, únicamente deberán facilitarse como parte del derecho de acceso los registros de las comunicaciones relacionadas con el solicitante del derecho y no así el resto de las comunicaciones con otros usuarios autorizados."

-Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física": *Las actuaciones de un operador, que incluye interacción los contactos designados por el usuario, suponen la obtención de información sobre dichos interesados, denominación de la información "actuación CRA-operador consigue hablar con contacto" o "Actuación CRA-palabra clave incorrecta", y actuación CRA-LOCSIN-localizado* sin palabra clave con "descripción extendida: el contacto no recuerda la palabra clave para acreditar la identidad y cerrar la incidencia ""*¿Es susceptible de ser proporcionada como respuesta al ejercicio del derecho de acceso del interesado*?": "*No obstante, únicamente deberán facilitarse como parte del derecho de acceso los registros de las comunicaciones relacionadas con el solicitante del derecho y no así el resto de comunicaciones con otros usuarios autorizados*."

- Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física": Estos logs proporcionan información en relación con las actuaciones de un operador, esto es, la verificación de que efectivamente sigue los procesos internos de Securitas Direct a estos efectos", "*descripción extendida: Visualización de las palabras clave por parte del operador en caso de que haya un contacto con el usuario a efectos de identificación*.", denominación de la información "*operator viewed codewords on demand*", *Es susceptible de ser proporcionada como respuesta al ejercicio del derecho de acceso del interesado*? "*Sin perjuicio de que se trate de un dato personal, no debería proporcionarse al interesado en la medida en la que afecta a una tercera persona distinto del ejerciente del derecho de acceso*."

- Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física": "Las actuaciones de un operador, que incluye interacción con el usuario, suponen la obtención de información sobre el interesado", descripción extendida: "se contacta con el usuario", denominación de la información: "*Service Req.: ***NÚMERO.1*", *¿Es susceptible de ser proporcionada como respuesta al ejercicio del derecho de acceso del interesado*?

- Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física": *Información relativa a un operador de carácter procedimental e interno de Securitas Direc*t, "*descripción extendida*" *Matrícula interna del operador que está actuando una incidencia concreta", denominación de la información: ACCESO REGISTRADO: El usuario* ******USUARIO.1*** *accedió a la ficha del cliente, En su caso podría ser considerado un dato personal del propio operador y, por tanto, no sería susceptible de ser trasladado al interesado ejerciente del derecho de acceso*."

- Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física": *En principio las pruebas y verificaciones rutinarias que deba hacer el técnico de Securitas Direct no proporcionan ninguna información sobre el usuario salvo que sean específicamente solicitadas por dicho usuario, descripción extendida: "El técnico realiza las comprobaciones reglamentarias para asegurar el funcionamiento correcto de los sistemas. A petición del cliente puede modificar algún parámetro del propio sistema (e.g. sonido, tiempo, sensores, etc.), denominación de la información: Pruebas y verificaciones obligatorias como parte del mantenimiento de la instalación". ¿Es susceptible de ser proporcionada como respuesta al ejercicio del derecho de acceso? Si el técnico introduce modificaciones o configuraciones específicas*

en el dispositivo por petición del usuario, dichos parámetros sí serían considerados como datos personales que deberán ser entregados al interesado."

-" *Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física*": *El registro de actuaciones del usuario supone la obtención de información personal sobre el mismo*", "*descripción extendida cancelación de la alarma por ser introducidos los códigos del usuario*", "*denominación de la información: códigos del usuario*", "*Es susceptible de ser proporcionada como respuesta al ejercicio del derecho de acceso del interesado?, SÍ."*

- "*Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física*": El registro de actuaciones relativas a una intrusión real, en caso de haberse captado una imagen de la intrusión proporciona *información personal", descripción extendida: línea de log que hace referencia a la imagen captada por los sistemas al detectar una intrusión real. Denominación de la información "VIDEO-VID" ¿Es susceptible de ser proporcionada como respuesta al ejercicio del derecho de acceso del interesado?" no debe proporcionarse al solicitante del derecho de acceso información relativa a las imágenes captadas en la medida en la que ducha información trata sobre un interesado distinto del ejercicio del derecho de acceso*"

- "*Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física*": *el registro de actuaciones del usuario supone la obtención de información personal sobre el mismo", descripción extendida: evento inyectado servicio desde la aplicación por parte del usuario- conexiones desconexiones remotas. Diversas peticiones efectuadas desde el terminal móvil del usuario", "denominación de la información central seguridad prioridad baja*"

- "*Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física*": *el registro de situaciones que puedan afectar al usuario como la comunicación de un corte de la corriente eléctrica supone la obtención de información personal sobre lo mismo", "descripción extendida: en este caso se informa a cliente por medio de un correo electrónico de un* ***(...)*** *por corte de corriente de su alarma", " denominación de la información corriente eléctrica auto".*

-Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física": *el registro de actuaciones del usuario supone la obtención de información personal sobre el mismo", "descripción extendida: des(...) por cliente app web en remoto", " denominación de la información códigos de usuario".*

-Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física": *el registro de actuaciones del usuario supone la obtención de información personal sobre el mismo", "descripción extendida: confirmación de* ***(...)*** *externo total, " denominación de la información central seguridad prioridad baja*

En el **ANEXO II**, titulado "*ESTUDIO GENERAL DE LA CONSIDERACIÓN DE DATO PERSONAL DE CADA LOG*", (pág. 53 al final) se procede a la realización del análisis, "*de forma general*", y "*sin aplicación específica a un interesado concreto*", de la consideración como dato personal de las líneas de log genéricas que normalmente pueden ser utilizadas en los sistemas de Securitas Direct durante el desarrollo de su actividad.

"*No se han analizado aquellas líneas de log no derivadas de forma directa de los servicios de sistemas de seguridad proporcionados por Securitas (i.e. logs con denomina-*

ción: FR0 a FSZ; ROF y ROI)". Asimismo, tampoco han sido objeto de estudio aquellas líneas de log que, de conformidad con la información facilitada por Securitas, no tienen aplicación práctica a fecha de redacción del presente informe: IAC, ICA, PID, PDD, TLL y TWC"

El cuadro contiene la identificación de los logs en base a tres columnas.

-La primera columna incluye la "*(...) de la señal"*, por orden alfabético, que suele comprender un código de tres letras mayúsculas, que se "*describe*" en la segunda columna con una descripción general, usualmente en inglés, algunas claves como *FG* ,*SK masking*", *OPDI Shutter*, *Sent when CP detects RX failure in FG*, que luego se refieren en *la tercera columna: "descripción extendida proporcionada por SD*"

Se observa que claves que aparecen en el documento entregado al reclamante el 14/12/2021, en el campo "*Signal clasification*", como *RPT*, IGC no figuran en esas claves del Anexo II. Además, se encuentran códigos como el *TAC* que figura entregado al reclamante como dato y en anexo II se indica que no es dato personal.

También se hallan claves (TTR o TTS) que figura NO en ¿se considera dato personal?, que indica" *Esta línea de log, si bien traslada información sobre un posible sabotaje en los sensores no proporciona información directamente sobre el interesado ni, tampoco, sobre un patrón de conducta o un análisis de su personalidad. Por lo tanto en la medida en la que no se traslada información directa sobre un atributo del interesado ni Securitas Direct pretende analizar un patrón de conducta o influir sobre él en modo alguno, la información facilitada por la línea de log analizada no debería ser considerada como dato personal. En este sentido, se trata de un descriptivo del proceso técnico e interno de Securitas Direct"*

Algunas claves se relacionan con "*descripción extendida proporcionada por Securitas: realización de test de Securitas para verificar el estado del sistema FOG*", o en otra "*comprobación bajo el protocolo de actuación de Securitas Direct del estado del sistema FOG*", o "*nivel de cobertura de información **(…)** de panel*".

-La cuarta columna se titula: "*Vinculación de forma directa o mediante inferencia, a una conducta o información de una persona física*", en la que se introduce en unas líneas el razonamiento sobre esa cuestión, y que como consecuencia, da lugar a la información de la última columna, denominada "*¿Se considera dato personal*?" con si, o no. En el no, se puede asociar a: "*No se encuentra vinculación directa con información de un cliente en la medida en que se trata de señales informativas de carácter técnico y no se proporciona información en relación con ninguna característica, patrón de conducta u otra información de una persona física*."

2) Resume sus actuaciones en el tiempo, tras la obtención del citado informe, al objeto de valorar su actuación en el ejercicio del derecho del reclamante.

a) -26/02/2021, respuesta al burofax recibido el 9/02/2021, en "*el que se nos requieren los "logs" generados por el sistema de alarma para el período solicitado. En este escrito se facilitan los "logs" que consideramos que son datos personales, tal y como son registrados en nuestros sistemas, y debido a su configuración se incluye una descripción del mismo a fin de hacerlos inteligibles, algo que excede de lo que podríamos haber hecho. Este escrito lo recibió la parte reclamante el 3/03/2021. Ver págs. 26 a 31 de la documentación obrante en el expediente*. "

-*18/05/2021,* como consecuencia de la recepción del expediente E/04382/2021 (traslado de la reclamación en el procedimiento de ejercicio de derechos de la luego: TD/ 00167/2021), *"se vuelve a remitir al reclamante, por correo electrónico, la misma respuesta facilitada el 26/02/2021, esto es, los "logs" que se han considerado que son datos personales. de conformidad con el informe realizado.*

-14/12/2021, se vuelve a remitir al reclamante, como consecuencia de la resolución del Recurso de Reposición Nº RR/00658/2021 contra la TD/00167/2021, la misma información aportada en los escritos de fechas 26/02 y 18/05/2021. "*En esta ocasión en un formato diferente, por evento, en lugar de agregado, para facilitar la comprensión de éstos. Ver págs. 153 a 160 de la documentación obrante en el expediente*."

"*Se han enviado en dos formatos diferentes, agrupados por evento e individualizados, tal y como se registran en los sistemas por fecha de evento", "incluyendo información complementaria que permitiese al reclamante entender la misma".* Se incluye una descripción del significado del evento. "*Los registros generados por los sistemas han sido aportados tal y como se generan en éstos, y aun así se han hecho esfuerzos que incluso excedían de la obligación de mi representada, para que el receptor pudiera entender el evento que reflejan*."

3) "*SECURITAS DIRECT en escrito presentado a la Agencia de 18/06/2021, páginas 106 y 107 del expediente* (dentro de la TD/00167/2021) *ponía de manifiesto que generó logs hasta las 20:09 h del día 27/11/ 2015, hora y fecha en la que se produjo la intrusión en el domicilio del reclamante y durante la cual dicho sistema de alarma quedó completamente inutilizado a partir de esa fecha no pudo generar más logs."*

En relación con la memoria interna del dispositivo, también la reclamada puso de manifiesto en su escrito de 18/06/2021 que *"tras el análisis de la memoria interna de la alarma instalada solo constaba un log generado para ese marco temporal el cual constaba en nuestro burofax de 26/02/2021".*

Considera, que *"en diciembre de 2021 había ejecutado el ejercicio de derecho de acceso a datos realizado por el reclamante de manera reiterada*"" *en dos formatos diferentes, agrupados por evento e individualizados, tal y como se registran en los sistemas por fecha de evento. Se incluye una descripción del significado del evento".*

4) "*La Agencia considera en el acuerdo de inicio, que, sin perjuicio de haber enviado al reclamante los registros y señales solicitados y generados que son datos personales, "cabría la posibilidad de haber proporcionado todos los "logs" a la Agencia, hasta el mínimo detalle y marcarlos como confidencial en el caso de que se opusiera a una eventual difusión*".

Pone en tela de juicio la posibilidad de atender de esa forma el derecho de acceso, al no reflejarse en norma alguna, considerándolo un acceso indirecto a la información a través de la AEPD, aun cuando estos no sean datos de carácter personal. Indica que ha enviado al reclamante los datos personales obrantes en la información solicitada tras su conclusión de su informe jurídico de análisis sobre logs, "*dentro del periodo solicitado*", "*en dos formas diferentes*", y en tres ocasiones.

5) Los que no considera datos personales, son "*logs de carácter técnico, señales informativas, registros descriptivos de procesos internos y técnicos, configuraciones*

de dispositivos o información estadística, información que contiene procesos técnicos internos de SD cuya revelación a terceros implicaría en muchos casos la comunicación de nuestro know how".

"*Queriendo dar cumplimiento a lo planteado por la Agencia en el escrito del acuerdo de inicio*", adjunta:

DOCUMENTO 2, tabla Excel, que *"contiene* **todos** *los registros emitidos por el sistema de alarma sobre el que recae la petición" ordenados cronológicamente",* de modo que figuran secuencialmente, según se producen: *"En color verde son datos personales de acuerdo con el informe.", y los de "color rojo, aquellos que no lo son, por ser técnicos y confidenciales quedando sometidos a la normativa de secretos industriales, pudiendo ser utilizados solo por la Agencia".*

*"Del total de los logs recogidos del sistema de alarma del reclamante para el período solicitado- 412 registros- ya se han puesto a disposición del reclamante un total de 273 registros***."**

Las hojas Excel que aporta son similares al formato proporcionado al reclamante el 14/12/2021, *y "reflejan los registros como son, y aparecen registrados en los sistemas*."

Aparecen en ocasiones logs de misma fecha y hora que se aprecia que son considerados dato personal y otro que no, figurando con distintas claves de la "*(...) del evento*", distinguidos en rojo los considerados no datos personales, ejemplo 27/11/2016 20:09:47. Incluso figuran dos logs en rojo, no datos personales, a misma fecha y hora.

DOCUMENTOS 3, y 4, tablas Excel, relacionadas de algún modo con el 2. Reúnen en forma separada, los que son logs de datos personales (3), y los que no (4), también en los mismos colores que el documento 2. El documento 3 contiene, según la reclamada, "*los registros emitidos por el sistema de alarma sobre el que recae la petición. Este documento fue facilitado al reclamante mediante burofax de 14/12/2021 y refleja los registros como son, y aparecen registrados en los sistemas*." Aparece ordenado cronológicamente siendo la primera fecha 27/11/2015, 20h 09, y ese mismo día hay diversos registros, el ultimo de 20:17:07, y el siguiente pasa a 4/12/2015, 11:05:04

El documento 4, con los logs técnicos que no son considerados por la reclamada de carácter personal, comienzan en el registro el 26/11/2015, y la siguiente fecha es 27/11/2015, siendo el primero de 9:39:43, y el ultimo de 20:11:34. Pese a la manifestación de la reclamada de que la alarma fue destruida el 27/11/2015 a las 20:09, figuran logs (sólo técnicos) entre el 28/11 a 4/12/2015, excepto del 29/11. Cada día se reflejan cuatro logs, con el termino común de "*GTI MISSING TEST*", (Log que informa de la pérdida de comunicación con el dispositivo) hasta 4, uno por día. El día 4/12/2015 figura GTI: incidencia cancelada, cliente ya existe en cola manual 14, sin clave alguna en descripción ni en clasificación de señal.

Resume que los logs asociados al sistema de alarma del reclamante que "*no consideramos datos de carácter personal", son de carácter técnico, señales*

informativas, registros descriptivos de procesos internos y técnicos, configuraciones de dispositivos con información estadística, información que contiene procesos técnicos internos de Securitas Direct cuya revelación a terceros implicaría en muchos casos comunicación de nuestro "know now" con el perjuicio que podría suponer de forma directa y respecto a la seguridad de todos sus clientes de forma indirecta".

6) -Sobre la cuantía de la sanción del acuerdo de inicio:

a) Respecto al 83.2.a) del RGPD, considera que no se puede tomar 2017 como fecha de inicio temporal como un agravante dado que la primera tutela de ese año fue inadmitida por la Agencia en base a que no se consideraban los logs datos de carácter personal.

"*Sobre el tiempo transcurrido en conexión con el daño ocasionado y la seguridad de las instalaciones, el reclamante no ha acudido a la vía judicial, siempre a la vía administrativa de protección de datos, habiendo utilizado la reclamada las "palancas legales" que a su derecho convenían y se ofrecían a su alcance, lo que no puede ser objeto de penalización*". Se dio respuesta al acceso solicitado antes del inicio del procedimiento sancionador hasta en tres ocasiones.

b) Respecto al artículo 83.2.b) del RGPD, "*actuación negligente", basada en que el reclamante consideró en octubre de 2021, de forma subjetiva, que todavía no se había cumplido con su petición, considera que no es una aproximación del todo cierta, ya que había dado cumplimiento al ejercicio de derecho de acceso en dos ocasiones, en febrero y mayo de 2021*."

"Lo que ocurrió en diciembre de 2021, debido a que esta parte, dicho sin ánimo de ofender, ya no sabía cómo cumplir de nuevo con el ejercicio de derecho, procedió a presentar al reclamante la misma información ya presentada en febrero y mayo de 2021 pero con un formato diferente (si se cotejan ambos documentos, se puede comprobar que la información de ambos es la misma). Además, en ninguna de las resoluciones emitidas por la Agencia se planteó la posibilidad de aportar a la misma la totalidad de los logs marcando los confidenciales, "*como si se ha venido a hacer en este acuerdo de inicio, sin determinarse qué artículo de marco normativo vigente contemplaba tal posibilidad". La mera y reiterada disconformidad del reclamante, no debe ser, por si solo, la causa que motiva la infracción o, en su defecto, la imposición de una multa*"

7) En cuanto a la afirmación que hay una vinculación de la actividad del infractor con el tratamiento de datos en el marco de la prestación de sus servicios, considera que precisamente, lo que se trata en este caso es si los logs generados por el sistema de alarma son o no datos personales, algo, que tras el informe que ha aportado como documento 1 permite diferenciar que unos sí lo son, que han sido entregados en varias ocasiones al reclamante y otros que no lo son.

8) Considera que existen acreditadas una serie de atenuantes que permitirían aplicar "*un grado menor al propuesto en el acuerdo de inicio*". Dichas atenuantes serían:

a) No se puede calificar de no haber atendido las solicitudes de ejercicio del derecho como infracción grave del artículo 72.1.k) del RGPD, dado que se dio acceso en

febrero y mayo de 2021, en parte, pero no en todo, el derecho si había sido atendido, "*sería una atenuante para aplicar sobre el referido artículo y considerarla como una infracción leve que encajaría en el artículo 74.c de la LOPDGDD*.", que indica:

"*Se consideran leves y prescribirán al año las restantes infracciones de carácter meramente formal de los artículos mencionados en los apartados 4 y 5 del artículo 83 del Reglamento (UE) 2016/679 y, en particular, las siguientes:*

c) No atender las solicitudes de ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, salvo que resultase de aplicación lo dispuesto en el artículo 72.1.k) de esta ley orgánica."

-Existe diligencia debida, "*con el único fin de cumplir con la petición del reclamante y del propio alcance del derecho de acceso a sus datos de carácter personal, haciendo un esfuerzo, entre ellos, económico se puso en manos de un tercero independiente de reconocido prestigio, a los efectos de disgregar, de entre todos sus logs, cuáles son los considerados como datos de carácter personal (según la definición de "dato de carácter personal") y cuáles no lo son, y que son secretos comerciales"*

-Concurre buena fe, como se demuestra en que "*se ha dado cumplimiento al derecho hasta en tres ocasiones*", "*una vez tuvo claro el criterio de que logs son datos personales y cuales no*", dando siempre la misma información. En función del criterio de la AEPD, en base al acuerdo de inicio, se han aportado todos los logs.

-Considera que la actuación del reclamante expresando su insatisfacción "*con lo que de forma subjetiva considera que son los logs y como deben venir representados sobre el papel, no puede ser condicionante adicional para que se proponga imponer una multa que entienden desproporcionada, sino lo contrario, debería ser motivo para que la penalización sea menor a la propuesta*."

Solicita se tenga por cumplido el ejercicio del derecho con todos los logs ahora aportados.

SÉPTIMO: Con fecha 23/11/2022, se acordó iniciar un periodo de practica de pruebas.

1-Se dieron por reproducidos a efectos probatorios la reclamación interpuesta por el reclamante y su documentación, los documentos obtenidos y generados durante la fase de admisión a trámite de la reclamación, y el informe de actuaciones previas de investigación que forman parte del procedimiento TD/00167/2021.

Asimismo, se da por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio del procedimiento sancionador referenciado, presentadas por la reclamada, y la documentación que a ellas acompaña.

2-Por guardar relación con la petición originaria, se incorporan como prueba al procedimiento:

a) La documentación aportada por el reclamante y la obtenida y recogida de la reclamada en cuanto a la tutela de derechos 1564/2016, resuelta el 8/09/2016, así como documentación de ambas partes producida en su tramitación.

b) La documentación aportada por el reclamante y la obtenida y recogida de la reclamada en cuanto a la tutela de derechos 1593/2017, así como documentación de ambas partes producida en el recurso de reposición resuelto el 2/01/2018, RR/779/2017, y los documentos que forman parte de dichos expedientes.

c) La documentación aportada por el reclamante y la obtenida y recogida de la reclamada en cuanto a la tutela de derechos resuelta por la Agencia TD/00167/2021, los trámites con ella relacionados incluidos el traslado de la misma a la reclamada E/4382/2021, y la admisión a trámite y gestión y tramitación de la misma, así como el posterior recurso de reposición resuelto RR 658/2021 de 27/10/2021.

d) La Sentencia de la Audiencia Nacional (AN), sala de lo Contencioso administrativo sección primera, de 23/07/2019, recurso 146/2018, y por relación, el auto del TS sala de lo Contencioso administrativo sección primera, de 29/05/2020 número de procedimiento 378/2020 de admisión a trámite del recurso de casación de la reclamada, del que luego desistió, figurando como tal, en el auto del TS, recurso 378/2020 de 15/09/2020 en el que se indica que el representante de Securitas "*presentó escrito el 24/07/2020, desistiendo del recurso preparado*", declarando "*terminado el recurso por desistimiento*", y comunicado a la AEPD en escrito del Letrado de la Admón. de Justicia de 29/10/2020, constando como objeto asociado del expediente: *PS 2181 22 san y ts.*

3.Se solicita a la reclamada que en el plazo de quince días, aporte o informe de:

3.1-Aporte copia de los términos contenidos en el ejercicio del derecho de acceso formulado por el reclamante el 2/02/2021.

Se recibe respuesta el 30/12/2022.

En primer lugar, subraya que el procedimiento que se le sigue es por infracción del artículo 58.2.c) del RGPD:

"*ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado en virtud del presente Reglamento*".

Para ello, considera relevante la distinción entre los logs que tienen la condición de datos personales o los que se refieren a "*aspectos simplemente relacionados con el funcionamiento de los sistemas de alarmas comercializados, cuya revelación podría generar una vulneración de su derecho al secreto comercial, y la puesta en riesgo de su funcionamiento futuro, al ponerse en conocimiento de terceros ajenos a la organización*".

Estima que algunas de las cuestiones que se plantean en pruebas por el instructor, "*no guardan relación con el objeto del procedimiento, sino más bien con el adecuado funcionamiento del sistema de alarma contratado*". La información que proporcionará se circunscribirá "*al objeto del procedimiento", sobre si dio "adecuado cumplimiento a*

lo acordado por la AEPD", así como "*si las informaciones que no facilitó al reclamante, en aplicación de lo ya invocado en las alegaciones, contenían o no datos personales de aquel, sin que entiendan que proceda facilitar información relacionada con el comportamiento en relación con los hechos acaecidos en el domicilio del reclamante*".

Aporta burofax del reclamante sobre ejercicio de derecho firmado el 2/02/2021, con envío 9/02/2021, anotado a mano: recibí 10/02/2021.

El escrito parte de la base de que "e*l 4 de diciembre del 2015 la vivienda sufrió un asalto y robo sin que el sistema de alarmas señalado se activara, lo detectara ,emitiera y recibiera la señal de alarma debida, siendo gravemente dañada la centralita y resultando que la primera noticia que Securitas Direct España tuvo fue la llamada de mi representados, informando sobre ella. El sistema de alarma venía sufriendo determinadas incidencias con ciertos problemas de conectividad*", para pasar a valorar la exigibilidad al reclamante por Securitas de los gastos de reposición de la centralita, tras el incidente, la suspensión del servicio desde el 23/12/2016, al parecer por corte debido a impago de gastos de reposición, indicando los titulares que dieron por resuelto el contrato y exige a su vez una serie de devoluciones de cantidades en diversos conceptos.

A renglón seguido, reitera la petición de la información obrante en servidores relativa a los registros y señales enviadas por el equipo de alarma entre los días 26/11 y 18/12/2015. Le menciona la sentencia de la AN, su firmeza y requieren su cumplimiento.

3.2-Copia del contrato suscrito con el reclamante en el que figuren las condiciones generales y particulares del servicio y la información del ejercicio de derechos, incluyendo la cláusula 14 de política de privacidad a la que alude en su ejercicio de derechos de 7/04/2017.

Copia de la instrucciones entregadas al usuario, por escrito, del funcionamiento del servicio, informándole de las características técnicas y funcionales del sistema y de las responsabilidades que lleva consigo su incorporación al mismo.

Se aporta, como DOCUMENTO NÚMERO 3 contrato número ******NÚMERO.2*** celebrado el 30/07/2014 con el reclamante (en adelante, el "*Contrato*"), incluyendo, en las páginas 9 y 10 del documento, la cláusula 14, referida a protección de datos personales.
Del contrato de "*servicio de seguridad*", cabe referenciar:

Condiciones particulares:

-Se recogen datos personales: e mail, nombre, apellidos, dirección y teléfono.
-El servicio incluye la instalación, mantenimiento y explotación de centrales de alarmas.

Condiciones generales

-*"2. descripción y el alcance de los servicios objeto del contrato, A) servicio de instalación y mantenimiento",* figura que la instalación comprenderá los elementos y componentes contemplados en las condiciones particulares del presente contrato y Securitas Direct prestará un servicio de mantenimiento básico que incluye para el cliente: los servicios de comprobación remota del funcionamiento de todos los componentes (chequeo técnico según normativa vigente).

También se refiere a la definición y distinción de avería, "*el daño que impide el funcionamiento adecuado de un sistema de seguridad para cumplir el fin para el cual se halla destinado*" y "*problema técnico*" "*aquella incidencia que implique la necesaria intervención por SECURITAS DIRECT para comprobación, sea o no presencial, y que, en ningún caso, impida el total funcionamiento del sistema de seguridad del CLIENTE*."

En el punto B) se refiere el Servicio de conexión a central receptora de alarmas.

-en 6: "*obligaciones del cliente*", se establece entre otras:

a) "*deberá, en todo caso, conectar el sistema de alarma cada vez que pretenda evitar el acceso de personas no autorizadas al lugar y, especialmente, cada vez que el lugar quede abandonado y sin vigilancia. La acreditación de la conexión de la alarma corresponde, en todo caso, al CLIENTE. Por ello, la contratación del servicio de todos los códigos controlados será requisito para poder acreditar de manera fehaciente el estado de conexión de la alarma. Si no se tiene contratado por el CLIENTE el servicio que permite acreditar que la alarma está conectada, a él le corresponde acreditar la conexión porque la conexión es un acto que deriva de la actuación de quien contrata el servicio y no de SECURITAS DIRECT."*

o) Notificará en todo momento las posibles variaciones de personas de contacto o teléfonos para el caso de que sea necesario localizarle."

"*10. DERECHOS SOBRE LA INSTALACIÓN Debido a que la rápida evolución tecnológica convierte en obsoletos los sistemas de control y comunicación, SECURITAS DIRECT mantendrá la propiedad del sistema de seguridad instalado para poder actualizar el software y los componentes del mismo, con el único fin de prestar los servicios de seguridad más avanzados.*

- 14. POLÍTICA DE PRIVACIDAD

A) INFORMACIÓN EN MATERIA DE PROTECCIÓN DE DATOS AL CLIENTE: Los datos personales proporcionados por el CLIENTE a SECURITAS DIRECT, así como cualquier otro dato que pudiera facilitarse a lo largo de la relación contractual, serán incluidos en un fichero, cuyo responsable es SECURITAS DIRECT ESPAÑA, SAU…, única destinataria de los datos, con la finalidad principal de llevar a cabo la relación contractual, la gestión propia de la actividad, el mantenimiento, desarrollo y control de la relación contractual. "

"*C) TRATAMIENTO DE IMÁGENES Y/O SONIDOS OBTENIDOS A TRAVÉS DEL SISTEMA DE SEGURIDAD CUANDO EL EQUIPO INCORPORE SISTEMAS DE FOTODETECCIÓN. - Al verificar un salto de alama por parte de SECURITAS DIRECT*

"SECURITAS DIRECT a través de su Central Receptora de Alarmas captará y grabará imágenes y/o sonidos a través de los dispositivos de seguridad instalados en los lugares objeto de protección del CLIENTE, de conformidad con el artículo 48 del Reglamento de Seguridad Privada, es decir, verificando a través de todos los medios técnicos a su alcance las alarmas recibidas y una vez agotada dicha verificación si fuera procedente, transmitirá dichas imágenes y/o sonidos obtenidos con motivo del salto de alarma tratado a la autoridad policial o judicial competente.

SECURITAS DIRECT adquiere la condición de Responsable del fichero de gestión de sistemas de videovigilancia con acceso a las imágenes del CLIENTE, debido a su condición de persona física y que el sistema de seguridad con acceso a imágenes se efectúa en su domicilio particular. No tendrá la consideración de intromisión ilegítima en el derecho al honor, a la intimidad personal y a la propia imagen, la captación, reproducción y tratamiento de las imágenes y sonidos con motivo de un salto de alarma generado por el elemento de protección por imagen instalado y tratado a través de la Central Receptora de Alarmas de SECURITAS DIRECT.

El CLIENTE sólo podrá tener acceso a información sobre cualquier incidencia o grabación realizada con motivo de un salto de alarma, enviando solicitud escrita a través de los medios que así lo permitan indicados en la cláusula 20 de las condiciones generales, en la que deberá constar la identidad del titular del contrato acompañando fotocopia de su DNI, CIF, NIE o pasaporte en vigor, así como la fecha, hora y lugar en el que presumiblemente sucedió la grabación. SECURITAS DIRECT, custodiará las grabaciones obtenidas como consecuencia de los saltos de alarma generados por el sistema de seguridad instalado, y cumplirá con sus obligaciones de conservación, inutilización y destrucción."

El citado contrato incluye en su Anexo I, "*el proyecto de instalación*", con las características del estudio de emplazamiento y riesgos, con la propuesta del diseño de seguridad y con los elementos configurados en el plan de instalación, así como los elementos y zonas de riesgo protegidas a través de verificación de señales de alarma por audio, imagen-video, y presencial.

El Anexo II, refiere el: "*PLAN DE ACCIÓN*", en que figuran entre otras:

-*"lista de contactos*", cuatro personas identificadas por nombre y apellido, ordenadas por número creciente, todos con "*llaves*". El primero, el reclamante, como "*cliente*", la persona "*que firma el contrato, propietaria del sistema de alarma*" asociado a dos teléfonos. Las otras tres: "*relación con el abonado*": "*familiares*" con un teléfono.
Las cuatro personas figuran en el "*plan de acción estándar*" en el cuadro, ordenados como "*contacto*" de 1, el reclamante, a 4.

-las palabras clave o "*maestra*" del cliente, la clave coacción y la clave SECURITAS.

- Dentro del Plan de acción, figuran las *"CONDICIONES DEL SERVICIO DE EXPLOTACIÓN DE CENTRAL RECEPTORA DE ALARMAS" destacando entre otros:*

-"CLIENTE: Persona física/jurídica que firma el CONTRATO, que es propietaria del sistema de alarma descrito en el citado CONTRATO y que es poseedor de la palabra clave maestra. El CLIENTE podrá tener en cualquier caso la condición de usuario"

"*USUARIO: Persona física a la que el CLIENTE autoriza el acceso al inmueble y al uso del sistema de alarma, poniendo a su disposición los medios de conexión y/o desconexión del mismo.*

"PERSONAS DE CONTACTO: Persona física que puede coincidir o no con el CLIENTE del contrato y que es poseedora de la palabra clave maestra."

2. PALABRA CLAVE Constituye un dato necesario para la prestación del servicio contratado. Su poseedor queda obligado a mantener la confidencialidad de la misma, no debiendo transmitirla a terceras personas.

Tipos de Palabra Clave:

- Clave SECURITAS: Identifica a SECURITAS DIRECT y debe facilitarse por la misma en cualquier comunicación telefónica con cualquiera de las personas descritas en apartado 1 del presente documento.

- Clave MAESTRA CLIENTE: Identifica al CLIENTE y a los contactos principales. Debe ser proporcionada por estos cuando contacten con SECURITAS DIRECT telefónicamente. Permite y da acceso a todo tipo de gestiones y modificaciones, ya sean administrativas (contrato, plan de acción, etc.), u operativas (verificación de saltos de alarma).

- Clave COACCION: En la llamada de verificación ante un salto de alarma debe facilitarse a SECURITAS DIRECT, por quien se encuentre en el inmueble ante una situación de peligro real para su integridad física y/o patrimonial

3. PROCEDIMIENTO DE VERIFICACIÓN ANTE SALTO DE ALARMA

La Central de Alarmas de SECURITAS DIRECT ejecutará el pertinente proceso de verificación de los saltos de alarma registrados por el sistema de seguridad instalado, a través de los medios a su alcance contratados o dispuestos por el CLIENTE, tales como, habla escucha, imagen y/o llamada al teléfono fijo del inmueble, llamando a los teléfonos de contacto facilitados por el CLIENTE en el presente documento y, en su caso, enviando al Servicio Acuda acompañamiento a Policía o al Servicio Acuda para verificación Full Service, en el caso de que el CLIENTE hubiera contratado este último servicio.

SECURITAS DIRECT cursará el correspondiente aviso a las Fuerzas y Cuerpos de Seguridad (en adelante, "F.C.S.") sólo en el supuesto de quedar acreditada la realidad del hecho generador del salto de alarma, una vez realizada la verificación de forma

válida, a través de los medios existentes, de acuerdo a la normativa vigente en materia de Seguridad Privada.

A efectos de iniciar el protocolo de actuación, se considera salto de alarma las señales recibidas en la Central Receptora de Alarmas procedentes de la captación de los elementos de detección de intrusión, del botón SOS, del botón antiatraco, y código de coacción.

-En el contrato existe un apartado que recoge el protocolo en casos de saltos de alarma*, "procedentes de la pulsación del botón SOS, botón antiatraco, código de coacción y cuando se facilite la palabra clave de coacción.",* en caso de "sin *desconexión de usuario":* verificando *"mediante el acceso al módulo habla-escucha del sistema y/o llamada al teléfono fijo del inmueble, siempre que se disponga de este último. Si a través de estos medios:*

- Se obtiene contestación: se procederá a identificar a la persona con la palabra clave maestra o de contacto. Si la palabra clave es correcta, se proporcionará al usuario las instrucciones técnicas precisas para que desconecte el sistema.

- Si la palabra clave no es correcta o no se obtiene contestación: SECURITAS DIRECT procederá a dar cumplimiento a los procedimientos de verificación previstos en la normativa de Seguridad Privada vigente así como a utilizar los medios complementarios de verificación tal como proceder a la llamada de comprobación a los CONTACTOS PRINCIPALES y/o OPERATIVOS establecidos, y/o al Vigilante de Seguridad y/o F.C.S. si se tratara de una alarma real confirmada. En todo caso, la decisión de cursar el aviso corresponderá exclusivamente a SECURITAS DIRECT.

En caso de que se diera "*desconexión de usuario*", es el supuesto en que salta la alarma, y en un tiempo inferior a 20 segundos (desde el salto de alarma), se recibe señal de desconexión en la CRA. En este caso, "*se emitirá de modo automático una locución grabada a través del módulo habla escucha del sistema, en la que se informará al cliente de la señal recibida así como de la ejecución de la desconexión por el usuario o persona autorizada y de la cancelación de la incidencia"*

"En el supuesto de que la señal de desconexión se reciba en un tiempo superior al indicado en el párrafo anterior, SECURITAS DIRECT procederá a verificar el salto de alarma mediante el acceso al módulo habla-escucha del sistema y/o llamada al teléfono fijo del inmueble, siempre que se disponga de este último, para realizar las comprobaciones que entienda oportunas según su diligencia como Empresa de Seguridad y que se hallen ajustadas a la normativa de Seguridad Privada aplicable."

En documento ANEXO III*" certificado de instalación y conexión",* se indica que "*los elementos y dispositivos de seguridad instalados al cliente se corresponden con el grado **2** de seguridad, establecido en el artículo 2 de la orden INT/316/11 de 1/02 y disponen de la correspondiente homologación de acuerdo a las características establecidas en las UNE-EN 50130, 50131, 50132, 50133, 50136 y en la Norma UNE CLC/TS 50398*

- En un cuadro, figura el tipo de dispositivo de los elementos que forman el sistema instalado.

- Como DOCUMENTO NÚMERO 4, aporta el manual de usuario del sistema de alarma (en adelante, el "*Manual*") en su versión existente al tiempo de celebrarse el contrato con el reclamante. Destaca del mismo:

-Panel de control con transmisión GPRS: Comunicaciones GPRS ***(...)***, SMS, tarjeta SIM Securitas Direct incluida. Soporta transmisión de imágenes. Habla/ escucha alta sensibilidad**.** Único con intercomunicador personal portable *para pedir socorro. Pulsador SOS. Sirena interior. Admite hasta 32 interfaces de usuario control domótico*

-Lector de llaves/ llaves inteligentes: permite activar y desactivar fácilmente su alarma sin tener que memorizar complicados códigos. Se pueden activar distintos modos: día, perimetral…

-Detector de movimiento con Cámara color y flash desde nuestra central receptora podemos ver lo que ocurre en su hogar o negocio en caso de salto de alarma permiten tomar secuencias de imágenes flash incorporado para visión nocturna y disuasión

-Comunicaciones:" *supervisión de las comunicaciones mediante un test periódico*."

-Para la activación, cuenta con diversos modos cómo activado total al salir de su casa de modo que quedan protegidas todas las zonas de detección del sistema de seguridad, o modos parciales: que pueden ser activado modo día o activado modo noche o activado modo perimetral.

En descripción y uso de panel de control con teclado, se explican las diferentes funciones de los botones que figuran, desde la función SOS, caso de emergencia que se puede enviar a Securitas Direct con un avisador de luz que indica que se ha recibido correctamente la señal luminosa de cobertura del panel de control, "***(...)***", función de "*manos libres*" para recibir llamadas entrantes y que permite responder, llamadas al 112, y otra serie de funciones.

3.3-Descripción del funcionamiento del sistema de alarma contratado que se instaló en la propiedad del reclamante, composición de elementos (centralita del sistema de alarma ubicada en el domicilio, componentes de esta, panel de control, sensores o detectores de alarma que se comprenden en el sistema, kit de alarma u otros accesorios del sistema y conexión con la Central Receptora de Alarmas).

Se pide también que informen del sistema o vía de comunicación que utilizaba el dispositivo instalado en el domicilio del reclamante.

Señala que el manual describe en sus páginas dos y tres los elementos básicos del sistema de alarma

También en el contrato se incluyó en cuanto a elementos adicionales contratados:

Un mando a distancia, para conectar-desconectar la alarma.

Un flash sirena exterior, que se ubica en el interior de la instalación y suena cuando, por ejemplo, se activa la alarma.

Dos detectores magnéticos, dos detectores sísmicos (*aunque en el contrato figuran separados, son los mismos dispositivos, conocidos como "shocksensor", que detectan apertura, cierre y vibración, no recogen imágenes*".)

Un elemento de verificación por audio habla escucha, "(*Se encuentra en el interior del panel de control y es para realizar verificaciones de audio y escucha en caso de salto de alarma, también sirve para hablar con el cliente a través de la centralita)."*

Tres elementos de verificación por imagen fotodetector videosensor, (Detectores con cámara que reaccionan a los cambios de temperatura detectados por el movimiento, de tal forma que, si detectan movimiento estando conectados, disparan la alarma y recogen imágenes.)

Un detector perimetral exterior con imagen (Misma descripción que los fotodetectores pero de exterior)

Un lector de llaves inteligentes (*tag reader*) que es el dispositivo que se utiliza para conectar/desconectar la alarma. Que se relaciona con 6 tag (llaves inteligentes que se utilizan para desconectar la alarma pasándolas por delante del lector de llaves inteligentes.

"La única modificación respecto al estado inicial fue el cambio de los dos magnéticos/sísmicos por tres dispositivos volumétricos, que son detectores sin cámara que reaccionan a los cambios de temperatura detectados por el movimiento, de modo que si detectan movimiento estando conectados, disparan la alarma". Indica pues que tras el alta del servicio, en el momento de la intrusión existían tres fotodetectores, y tres volumétricos, además del resto de elementos ya señalados.

Remite a la información incluida en el manual para completar el funcionamiento del sistema.

"*En cuanto al sistema de conexión con la Central Receptora de Alarmas (en adelante, "CRA"), ésta se lleva a cabo mediante una tarjeta SIM integrada en el panel de control*."

3.4-a) Forma en la que se generan y almacenan los logs del funcionamiento del sistema de la alarma. Si además del funcionamiento o generación por la máquina, ¿se pueden crear logs por operarios de Securitas?, ¿en qué circunstancias.?

Manifiesta que "*el sistema genera y almacena registros derivados de:*

-Interacciones del cliente con el sistema de alarma, por ejemplo: conexión, desconexión.

-Verificaciones internas del sistema: ejemplo cobertura ***(...)****, y*

-Actuaciones del sistema de alarma en el desempeño de su función, por ejemplo salto de alarma."

"*En cuanto a la posible generación de nuevos logs por los operarios de SECURITAS DIRECT, es preciso indicar que el catálogo de logs que pueden generarse por la interacción del sistema instalado y la CRA es cerrado, es decir, no es posible la creación de nuevos logs distintos de los que el sistema permite generar. Por otra parte, obviamente, algunos de estos logs previamente configurados sí se generarán como consecuencia de la interacción del sistema con una actividad desarrollada por un operario o usuario autorizado de SECURITAS DIRECT, así como por el propio titular del sistema o las personas autorizadas por éste. No obstante, como se ha indicado, los mismos se encontrarían en el catálogo de los que es posible generar en el sistema y no presentarían ningún tipo de novedad respecto de los ya existentes, al ser ello imposible*."

b) Informen, si la centralita del sistema de alarma en sí, es capaz de almacenar registros o solo origina y envía señales, y qué señales o registros se originan y cuál sería el destino.

Respondió que:"*La centralita (panel de control) del sistema de alarma sí es capaz de almacenar registros, de hecho, alberga* ******NÚMERO.3*** *eventos los cuales se van borrando de manera cíclica, en función de los registros que se vayan generando y grabando continuamente. Según se van generando y grabando registros nuevos, se borran los más antiguos manteniendo un orden temporal de grabación y borrado siempre dentro de los ***NÚMERO.3 registros que puede albergar*."

Dentro de estos eventos registrados debe diferenciarse entre:

(i) *aquéllos que generan un log, copia de los cuales han sido facilitados en el documento Nº 2 de los aportados juntos con el escrito de alegaciones al Acuerdo de Inicio (*recogen mezclados logs técnicos junto a los considerados logs de datos de carácter personal, en orden secuencial de fecha y hora, con claves de: *"clasificación señal*", clave que se explicita en el ANEXO II de alegaciones al acuerdo de inicio junto a si se considera o no dato personal y porqué), la descripción, la descripción más amplia (llamada en la columna "***(...)***"), comentario, evento, extensión de evento, prioridad, zona.

(ii) y otros eventos meramente técnicos y relacionados con la interconexión producida para la remisión de los logs a la CRA de SECURITAS DIRECT (e.g. canal por el que se remite el log, conexión exitosa, acuse de recibo, etc.). Dado que los mencionados en el punto ii únicamente se refieren a la remisión y no a ningún tipo de actuación concreta, no generando un log, no formarían parte de lo solicitado por el Reclamante.

"*El destino de dichos registros es la CRA, si bien la información mencionada en el punto (ii) así como los logs que no reflejan un evento relevante relacionado con el funcionamiento de la alarma no se comunican y permanecen en la memoria interna de la centralita y sólo son accesibles por el personal de SECURITAS DIRECT en caso de que se produzca un evento que exija la realización de un análisis forense. En todo caso, los logs que permanecían en la memoria interna de la centralita inutilizada por la*

actuación ocurrida el 27 de noviembre de 2015 han sido incorporados a la información facilitada en el mencionado Documento Nº 2 del escrito de alegaciones al Acuerdo de Inicio."

c) Al hablar de memoria interna del dispositivo, dónde se ubica esa memoria interna ¿qué eventos registra, diferencias con las señales que puede enviar a la central de alarmas el panel de control? .

Responde que se encuentra alojada en la placa base de la centralita-panel de control-.

En cuanto a los eventos que refleja, ya los ha detallado.

d) Informen si es posible y en qué circunstancias, activar o desactivar la alarma desde la CRA, y si la operación se puede registrar en logs y si en este caso, se ha producido algún evento de este tipo en el periodo de acceso solicitado.

Responde que "*Desde la CRA, los operadores tienen la capacidad de activar o desactivar la alarma únicamente a petición del cliente, en el marco de una interacción telefónica con éste. Esa petición queda debidamente registrada, por medio de su correspondiente log*."

"*En el supuesto analizado en el presente expediente, dicha funcionalidad sí se utilizó dentro del período solicitado, y prueba de ello son los registros que se detallan a continuación, los cuales forman parte de la información enviada a la Agencia*:

• (...):

o 18/12/2015 a las 20:08:57 - Orden enviada (...) Total por usuario: ***B.B.B.***. o 18/12/2015 a las 20:09:08 - (...) externo Total.
o 18/12/2015 a las 20:19:59 - Orden enviada (...) Total por usuario: ***B.B.B.***. o 18/12/2015 a las 20:19:59 - (...) externo Total.
O 18/12/2015 a las 20:20:07 - Orden enviada (...) Perimetral por usuario: ***B.B.B.***.

o 18/12/2015 a las 20:20:19 - (...) externo Perimetral

• (...):

o 18/12/2015 a las 20:18:56 - Orden enviada Desarmar por usuario: ***B.B.B..***

o 18/12/2015 a las 20:19:11 - Des(...) externo: ******NÚMERO.4***.
3.5-Modo/s de **verificación de la alarma** aplicable/s en este caso, y que logs se generan y señale los que con este descriptivo, figuren en el período solicitado por el reclamante.

Responde que "*los logs que se generan para la verificación del funcionamiento de la alarma pueden clasificarse de la siguiente forma:*

(i) aquéllos que se generan como consecuencia de una interacción del titular del contrato o de un autorizado por el mismo con el sistema de alarma;

(i) los derivados de una interacción humana producida desde la CRA; y

(ii) los que se generan de forma automática, sin intervención humana de ningún tipo.

En este sentido, y teniendo en cuenta que únicamente los logs enumerados en los puntos (i) y (ii) implican un tratamiento de datos personales, y de éstos sólo el enumerado en el punto (i) supone el tratamiento de datos del Reclamante o las personas autorizadas por el mismo, en el Documento nº 1 aportado por la reclamada junto con su escrito de alegaciones, se aclaraba que el derecho de acceso por el interesado a sus propios datos, únicamente afectaba a los contenidos en el citado punto (i) y no a los relacionados en los puntos (ii) y (iii), que no incorporan datos personales del Reclamante.

En concreto, y en lo que respecta a todos los logs aportados a la Agencia, encajarían en lo descrito en esta respuesta los siguientes logs que representan verificaciones de alarma:

• Logs comprendidos entre el 27/11/2015 desde las 20:09:47, hasta las 20:17:07, momento en el que se contacta con un plan de acción.

• Logs comprendidos entre el 06/12/2015 desde las 01:15:04 hasta las 01:17:40.

3.6-a) Informen sobre los aspectos de funcionamiento de la configuración y tipos de configuración, del dispositivo en el sistema de seguridad contratado por el reclamante, y por los distintos tipos de usuarios que se contemplaban y tenían acceso en la configuración del dispositivo, si existieran. Modo por el que se identifican en los logs las distintas acciones de los posibles usuarios en sus distintos roles que puedan asumir: titular, autorizados, contactos en los distintos elementos del sistema. En uno de los nombres de log figura *"usuario* ******USUARIO.1*** *accedió a la ficha del cliente*", quién es este usuario, dado que en otros supuestos se refieren al personal de la entidad como "*técnico*", *"operador*".

a) En cuanto al término usado en logs, "*contacto designado*", descripción de a quién se refieren, y su relación en su caso con los autorizados al acceso al sistema, y en este caso ¿si el contacto designado es solo el titular del contrato de alarma? Relación de acciones llevadas a cabo por titular o personas autorizadas en cuanto a situaciones técnicas en que se puede encontrar el sistema, ***(...)***/(...), y si pueden resultar identificables dichas acciones relacionándolos con la persona que interacciona.

b) Informen del número de Usuarios autorizados en el sistema de alarma contratado por reclamante, número de contactos designados, y si solo era contacto designado el titular del contrato, roles que diferencia en sus actuaciones y sus límites al usuario autorizado frente al contacto designado. ¿para qué tipo de acciones cada uno? y ¿qué tipo de acciones solo puede llevar a cabo el titular?

c) Documento en el que el titular del servicio hubiera dado los datos de los usuarios autorizados, los contactos designados.

Responde que "*para aclarar el modo de interacción de los sistemas de alarma con la CRA, se responde en conjunto. Los contactos autorizados se entiende lo* serían, por el titular que contrató el sistema, el reclamante, mientras que los usuarios con acceso al sistema se corresponderían con el personal de SD.

Los contactos autorizados o designados pueden interactuar, en todo caso o bajo ciertas circunstancias con la CRA, realizando una comunicación a la misma en que pueda solicitarse la modificación de determinadas características del plan de acción establecido en el contrato (e.g. tiempo de retardo en la activación/desactivación del sistema, actualización de los teléfonos de contacto, etc.). En todo caso, esa interacción deberá ir precedida de la palabra clave también establecida en el contrato. Asimismo, los contactos autorizados, por su orden serán los destinatarios de las llamadas que SECURITAS DIRECT pueda realizar en caso de existir algún tipo de incidencia en el funcionamiento del sistema. En este concreto caso, como puede comprobarse, el Reclamante designó en el Contrato a cuatro contactos autorizados, estableciendo igualmente el orden de los mismos para el supuesto de que fuera necesaria la interacción con aquéllos (véanse las dos últimas tablas en la página 16 del contrato). Junto con los contactos autorizados y el titular del contrato, las otras personas físicas que operan en el sistema son los usuarios, identificados como los agentes de SECURITAS DIRECT que pueden recibir una determinada incidencia como consecuencia de una interacción con el titular o aquellos contactos designados y en su caso, llevan a cabo las operaciones solicitadas por aquéllos. Ello daría lugar a la generación del consiguiente log que en la valoración adjunta al documento de alegaciones al Acuerdo de Inicio eran consideradas como datos personales del Reclamante, al proceder de una acción instada por éste o sus autorizados.

*A fin de que los usuarios autorizados de SECURITAS DIRECT no resulten directamente identificables o sean accesibles por terceros, cada uno de ellos cuenta con una denominación unívoca o "matrícula" formada por caracteres alfanuméricos que permite exclusivamente su identificación interna por la sociedad. Tal es el código "****USUARIO.1***" *que figura en uno de los logs y sobre el que se ha planteado por la AEPD la cuestión de los usuarios. En este caso consta la matrícula del interesado y no su denominación genérica dado que el acceso se produjo como consecuencia de la interacción llevada a cabo por el titular del contrato, garantizándose así la trazabilidad de lo solicitado y la determinación por SECURITAS DIRECT de quien atendió a dicha solicitud.*

Finalmente, dentro de los usuarios del sistema cabe hacer referencia a los restantes técnicos u operadores, ***(…)****. En este caso, el log generado por su actividad no genera una matrícula, al no ser precisa la garantía de trazabilidad antes mencionada.*

A efectos de los logs aportados en este caso, aquellos que generan una interacción entre el titular o un contacto designado por éste y SECURITAS DIRECT son los comprendidos entre el 05/12/2015 a las 14:19:04 y las 14:45:45, donde ******USUARIO.1*** *accede a la ficha de cliente para gestionar y acordar un mantenimiento con el cliente asociado al evento que ocurrió el 26/11/2015.*

Posteriormente también a las 18:38:10 del día 05/12/2015, aparece en el log la matrícula ******MATRICULA.1****, que es el técnico que se desplaza físicamente al*

domicilio del reclamante para realizar el mantenimiento correspondiente, y se conecta al sistema para llevarlo a cabo.

Finalmente, el 18/12/2015 a las 20:08:18 se loga el empleado de SECURITAS DIRECT ***B.B.B.****, como consecuencia de una llamada del cliente a SECURITAS DIRECT donde consulta el estado de conexión de la alarma en ese momento. Para ello, el empleado debe acceder a través de una herramienta interna, que requiere el logado a partir de su correo electrónico profesional y contraseña, a través de la que puede verificar el estado de conexión del sistema e interactuar con el sistema en virtud de lo que se solicita el cliente. Si bien, queda registrada esta interacción en los logs, el cómo debe ejecutarse es lo que implica que en el registro en lugar de matrícula aparezca el correo electrónico (sin @securitasdirect.es). En este caso, el Reclamante se comunicó con el operador de SECURITAS DIRECT que figura identificado en estos logs y que en el momento de iniciarse la conexión hubo de identificarse previamente ante el Reclamante, por lo que éste ya disponía de la información identificativa de este empleado en el momento de realizarse la conexión."*

3.7 a) Funcionamiento de la programación del dispositivo al entrar al domicilio con el sistema de seguridad en activo, para desactivarse, o al revés, para dejarlo configurado cuando se abandona la vivienda, considerando además, que puede haber distintos usuarios, y como tiene que operar cuando accede otro usuario distinto al que dejó programada de salida la alarma.

Respondió que "*el Manual incorpora el procedimiento de activación y desactivación del sistema de alarma como consecuencia de la interacción de un usuario, no siendo a estos efectos necesario que la activación y desactivación se lleven a cabo por un mismo usuario*."

a) Indiquen si el servicio contratado incluía el control de la aplicación con dispositivo o terminal telefónico móvil y como interaccionaba con los logs almacenados en el servidor en el periodo solicitado.

Indica que "*el sistema contratado permitía su activación y desactivación desde la aplicación (en adelante, la "App") que el usuario podía instalarse en su dispositivo móvil (existe dicha aplicación en versión iOs y Android). Teniendo en cuenta lo anterior, cuando se produce una interacción del titular o un contacto autorizado que implique la conexión o desconexión del sistema de alarma, dicha incidencia se registra en la memoria interna del dispositivo, aunque sólo se transmite a la CRA en caso de que la actuación responda a la existencia de una incidencia de seguridad. En ese supuesto, es decir, cuando se produce una incidencia de seguridad (e.g. desconexión como consecuencia de un salto de alarma) y posteriormente se desconecta el sistema, el log queda registrado en la CRA identificando al usuario (llave, mando o código) que ha realizado la acción. Igualmente, si la desconexión o la conexión se realiza desde la App se transmite el log a la CRA, reflejando que se ha producido una acción a través de un dispositivo Iphone o Android, pero no se refleja el número de teléfono desde el cual se realiza esta acción*.

En el presente supuesto estos registros serían los siguientes:

• *06/12/2015 a las 1:15:27 – Desconexión. KF 00 - User: 07 Desconexión por salto de alarma de la 1:15:04 (...). Este log registra una desactivación del sistema de alarma por medio de un mando a distancia a raíz de un salto de alarma.*

.En cuanto a logs asociados a interacciones con el sistema de alarma a través de la APP instalada en el móvil del reclamante", refiere peticiones desde IPhone de distintos tipo: petición de estado, de ***(...)***, de imagen en diversas fechas a partir de 6/12/2015.

En todo caso, la memoria interna de la centralita (Panel de Control) a la que ha podido acceder mi mandante, es decir la inicialmente instalada y destruida en los hechos acaecidos el día 27/11/2015, no incorpora, dentro del período temporal respecto del que se ejerció el derecho de acceso, ningún log referido al ***(...)*** *o des(...) del sistema de alarma, siendo esta, y no otra, la razón por la que la información facilitada al Reclamante no incorpora ningún registro de esta naturaleza en relación con el dispositivo inutilizado. Respecto de los logs que constasen en la memoria interna del instalado en fecha 5 de diciembre de 2015, tal y como se analizará al dar respuesta a la cuestión formulada en el punto 4.14 del escrito de esa AEPD", (3.14 de esta propuesta) "mi mandante no pudo en ningún momento acceder a la información, por lo que no le resultaba posible facilitarla al interesado*."

3.8-a) Si de acuerdo con la normativa específica del sector del funcionamiento de alarmas, se efectúan **revisiones periódicas,** cuales serían estas, y si se hacen constar en los logs, determinando cuales son los logs concretos que responden a dichas revisiones. Si el denominado registro de incidencias, del que se habla en la OM 316/2011 de 1/02 de funcionamiento de los sistemas de alarma guarda alguna relación con los logs generados por el sistema.

Responde que: "*las revisiones periódicas están previstas en el artículo 43 del RD 2364/1994 por el que se aprueba el Reglamento de Seguridad Privada y el artículo 5 de la Orden INT/316/2011. Estas revisiones comprenderían al menos, la obligación de realizar sólo una revisión anual presencial. La CRA de SECURITAS DIRECT tiene capacidad de realizar estas comprobaciones de manera remota, normalmente cada tres meses. Además, indica que se realizan test diarios de comunicación y correcta transmisión del sistema de alarma con la CRA de forma automática.*"

Se adjuntan ejemplos de las citadas verificaciones:

06/12/2015 18:45:42 Uso de Panel: Tot 00, Parc 00, Per 00, Anx 00
05/12/2015 18:38:10 INSTALACION EN PRUEBAS
05/12/2015 18:38:10 INSTALACION EN PRUEBAS PARA MANTENIMIENTO - ***NÚMERO.1 POR TECN
05/12/2015 18:38:10 000:08:00 ALL ZONES
05/12/2015 18:38:10 TECHNICIAN: ******MATRICULA.1-C.C.C.*****

"*De las revisiones presenciales queda constancia en el log del sistema de gestión de las alarmas de la CRA, ya que el técnico debe ir comprobando una serie de parámetros del sistema y realizando las distintas comprobaciones de funcionamiento. Así mismo, tal y como se contempla en la normativa, si se realizasen revisiones remotas, estas quedarían reflejadas en la memoria de eventos del sistema de alarma*

(art 5.2 OM y anexo III mantenimiento presencial trimestral con posible alternativa a automatizada auto test y bidireccional."

b) Diferencia de las revisiones y las operaciones de mantenimiento de la instalación en estado operativo, donde se regulan esas últimas, y a través de que modalidad se llevan a cabo esas operaciones de mantenimiento.

Indicó que "*La revisión es una tarea obligatoria, preventiva y periódica descrita en el citado Reglamento de Seguridad Privada y la Orden Ministerial 316/2011, y el mantenimiento es una tarea correctiva destinadas a solventar incidencias puntuales que no permitan el correcto funcionamiento del sistema de alarma, y que tienen como objeto la subsanación de dichas incidencias. La revisión se lleva a cabo, tal y como se ha puesto de manifiesto en el apartado a), mientras que el mantenimiento dependerá de la necesidad y la naturaleza de la incidencia, pudiendo realizarse de manera presencial o remota*."

3.9- Si existe alguna relación entre los libros registro de revisiones, libros registros de alarmas, registro de incidencias, OM 316/2011 de 1/02 de funcionamiento de los sistemas de alarma, y los logs generados por el dispositivo instalado en el domicilio del reclamante, si datos de los logs se traspasan a dichos libros, y su relación con la consideración de dato personal del titular.

Respondió que "*Las empresas de seguridad, según la actividad para la que se encuentren autorizadas por el Ministerio del Interior, están obligadas a la llevanza de determinados libros. En el caso de SECURITAS DIRECT, deberá llevar los siguientes Libros, cuyos modelos han sido aprobados oficialmente por el Ministerio del Interio*r:

• *Libro Registro de Alarmas. Se completa y custodia por parte de SECURITAS DIRECT Está destinado a registrar los avisos de alarmas confirmados que se comunican a las Fuerzas y Cuerpos de Seguridad. "En el presente caso, no hubo ninguna alarma confirmada por lo que no se recogerían en este libro""* Aporta impresión de parte del libro en la que no figura inscripción.

• *Libro Registro de Revisiones de Empresa. Completado y custodiado por Securitas Direct, se encuentra destinado a registrar todas las revisiones periódicas presenciales que se realizan a los sistemas de alarma de sus clientes operativos.*

• *Libro Registro de Comunicaciones con las Fuerzas y Cuerpos de Seguridad, cuyo objeto es el registro de las colaboraciones y auxilios que se realizan durante el año con las Fuerzas y Cuerpos de Seguridad.*

"En ninguno de los citados libros se registran o traspasan logs o señales de los sistemas de alarmas tal y como los registra el propio sistema, sino que se registra la información de ese evento comunicado a las Fuerzas y Cuerpos de Seguridad aportando los datos que se piden en el libro".

3.10-Para verificar el modo en el que figura el registro o log en bruto en el sistema, se solicita que aporten copia del **log en bruto**:

a) De 15/12/2015, 4:50:24-Señal informativa- que era el primero que constaba en el derecho de acceso entregado al reclamante en su escrito de 23/02/2021.

a) Uno de los logs de 27/11/2015, que aparecen agrupados en "*Actuación CRA*", y en "*descripción extendida"* consta "*distintas actuaciones genéricas del operador humano*…"

Señala que todos los logs generados en el sistema aparecen recogidos en su integridad en el documento aportado como documento dos, junto con el escrito de alegaciones al acuerdo de inicio.

Aportan documento 5 con el extracto de los concretos logs solicitados

Los logs del 27/11, ocupan 8 líneas, actuación central receptora de alarmas.

b)Indique como sale la información referida en "*descripción extendida del log*" antes de la elaboración, o dónde se acude para que en algunos casos sea tan genérica o abierta la descripción. Si estas descripciones genéricas no pueden ser detalladas más.

Respondió que "*Tal y como puede comprobarse en la información contenida en la respuesta anterior, la "descripción extendida del log", que se incorporaba en la primera de las respuestas dadas al Reclamante por mi mandante, no se contiene en los logs generados por el sistema, que se reprodujeron tal cual son mostrados en la segunda de las respuestas. Esta descripción se introdujo en la primera respuesta al Reclamante con la única y exclusiva finalidad de clarificar el alcance y significado de los mismos. En este sentido, SECURITAS DIRECT consideró que la información facilitada al Reclamante en bruto (documento número 2 de los aportados junto con las alegaciones al Acuerdo de Inicio) y sin una mínima descripción del significado de los logs podría carecer de utilidad para el Reclamante*".

3.11-En sus alegaciones, indicaron que:

"… *los registros considerados como datos personales han sido aportados en tres ocasiones y en dos formatos diferentes e incluyendo información complementaria que permitiese al reclamante entender la misma. Cabe recordar que los registros generados por los sistemas de mi representada han sido aportados tal y como se generan en éstos, y aun así se han hecho esfuerzos que incluso excedían de la obligación de mi representada, para que el receptor pudiera entender el evento que reflejan*".

Se solicita que aporten o informen de cuál es la información complementaria que contribuye a entender la misma y de donde procede.

Responde que "*la información complementaria a la que se hace referencia en esta cuestión es la referida a la "descripción extendida del log", ya mencionada en el apartado anterior que mi mandante incorporó a las respuestas facilitadas al interesado en el momento de dar respuesta en todas las ocasiones junto con cada uno de los logs, tratando de exponer, aunque fuera mediante una breve descripción, las acciones*

a las que respondía cada uno de ellos. En este sentido, mi mandante hizo todos los esfuerzos razonablemente exigibles por atender con la mayor claridad posible lo solicitado por el Reclamante, no limitándose a facilitar los logs en el formato en que se generan en los sistemas de SECURITAS DIRECT, sino clarificando brevemente el alcance de cada una de las líneas de Código facilitadas."

3.12 Respecto a las "*interacciones activas del propio usuario con los sistemas en físico o a través de la aplicación móvil*.", "*interacciones pasivas del usuario o de terceros que puedan proporcionar información con su forma de actuar*", señalen ejemplos, y si en todos los casos podrían ser datos de carácter personal o no, y logs que se puedan hallar dentro de estas categorías.

Respondió que "*Las interacciones activas del propio usuario con el sistema quedan reflejadas en el correspondientes log. En particular, cabe hacer referencia a las conexiones y desconexiones del sistema de alarma, que sólo quedan registradas en caso de haberse producido un salto de alarma previo, tal y como se indica en la respuesta a la cuestión planteada en el punto 4.4 del escrito de esa AEPD",* (en esta propuesta 3.4).

Junto con dichas interacciones físicas, el cliente puede tener otras complementarias o adicionales como p.e. pulsar el botón "*112*" que genera una llamada directa a través de la centralita al 112. También, como interacción física puede pulsar el "*SOS*" desde la centralita y desde el lector de llaves (tag reader). De igual manera, se puede pulsar un "*código de coacción* "a través de los números indicados en la centralita o puede generar intencionadamente una señal de manipulación/sabotaje o tamper, consistente en retirar un dispositivo por un determinado motivo (e.g. porque se va a pintar la vivienda) o sin él (e.g. porque lo golpea accidentalmente).

Finalmente, a través de la aplicación móvil, se pueden realizar conexiones y desconexiones de la alarma, consulta de estado de sistema, revisar facturas o realizar una petición de imágenes.

Ejemplos relativos a interacciones físicas del sistema vienen definidos en la columna "****COLUMNA.2* ***(...)***".

Respecto de las "*interacciones pasivas*", *no implican la realización de una actividad concreta del titular o sus contactos, sino que contienen información que, en caso de ser analizada, algo que SECURITAS DIRECT no lleva a cabo, podrían revelar hábitos de conducta de aquéllos (e.g. reiteración de períodos en que el sistema está* ***(...)****, que denotarían ausencia de la vivienda objeto del sistema de seguridad), por lo que se consideraron datos personales y fueron facilitados al Reclamante. En consecuencia, esta información no se deriva de un log específico sino de un análisis más detallado de los logs que, como se ha indicado, no lleva a cabo mi representada*."

3.13- Manifestaron que "*le informamos que* ***(…)*** *los sistemas de alarma de Securitas Direct registran y almacenan la información procedente de los eventos con origen técnico y de los eventos con origen en la interacción de los dispositivos instalados en el domicilio de los clientes*". Especifique sobre esta memoria interna en que dispositivo existe, cuál es su función, y que eventos registra, de donde proceden, cuanto tiempo

se almacenan y cuando se recogen, así como con que dispositivos interactúa. Y ¿cómo se produce el guardado y con que periodicidad, y su destino.?

Respondió que "*la memoria interna del dispositivo se encuentra en la placa base de la centralita de alarma (Panel de Control), siendo su función registrar los eventos en el sistema que se generan y almacenando únicamente los últimos ***NÚMERO.3 realizados, tal y como se ha indicado en la pregunta 4.4.b) (*en esta propuesta 3.4.b). *Estos registros se van borrando, de manera cíclica, en función de los nuevos registros que se vayan generando y grabando, de forma que la generación de un nuevo registro implica el borrado del más antiguo de esos ***NÚMERO.3. Dichos eventos pueden responder a interacciones del panel con:*

(i) los titulares y contactos autorizados por el mismo;

(i) *los restantes dispositivos del sistema (e.g. sensores volumétricos o fotodetectores); o*

(iii) el backend de SECURITAS DIRECT."

La reclamada manifestó que "*Tras el acceso a los registros contenido en la memoria de la alarma se ha comprobado que ésta se encontraba conectada desde el día 22/11/2015 a las 11 56 y que no presentaba anomalía alguna, asimismo, el sistema de alarma registró y envío señales de captación de movimiento a las 20:09 h del 27/11/2015, no registrando evento alguno con posterioridad*."

3-14 El reclamante manifestó en el procedimiento de ejercicio de derechos TD/00167/2021, que "*la solicitud de acceso a los registros contenidos en la memoria se refieren tanto a "la central de alarma destruida como a la que se instaló en mi vivienda el 5/12/2015 y que siguió generando señales y registros*". A tal efecto, se solicita que informen sobre la que el reclamante dice se instaló el 5/12/2015, ¿si era dentro del mismo contrato?, motivo por el que se instala y ¿qué incidencia tiene en los logs de la destruida?, y ¿por qué no se dieron los logs de la memoria interna desde dicha fecha a 13/12/2015.?

Respondió que "*Ante todo, es preciso indicar que mi mandante sí facilitó aquella información referida a los logs generados durante el período de tiempo indicado en su solicitud, tal y como obra en el expediente, en que se incorporan las dos respuestas facilitadas al Reclamante por SECURITAS DIRECT (la primera de ellas incorporando una descripción detallada de los logs y la segunda facilitándole los logs tal y como se recogen en los sistemas de mi representada).*

En este sentido, se han incorporado a las sucesivas respuestas tanto los logs almacenados en la CRA, como los procedentes de la memoria interna contenida en la centralita (Panel de Control) destruida el 27/11/2015. En cuanto a los logs generados a partir de la instalación de una nueva centralita, la CRA, y por tanto mi mandante, únicamente puede acceder a los logs que son transmitidos a la misma desde la memoria interna del dispositivo, pero no a los de carácter meramente técnico que se generasen en dicha memoria interna, dado que SECURITAS DIRECT únicamente puede acceder al contenido de dicho dispositivo en caso de que se hubiera producido

un incidente que exija su análisis forense. En este caso, dado que dicho incidente no tuvo lugar, el dispositivo permaneció en la vivienda del Reclamante hasta la finalización del Contrato, sin que en ningún momento SECURITAS DIRECT pudiera acceder a dicha memoria interna ni fuera necesaria la realización de ningún análisis forense de su contenido, al no haberse producido un incidente que lo exigiera. Como puede comprobarse, en dichas respuestas sí se contiene información referida al período mencionado en la cuestión planteada. No obstante, se aclara que dichos eventos se encuentran incorporados al documento aportado por mi mandante como Nº 2 al escrito de alegaciones al Acuerdo de Inicio, y generados a partir del citado día 5 de diciembre de 2015.

Por otra parte, en caso de destrucción de la centralita (Panel de Control), y siempre dentro del alcance de los servicios contratados, se procede a reemplazar aquél por uno distinto, siendo dicha instalación, y los logs generados desde el momento de la instalación parte del desenvolvimiento del citado contrato. En el caso que nos ocupa, el motivo del remplazo de la centralita (Panel de Control) el día 5 de diciembre de 2015, fue debido a los daños sufridos derivados de la intrusión ocurrida en fecha 27/11/2015. Como ya se indicó en la respuesta a una pregunta anterior, los logs no quedan modificados por el hecho de producirse esta sustitución en el dispositivo, siendo los que se derivan de la interacción del sistema de alarma con la CRA."

3.15 ¿Por qué motivo indica en el recurso de reposición contra el procedimiento de ejercicio de derecho TD/167/2021 que "*en formato líneas de código" satisfaría en menor medida el cumplimiento de los requisitos exigidos por el RGPD para que el derecho de acceso pueda ser considerado atendido adecuadamente*"? Y ¿cuál es el formato "*líneas de código*", ¿si es el de los logs cronológicamente, sin agrupar? Aporte copia de un formato *líneas de código* como ejemplo, el del quinto punto del acceso entregado al reclamante el 23-02-2021 "*actuación CRA*" e indique a que se refiere en el recurso de reposición contra la TD/00 167/2021 con que la información *"se encuentra listada en la tabla adjunta al escrito de 23/02/2021*", si se trata de la explicación general que contiene cada columna o a que otra información, y ¿dónde aparecía listada?, reenviando copia de la misma y si se envió al reclamante.

Responde que "*Dado que conforme a las exigencias del artículo 12.1 RGPD la información facilitada al interesado solicitante del derecho de acceso debe facilitarse de forma "concisa, transparente, inteligible y de fácil acceso", y como ya se ha indicado reiteradamente en este escrito, SECURITAS DIRECT consideró que <u>la mera reproducción de las líneas de código correspondientes a los logs generados por el sistema, en el formato en que a mi mandante le son visibles, no permitiría al Reclamante conocer el alcance, sentido y significado de cada uno de los logs remitidos en respuesta a su solicitud de ejercicio del derecho de acceso.</u>*

Por este motivo, <u>se remitió la información con indicación del log correspondiente, la fecha y hora de su generación y la descripción del significado del citado log.</u>

Ello no obstante, y dado que el interesado no estuvo de acuerdo con la información facilitada, se le hizo igualmente entrega de la información en bruto y tal como se genera en los sistemas de SECURITAS DIRECT, siendo dicha información la que se

recoge, sombreada en color verde, en el Documento Número 2 aportado por esta parte junto con su escrito de alegaciones al Acuerdo de Inicio."

3.16 Se solicita a la reclamada que informe en que se parecen, y que diferencias existen entre los accesos entregados al reclamante en escritos del 23/02/2021, 18/05/2021 y los de 14/12/2021, en cuanto a cantidad y contenidos de logs, y por qué no se enviaron en este último y en el de mayo, claves o indicación clara de diversas expresiones que se utilizan en dicho cuadro.

Respondió que: "*Tal y como se ha indicado en diversas ocasiones a lo largo del presente escrito, las diferencias existentes entre las dos respuestas facilitadas al interesado únicamente es en el formato de las mismas, conteniendo en los dos supuestos los mismos logs. Así, en la facilitada el 23 de febrero de 2021 hacía constar cada uno de los logs recogidos en los sistemas de SECURITAS DIRECT que contenían datos personales, incluyendo en la primera columna los momentos en que se habían generado y en la tercera de ellas una descripción resumida del significado del correspondiente log. Por su parte, en la facilitada el 18 de mayo de 2021, y reproducida posteriormente en fecha 14 de diciembre de 2021, ante la consideración del Reclamante de que la información facilitada no le había sido entregada en el formato en que se recoge en los sistemas de mi mandante, se reprodujo la citada información, sin incluir la descripción explicativa de los logs. De esta forma, cada línea del documento (los marcados en verde en el Documento Número 2 adjunto a las alegaciones al Acuerdo de Inicio) se hacía referencia a un log individualizado, siendo lógicamente similares las líneas en que dicho log se repetía*.
Fuera de las citadas diferencias, referidas únicamente al modo de presentación de la información, pero no a su contenido, no cabe apreciar ningún tipo de diferencia adicional."

3-17 a) Indiquen para el servicio contratado por el reclamante, qué logs se generarían cuando ha saltado la alarma, según las distintas circunstancias que puedan darse, y que actuación o actuaciones se llevarían a cabo. Indique los logs que se relacionan con cualquier tipo de salto de alarma que existen en los cuadros, y las diferencias entre ellos, y características tenidas en cuenta para que sean considerados que contienen datos de carácter personal del reclamante o no.

Respondió que "*los logs generados con el salto de alarma sufrido por el Reclamante el día 27/11/2015 figuran en el documento aportado por SECURITAS DIRECT junto con el escrito de alegaciones al Acuerdo de Inicio, comprendiéndose entre el primero de los generados el 27 de noviembre de 2015 a las 20:09:47 y el generado el mismo día a las 20:17:07 horas. Igualmente en el citado documento se incluyen los restantes supuestos en que se produjo un salto de alarma y los logs generados, diferenciando los que contienen o no datos personales, según aparezcan sombreados en color verde o en color rojo y a partir de la información incluida en el informe que se adjuntó como Documento Nº 1 junto con las alegaciones al Acuerdo de Inicio del presente procedimiento. Como puede comprobarse, dichos logs se inician mediante la detección de una alerta de alarma volumétrica a las 20:09:47, generándose un código aleatorio (1155) que se genera con cualquier salto de alarma) para que, si se envía a un vigilante, éste pueda desconectarla (en este caso, no se utilizó para enviar a ningún vigilante, ya que se determinó que no era necesario). A partir de ese instante, constan los logs de verificación del sistema para el traspaso de la información a un*

operador, que realiza desde ese momento las llamadas pertinentes a quienes aparecen como contactos designados en el Contrato celebrado por el Reclamante. Como puede comprobarse dichos intentos son infructuosos respecto de los tres primeros contactos, al saltar el buzón de voz, pudiendo efectuarse la comunicación con el cuarto de los contactos que, sin embargo, no facilita la palabra que permite establecer la comunicación y que también consta previamente establecida por el Reclamante en el Contrato, concluyendo la tramitación de la alerta el 27 de noviembre de 2015 a las 20:17:07 horas.

Como también puede comprobarse, todas las actuaciones relacionadas con el salto de alarma y los intentos de contacto han sido consideradas datos personales y facilitadas al Reclamante, no teniendo tal consideración los logs exclusivamente relacionados con el modo en que los sistemas de SECURITAS DIRECT gestionan y encauzan las actuaciones a realizar en estos casos o los que se refieren exclusivamente al operador interviniente. La explicación justificativa de la consideración o no de la información como datos personales se contiene en el informe aportado por mi mandante como Documento Nº 1 junto con las alegaciones al Acuerdo de Inicio. Asimismo, puede comprobarse la existencia de distintos logs relacionados con saltos de alarma posteriormente desactivados el día 5 de diciembre de 2015 a partir de las 18:56:37, habiendo sido todos ellos facilitados al Reclamante por considerarse que incorporan datos personales relativos al mismo, dado que se trata de acciones encaminadas a probar el funcionamiento del sistema instalado en su vivienda, realizándose distintas pruebas de alarma (volumétricas, sísmicas, por coacción o magnéticas). También se produce un salto de alarma el día 6 de diciembre de 2015 a las 01:15:04 horas, pudiendo comprobarse los logs generados por el sistema, y que concluye con la comunicación con el titular que indica a las 01:17:22 horas que el salto de la alarma puede haber sido generado por la chimenea."

a) En el acceso solicitado, informar si de resultas de algún salto de alarma, fue comunicada a la Policía el posible acceso a la propiedad, y si queda registrado en logs, señalando cual seria.

Responde que "*la comunicación con la policía genera el correspondiente log, que en este caso no se generó al no producirse ese contacto*".

b) Igualmente, informen si en los logs figura algún evento de "*alarma no confirmada"*, señalando cuales serían y si se han considerado datos personales.

"*En la respuesta dada a la primera de las cuestiones contenidas en este apartado, se han indicado los saltos de alarma producidos y sus vicisitudes. La explicación acerca de si los logs generados contienen o no datos personales se incluye en el documento Nº 1 adjunto a las alegaciones al Acuerdo de Inicio*."

3-18-Si cuando se produce un salto de alarma, todas las actuaciones relacionadas con el dispositivo quedan en los logs y si adicionalmente, se pueden generar o crear otras por los propios operarios, y cuáles serían, indicando si todas serían datos personales, o no, y los logs de cada una de ellas (si dato personal del reclamante, no).

Respondió que: "*en la respuesta a la cuestión anterior se han descrito los saltos de alarma producidos en el sistema del Reclamante con los logs generados, pudiendo diferenciarse entre los que contienen o no datos personales. Igualmente, como ya se ha indicado, los logs generados por el sistema no quedan al arbitrio de los usuarios del mismo o del personal de SECURITAS DIRECT, siendo los previamente constituidos en el sistema, si bien lógicamente la actuación de dicho personal da lugar a la generación de los correspondientes logs previamente configurados."*

3-19 a) En cuanto a los protocolos que debe hacer motu proprio Securitas -chequeos y verificaciones técnicas, y relación con mantenimiento del sistema, especificar los artículos y la concreta norma que los regula, periodicidad o motu proprio, el protocolo interno resumido de actuaciones que desarrolla las mismas, y si la normativa de aplicación prevé la realización de informes de actividad de cada alarma mensuales para los propietarios, si estos informes se alimentan de logs extraídos del registro del dispositivo.

Responde que: "*Debe ante todo partirse de la diferencia entre una revisión y un mantenimiento a la que ya se ha hecho referencia en la respuesta dada a la cuestión incluida en el punto 4.8 "* (en esta propuesta 3.8) *del escrito de esa AEPD. Partiendo de dicha base, las revisiones y mantenimientos se regulan en los artículos 43 a 45 del Reglamento de Seguridad Privada y en el artículo 5 de la Orden INT/316/2011. En ellos se hace referencia a la periodicidad de las revisiones, así como el modo en que han de realizarse las revisiones presenciales y las remotas, ambas conforme a los Anexos II y III de la citada Orden. Los test de comprobación de la correcta comunicación y transmisión de la alarma, es un test que debe realizarse en función de las propias características del inmueble, partiendo de su diferente riesgo de atraco o intrusión (así, por ejemplo, en una joyería existe mayor riesgo, por lo que los sistemas de alarma deberán disponer de test periódicos de comunicación con una periodicidad menor, que en un sistema instalado en una residencia particular). Este aspecto se encuentra igualmente relacionado con los grados de seguridad y la certificación de los sistemas conforme a la norma UNE o UNE-EN que resultan de aplicación. Asimismo, el artículo 45 del Reglamento de Seguridad Privada regula la entrega a los titulares de las instalaciones de un manual de uso y mantenimiento preventivo y correctivo que el propio usuario deberá llevar a cabo, incluyendo acciones tales como el cambio de pilas de dispositivos, el control sobre la colocación de objetos que impida la captación de los detectores, etc. La normativa no regula la obligación de envío de informes de actividad de la alarma, de forma que cada empresa determina si se lleva a cabo el envío periódico de esta información. Además, el cliente puede consultar en la App las conexiones y desconexiones que haya realizado con las distintas llaves puestas a su disposición. El único supuesto en que se prevé la remisión de un informe al titular del contrato así como a las Fuerzas y Cuerpos de Seguridad, se produce en caso de que se haya producido un salto de alarma confirmado y éste no haya sido transmitido a las Fuerzas y Cuerpos de Seguridad, en que deberán incorporarse los motivos por los que no se produjo esa transmisión*."

b) En sus alegaciones indican: "*Securitas generó logs hasta las 20:09 h del día 27/11/2015, hora y fecha en la que se produjo la intrusión en el domicilio del reclamante y durante la cual dicho sistema de alarma quedó completamente inutilizado a partir de esa fecha no pudo generar más logs". Sin embargo, en el Anexo*

*l, que incluye los logs, figuran registros después de 27/11/2015, 20:0*9 h. ¿Cómo se explica este hecho? Y cual es el origen y finalidad de dichos logs, y porque no los consideran datos personales del reclamante.

Responde que: "*Los logs generados a partir del momento de producirse el salto de alarma, y una vez descartados los relacionados con los intentos de comunicación con los contactos designados por el Reclamante, se refieren a sucesivos intentos de comunicación entre SECURITAS DIRECT y el sistema instalado en el domicilio del Reclamante, que resultaron infructuosos y siendo interacciones máquina a máquina de carácter técnico."*

3.20 Explicación de por qué hay logs de distinto signo, según lo aportado, considerados datos personales o no, y dentro de estos más de uno, que coinciden en el registro exacto de la hora, ejemplo en los cuadros Excel aportados en alegaciones figura como no dato personal, *27/11/2015, 20:09:47,alarma volumétrico. Intrusión volumétrico, sísmico-según versión panel. Dispositivos que no necesitan restauración V8,8 a 9,5)- intrusión volumétrico radio Volumen*, y el log del día 5*/12/2015, 18:56:37/ALARM/URGEN/XPO09 RP-Alarma perimetral SER Volumétrica-foto. Intrusión volumétrico, sísmico-según versión panel. Dispositivos que no necesitan restauración V8,8 a 9,5)-*

Responde*:* "*Como ya se ha indicado en la respuesta a la cuestión planteada en el apartado 4.17*" (en esta propuesta 3.17) "*del escrito de esa AEPD, los dos logs mencionados en la misma difieren en cuanto a su contenido, dado que en el primero de los supuestos se produce un salto de alarma volumétrico de origen desconocido, que no aporta información acerca del interesado, Reclamante, mientras que el segundo se debe a la realización por aquél de diversas pruebas en el sistema de alarma reinstalado por SECURITAS DIRECT, deduciéndose del mismo la existencia de datos personales del propio interesado, que genera el salto del sistema de alarma a fin de verificar su adecuado funcionamiento*."

3.21 En la tabla que se dio a reclamante en 14/12/2021, así como en el documento 3, tabla color verde que aportó en alegaciones, y que son datos personales, existen diversos códigos en las columnas, numéricos, o de letras, sin los cuales no está clara la información. Se le solicita si sería posible la creación o recopilación del significado de dichas claves, que figuran en casi todas las columnas.

Respondió que: "*En relación con los códigos alfanuméricos que aparecen en la columna "SIGNAL", se trata del mensaje generado en el propio lenguaje del sistema de alarma que se traduce en la información que aparece en el resto de las columnas y esencialmente en la columna de "***COLUMNA.2* ***(...)****".*

*Por lo tanto, para entender el significado del código, hay que ir al campo de la columna "***COLUMNA.2* ***(...)****". El sistema remite mensajes que incorporan códigos alfanuméricos que posteriormente se traducen en las diferentes columnas del Log presentado. La columna "SIGNAL", recoge la parte del mensaje en "bruto" del sistema,*

en su propio lenguaje (lenguaje máquina) que luego se traduce en el resto de las columnas.

A tal efecto:

*• La columna "***COLUMNA.2 ***(...)** *es la traducción del evento de lenguaje de sistema a lenguaje técnico, para que el agente/operador entienda de qué trata el mensaje. Esta información se complementa con las columnas "****COLUMNA.1**" *y "****COLUMNA.2**" *que contienen información complementaria para que el agente/operador pueda entender el evento que se recibe en la CRA.*

*• La columna "ZONE", identifica el dispositivo de la alarma en el que se produce el evento (eg. **(...)**, identifica un fotosensor grabador en la posición 2 de programación) y la columna "AREA" describe la zona de la instalación que corresponde (eg, Home Sal??n)*

*• La columna "****COLUMNA.3**" *indica la prioridad de la señal, siendo los valores inferiores los de mayor prioridad.*

*• La columna "****COLUMNA.4**", *contiene el tipo de señal que representa al evento (e.g. INF es el código que se asocia a "información", que aparece en el ***COLUMNA.2 ***(...)**, *SS se asocia a "supervisión", como se recoge también en el ***COLUMNA.2 ***(...)**, *CC se asocia a "coacción", SO se asocia a "SOS", AAC se asocia a "corte de corriente", etc.…). De este modo, estos códigos se vinculan directamente con la información contenida en la columna ***COLUMNA.2 ***(...)**."

3.22 En el informe de 29/01/2021, aportado por la reclamada en alegaciones, documento I, tabla II, que contiene datos personales, aportado en sus alegaciones, consta la anotación: 05/12/2015 14:19:04/ACCESO REGISTRADO: El usuario ***USUARIO.1** accedió a la ficha del cliente/ Matrícula interna del operador que está actuando una incidencia concreta/ Información relativa a un operador de carácter procedimental e interno de Securitas Direct/se considera dato personal: SÍ/ En su caso sería considerado un dato personal del propio operador y por tanto no sería susceptible de facilitarse al interesado solicitante del derecho de acceso.

Se le solicita que responda quien es el usuario mencionado, y si accede a la ficha del cliente, guarda relación con sus datos, o accede a partir de que la alarma está funcionando, ¿porque no se le tendrían que proporcionar? De hecho, en el acceso se le ha proporcionado.

Responde que: "*Como ya se ha indicado en la respuesta a la cuestión planteada en el apartado 4.6 del escrito de esa AEPD, "*(en esta propuesta 3.6)"*la referencia alfanumérica al usuario se refiere a la matrícula del mismo en su condición de empleado de SECURITAS DIRECT, manteniéndose esa información seudonimizada a fin de que su revelación al Reclamante no implique una cesión de los datos de dicho usuario, toda vez que el acceso a la ficha de cliente del Reclamante no implica el tratamiento de datos personales de éste último, sino sólo del empleado* que accede a dicha información. *El dato ha sido facilitado al Reclamante a fin de entregar al mismo toda la información que pudiera resultar posible facilitar sin, por ello, perjudicar la actividad ordinaria de SECURITAS DIRECT ni las informaciones que se encontrarían*

protegidas por secreto comercial. No obstante, se reitera que del citado log no se desprende dato personal alguno referido a aquél. En este sentido, es reiterada la doctrina de la AEPD en cuya virtud el derecho de acceso no comprende el acceso a la información referida a los concretos usuarios del responsable del tratamiento que han accedido a los datos personales del solicitante."

3.23 En el mismo informe y misma tabla del caso anterior, figura el log de 18/12/2015, 20:08:18 ***COLUMNA.1 Logado: ***B.B.B.***, explican que "*El registro de actuaciones de un usuario supone la obtención de información personal sobre el mismo. Sí Se trata de un dato personal de un tercer usuario distinto del ejerciente del derecho de acceso y, por tanto, no sería susceptible de facilitarse al interesado solicitante del derecho de acceso*", como conocen que bajo ese log no se trata del titular que ejerce el derecho, motivo entonces por el que figuraba en la tabla entregada al reclamante el 23-02-2021 (hay otras más con la misma referencia).

Responde que:" *Como consideración previa, debe descartarse que la persona a la que se refiere el citado log sea la solicitante de acceso, no correspondiéndose ni con el Reclamante, ni con ninguna de las personas autorizadas por el mismo como contactos en su contrato, como se desprende de la propia identificación efectuada en la cuestión planteada. Hecha esta consideración, nos remitimos a lo indicado en la respuesta dada a la cuestión planteada en el punto 4.6 del escrito de esa AEPD*." (en esta propuesta 3.6).

3.24 En el documento 2 presentado en el registro denominado en alegaciones "*confidencial cliente total logs*", que contiene en rojo y en verde los logs, se le solicita que aclare, porque:

Figura como no dato personal en rojo el aviso:

27/11/2015 20:09: 47/comentario alarma volumétrica/ descripción intrusión volumétrico-sísmica según versión panel dispositivos que no necesitan restauración v 8, 8 a 9,5 intrusión volumétrico radio.

En la tabla I (informe de 29/01/2021, aportado por la reclamada en alegaciones) también se contiene el log.

Se solicita que informen si la alarma estuviera activada por el titular y se produce lo que figura en la información "*intrusión volumétrico radio*", por qué no lo consideran dato personal, al guardar relación con una información, configuración última efectuada, o que podría haberlo sido por el titular u otro usuario?, y que relación guarda con la siguiente que figura en verde, como dato personal, es misma fecha y hora, con distintos códigos, y con otra en rojo, misma fecha y hora "*descripción nivel de cobertura pane*l"

Además, se observa que figura la misma descripción en color verde como dato personal en fechas diversas del mismo cuadro, ejemplo 5/12/2015 18: 59 :08, 18: 59: 27, 18: 59: 48 18: 59: 57.

Responde que:" Tal y como se ha descrito en la respuesta formulada a la cuestión incorporada en el apartado 4.17 del escrito de la AEPD*"* (en esta propuesta 3.17) "*la*

información marcada en rojo responde a un evento técnico en el que no consta dato personal alguno del Reclamante (en este caso la detección de un salto de alarma) y por ello no forma parte de la información que debe ser objeto de entrega en el supuesto de atención de una solicitud de ejercicio del derecho de acceso efectuada por el citado Reclamante, conforme al artículo 15 del RGPD. Así se indica en el informe aportado por mi mandante como Documento Nº 1 adjunto al escrito de alegaciones al Acuerdo de Inicio (página 25) lo siguiente: *Esta línea de log, si bien proporciona información sobre un salto de alarma en los sensores, en la medida en la que no se traslada información directa sobre un atributo del interesado ni Securitas Direct pretende analizar un patrón de conducta o influir sobre él en modo alguno, la información facilitada por la línea de log analizada no debería ser considerada como dato personal. En este sentido, se trataría de un descriptivo del proceso técnico e interno de Securitas Direct." Los restantes logs generados en esa fecha y hora han sido facilitados al Reclamante cuando incorporan datos personales que pudieran referirse al mismo, no siendo facilitados en el supuesto en que se tratan de eventos meramente técnicos, siguiendo el contenido del mencionado informe (ver páginas 23 a 26 y 36 a 38 del mismo). Los logs generados el día 5/12/2015 a los que se refiere esta cuestión no derivan de un evento exclusivamente técnico, sino de la interacción del usuario con el sistema, haciendo saltar la alarma para comprobar su funcionamiento, por lo que efectivamente revelan datos personales de aquél y por este motivo sí han sido objeto de entrega al interesado al ejercitar su derecho de acceso, como también se describe en la respuesta a la cuestión planteada en el apartado 4.17 del escrito de esa AEPD*." (en esta propuesta 3.17).

3-25 a) Aclaren en documento 1, tabla I, logs de no datos personales, del informe de 29/01/2021, aportado por la reclamada en alegaciones, qué significa o a qué responde:

"*Logs, 06/12/2015 1:17:12, 06/12/2015 1:17:26/ SIN MOTIVO N/A No se proporciona información en relación con ninguna característica, patrón de conducta u otra información del usuario. NO*"(pág. 26/105)."

Responde que: "*Como se ha indicado en la respuesta a la cuestión 4.17"* (en esta propuesta 3.17) "*los logs citados responden a una incidencia técnica, que da lugar a una interacción con el titular de la que se desprende que dicha incidencia ha podido ser ocasionada por la chimenea y que no hay ninguna situación anómala. Estas interacciones han sido comunicadas al interesado en la respuesta facilitada a su ejercicio del derecho de acceso*."

Se aprecia pese a la respuesta, que los logs figuran en color rojo en el documento 2 de alegaciones al acuerdo de inicio.

-tabla I, a continuación del anterior: todos agrupados en (...): 0 "*27/11/2015 20:11:34 ,04/12/2015 11:04:50, 05/12/2015 9:30:10, 05/12/2015 10:48:31, 05/12/2015 13:14:21, 05/12/2015 14:17:44, 06/12/2015 1:15:22, 06/12/2015 16:33:51, 09/12/2015 8:54:14, 15/12/2015 2:38:08 15/12/2015 4:54:57"- Indicativo de que la incidencia se transmite a un operador humano o máquina. La señal, dada su relevancia, es transmitida a un operador máquina o humano para iniciar el proceso de gestión. No obstante, es un procedimiento interno del que no se puede inferir ningún dato personal del usuario. NO*". Se solicita aclaren significado clave (...):0, ¿cuál sería la incidencia?,

¿la señal procede de la centralita de alarma del domicilio?, y ¿porque no pone que incidencia se trata y no aclara definiendo a quien se transmite.?

Responde que "*El indicativo **(...)**:0 se limita únicamente a hacer constar en el sistema, tal y como se ha indicado, que se produce una **(…),** bien a un empleado a fin de que lleve a cabo las actuaciones que estén establecidas en función del evento que la haya generado, bien al propio sistema, para que lleve a cabo las verificaciones procedentes. De este modo, **(…)**, sino exclusivamente el procedimiento interno seguido por SECURITAS DIRECT ante una incidencia que figura en un log previo, con el que puede coincidir en la hora de generación, dado el automatismo con el que opera.*"

3-26 -en tabla I, de no datos personales, Logs existentes entre las fechas:

a) 28/11/201 22:21:18 y 04/12/2015 9:04:26
b) 04/12/2015 11:08:02 y 05/12/2015 13:16:56
c) 06/12/2015 16:33:51 y 06/12/2015 16:33:57
d) 15/12/2015 2:38:08 y 15/12/2015 2:38:12
e) 15/12/2015 4:50:38
*f) 15/12/2015 23:24:51 y 16/12/2015 12:20:34 / **(...)** transfer,* "*Asimismo, los logs describen las actuaciones internas y técnicas llevadas a cabo producto de esta desconexión*"

Informen cómo y por quién se inicia este procedimiento, y ante que evento se suele producir

Responde que: "*Como también se ha indicado en la respuesta a la cuestión 4.17*" (en esta propuesta 3.17) "*del escrito de esa AEPD, estos registros se derivan de la señal diaria que el sistema realiza automáticamente para verificar que el mismo se encuentra operativo. Al no existir respuesta por el sistema instalado en el domicilio del titular se generan los logs a los que se está haciendo referencia, pudiendo, a partir de ese log abrirse automáticamente un procedimiento de mantenimiento, a fin de que un técnico proceda en su caso a la reparación del dispositivo. En este sentido, tal y como consta en la información ya aportada, el día 4 de diciembre de 2015 a las 11:25:04 mi mandante se comunica con el contacto autorizado número 2 de los designados por el Reclamante en su contrato que indica, tal y como consta en la documentación, que mi mandante se ponga en contacto con ellos al día siguiente para la realización de pruebas según COM LOG que llamemos al día siguiente para pruebas. Por este motivo, las citadas comunicaciones del día 4 de diciembre de 2015 sí contienen datos personales y han sido objeto de entrega al interesado como consecuencia del ejercicio de su derecho de acceso*" Se aprecia que el log en que contacta con núm. 2, el 4/12/2015, podría ser el de 11:06:07

3-27 Dado que el log puede indicar que se detecta intrusión y da la información sobre saltos de alarma**,** motivo por el que el log de 6/12/2015 1:15:04 y los que agrupan en *Intrusión FOTO PIR RADIO* en la tabla I del documento 1, se considera que no es dato personal, no se está indicando que den el dato de la imagen, sino la información de que ha habido una intrusión, y motiven porque no sería dato personal dicha información.

Se observa además que un log con la misma fecha y hora, figura como dato personal, en verde en documento 2 de alegaciones acuerdo inicio, si bien con otra descripción: "*código para desarmar la alarma*" "*Central prioridad alta*" En otros logs de instantes posteriores figura "*todo bien*", "*indica que pudo ser la chimene*a" intercalándose otros logs de color rojo, no datos personales, sobre "*cobertura panel, imágenes para que CRA las descargue* o "*imágenes ya en CR*".

Responde que: "*Como se ha indicado en la respuesta a la cuestión 4.17",* (en esta propuesta 3.17) "*el log citado responde a una incidencia técnica producida en un fotodetector que, según* el criterio del reclamante, había sido generado por la chimenea de la vivienda. *Esta incidencia da lugar a un salto de alarma volumétrico, es decir, se identifica una intrusión o hecho anómalo, pudiendo el titular del contrato acceder a través de su App a la fotografía generada*."

3.28 a) misma tabla y documento mencionado anteriormente, logs de *15/12/2015 2:42:11 y 15/12/2015 4:50:19 CORRIENTE ELÉCTRICA (AUTO) Detección de falta de corriente eléctrica en el dispositivo. Información de carácter técnico de Securitas Direct. En la medida en la que no se traslada información directa sobre un atributo del interesado ni Securitas Direct pretende analizar un patrón de conducta o influir sobre él en modo alguno, la información facilitada por la línea de log analizada no debería ser considerada como dato personal.* Indiquen que supone la denominación, y si el dispositivo estuviera ***(...)*** por el titular, porque este log no se consideraría información de su titular ya que le podría afectar en su derecho.

Responde que: "*El log al que se refiere esta cuestión tiene un carácter exclusivamente técnico y se limita a detectar la existencia de un corte en el suministro eléctrico que afecta al dispositivo. SECURITAS DIRECT no puede conocer los motivos por los cuales se ha producido la ausencia de corriente. No obstante, el sistema sigue en funcionamiento, dado que el mismo está dotado de una batería auxiliar que permite su alimentación cuando la alarma se encuentra armada con el objetivo de identificar los incidentes que pudieran producirse durante el corte producido. A tal efecto, resulta irrelevante quién y en qué circunstancias procedió al* ***(...)*** *del sistema de alarma, dado que lo único que refleja el log es la existencia de la ausencia de corriente eléctrica en el dispositivo, de forma que no cabe identificar a persona física alguna por la ocurrencia de este evento ni el mismo aporta información alguna sobre una persona identificada o identificable. Esta incidencia genera la remisión de una comunicación al titular, indicándosele que se ha procedido al* ***(...)*** *eado del sistema como consecuencia del mencionado corte, tal y como puede comprobarse en la documentación aportada por mi mandante. El log generado por dicha comunicación sí contiene datos personales, y así se recoge en el documento remitido al interesado (logs generados el día 15/12/15 a las 4:50:24 que figuran en el documento remitido a aquél*)."

Se observa que en los logs de ese día se inician con anotaciones de no datos, en rojo a las 2:38:07 , cuatro logs, y el siguiente de 2:38:23 si es log dato personal, con información ***(...)*** y a las 4:50:un envió de e mail a dirección del reclamante, continuando figurando varios logs de no dato personal con referencias a "fallo supervisión", "*incidencia cancelada*, *pendiente de mantenimiento*".

-b) porque en varios de estos logs en ¿se considera que son dato personal?, indican como regla general que no, pero que si se recogen imágenes cuando se detectan movimientos a través de los sensores, en caso de que hubiesen captado al interesado, serian datos personales y se debería facilitar a este, y como conocen que la persona que accede es el titular, un autorizado, otro usuario?, y si, no debería informar al titular del hecho de que se han recogido imágenes, en todo caso.

Responde que: "*En relación con estos logs, no todos los sensores instalados en la vivienda del Reclamante recogen fotografías (e.g. en ese punto se hacía referencia a los sensores volumétricos).*

En todo caso, SECURITAS DIRECT sí puede conocer si la imagen, en caso de ser recogida si un salto de alarma implica el desarrollo del correspondiente protocolo (ver, por ejemplo, la respuesta dada al punto 4.17 del escrito de esa AEPD)" (en esta propuesta 3.17) "*que supone la comunicación con aquél o con los contactos designados. De este modo, si de dicha comunicación se derivase que la imagen se refiere al interesado se le facilitaría una copia de la misma, que igualmente sería accesible por aquél desde la App."*

3.29 En que consiste la *descripción extendida* que figura en alguna tabla como "*Matrícula interna del operador que está actuando una incidencia*".
Responde: "*ya se ha indicado en la respuesta a la cuestión contenida en el punto 4.6"* (3.6 en esta propuesta) *"la Matrícula interna del operador que está actuando en una incidencia" es el código alfanumérico interno que identifica de forma unívoca al empleado de SECURITAS DIRECT que está trabajando sobre el dispositivo para solventar o gestionar una incidencia técnica acaecida en el mismo*."

3.30 A que se refieren cuando manifiestan que sobre el sistema se realizan "*Verificaciones autónomas del sistema que se realizan sin intervención ni del usuario ni del prestador de servicio*", y objeto, entre que equipos se produce y si aparece regulado en la normativa de seguridad privada o en su propio protocolo y que puede suponer su no realización.

Responde que: "*Por "Verificaciones autónomas del sistema que se realizan sin intervención ni del usuario ni del prestador de servicio", y siguiendo lo manifestado en la pregunta 4.8"* (en esta propuesta 3.8) "*nos estábamos refiriendo a los test periódicos de comunicación y correcta transmisión del sistema de alarma con la CRA*."

3.31 a En el anexo II, información, indicaron que:

- "*No se han analizado aquellas líneas de log no derivadas de forma directa de los servicios de sistemas de seguridad proporcionados por Securitas (i.e. logs con denominación: FR0 a FSZ; ROF y ROI)". Asimismo, tampoco han sido objeto de estudio aquellas líneas de log que, de conformidad con la información facilitada por Securitas, no tienen aplicación práctica a fecha de redacción del presente informe: IAC, ICA, PID, PDD, TLL y TWC*". Se solicita explicación del significado de esta anotación.

Responde que: "*El significado de estas expresiones se refiere, como del contenido del propio informe puede deducirse, a logs que ya no operan en los sistemas de SECURITAS DIRECT o que no guardan relación con el funcionamiento del sistema de alarma del Reclamante, de forma que no encajan en lo solicitado por éste*."

b) *Existe un log que indica: "VCA/ Available Photo/Video Alarm in CRA Imágenes ya en CRA./ …No obstante lo anterior, las imágenes capturadas, en caso de que hubieran captado a algún sujeto, sí serían datos personales y deberían ser facilitadas al interesado siempre que el solicitante del derecho de acceso coincida con la persona capturada en las imágenes./Se considera dato personal: Si*. Explique por qué si las imágenes captadas del propio titular al detectarse la alarma dichas imágenes no pueden ser cedidas al titular del dispositivo, incluyendo si son las propias."

Respondió que: "*En relación con la entrega al interesado de imágenes capturadas habrá que diferenciar :*

(i) la situación en la que la persona que aparece en las imágenes es únicamente el propio solicitante del derecho de acceso, en cuyo caso deberán otorgarse junto con el resto de los datos personales pertinentes y,

(i) *la situación en la que el dispositivo capta imágenes de un tercero, en cuyo caso no podría otorgarse con el derecho de acceso pues supondría una comunicación de datos personales. En este sentido, el criterio sostenido por SECURITAS DIRECT coincidiría con el establecido por la propia AEPD en relación con el ejercicio de derechos en relación con los sistemas de videovigilancia. Así, en el apartado 2.3.10 de su Guía sobre el uso de videocámaras para seguridad y otras finalidades indica que este derecho "reviste características singulares, ya que requiere aportar como documentación complementaria una imagen actualizada que permita al responsable verificar y contrastar la presencia del afectado en sus registros. Resulta prácticamente imposible acceder a imágenes sin que pueda verse comprometida la imagen de un tercero. Por ello puede facilitarse el acceso mediante escrito certificado en el que, con la mayor precisión posible y sin afectar a derechos de terceros, se especifiquen los datos que han sido objeto de tratamiento". En cualquier caso, los titulares de los sistemas de alarma de SECURITAS DIRECT tienen acceso, a través de la App, a las imágenes captadas por los dispositivos en el momento en que se produce un incidente por salto de alarma mediante un dispositivo con capacidad de captar imágenes. Asimismo, estas imágenes son puestas a disposición de los Cuerpos y Fuerzas de Seguridad del Estado si fuera necesario. En todo caso, el posible acceso por el titular de un sistema de alarma a las imágenes, sin perjuicio de su licitud como cesión de datos, no formaría parte del derecho de acceso del interesado, tal y como se desprende de la doctrina de esa AEPD que se acaba de reproducir, al no referirse a sus propios datos*

b) Explique el significado de este log: "*SID Inactivity time Verificación periódica de movimiento dentro del domicilio. De la información conjunta proporcionada por: (i) el tiempo sin detectar movimiento; y (ii) fecha del log concreto cuando se trate de un análisis de un log real, podría derivarse el conocimiento de ciertos patrones de conducta de un usuario, por lo que esta línea de log podría ser considerada como dato personal. SÍ.*

Responde que: "*El informe aportado como Documento Nº 1 adjunto a las alegaciones al Acuerdo de Inicio, no sólo analizaba los concretos logs generados en relación con el sistema de alarma contratado y ubicado en la vivienda del Reclamante, sino la totalidad de los logs que podría producir un sistema de alarma, incluyendo aquéllos que en ningún caso se dieron en el supuesto controvertido, toda vez que mi mandante quería conocer el alcance de la aplicación del concepto de dato personal en el funcionamiento de los citados sistemas de alarma. Por este motivo, el informe diferenciaba en tres tablas los logs generados en la concreta relación del Reclamante con SECURITAS DIRECT, distinguiendo los que tendrían la consideración de dato personal (tabla 1 del anexo I) y los que no (tabla 2 del anexo I), así como los restantes logs que podría generar cualquier sistema de alarma, analizando si los mismos encajan o no en el concepto de dato personal (anexo II). El log al que se refiere esta cuestión no se encuentra entre los generados en el caso del sistema de alarma del reclamante, por lo que cabe considerar que la cuestión planteada carece de relevancia a los efectos del presente expediente."*

3.32 Si es posible que los logs se superpongan, existiendo por ejemplo el que hay registrado el ***(...)*** de alarma por el titular y posteriormente se vienen registrando otros eventos.

Respondió que: "*Cada línea de log es un registro único con fecha y hora, e incluso puede haber varios en el mismo minuto y segundo al tratarse de "máquinas" pero ello no supone una "superposición", sino la generación de varios logs simultáneos*."

3.33 a) Se solicita que informen si se puede proporcionar al reclamante la tabla ANEXO II que contiene la *(...) de la señal* y los *descriptores*,(informe de 29/01/2021, aportado por la reclamada en alegaciones) y motivo en caso de que fuera negativo.

Responde que: "*el anexo II se refiere a logs que en ningún momento se han generado en el sistema de alarma del* reclamante, *de modo que dicha información en ningún caso se relacionaría con su Contrato, con independencia de que la misma tuviera o no el carácter de dato personal. Al propio tiempo, como también se ha puesto de manifiesto en las alegaciones al Acuerdo de Inicio, el funcionamiento de los sistemas de alarma de mi representada y los logs que generan constituye un activo de SECURITAS DIRECT protegido por las normas que regulan el secreto comercial. De este modo, siendo irrelevante la información para el interesado y encontrándose, por el contrario, mi mandante protegida por el secreto comercial consideramos que ni la normativa de protección de datos personales, ni ninguna otra autorizan que aquél tenga acceso a esa información*."

Se aprecia que el Anexo II, llamado "*análisis general sobre la consideración de dato personal*" que se encuentra en el documento 1 aportado en alegaciones al acuerdo , contiene una clave de letras llamada "*(...) de la señal*" que también figura en el cuadro del documento 2, señales en verde, datos del reclamante, y que coincide con el formato del entregado al reclamante el 14/12/2021. A titulo de ejemplo, figura tanto en anexo II como en el cuadro entregado al reclamante: IDE, la descripción de la señal "*External disarm*", así como la descripción extendida proporcionada por SD y una explicación de vinculación de forma directa o mediante inferencia a conducta o

información de persona física, y SI en dato personal, por lo que se trataría de explicaciones que tienen que ver con el contenido de lo que se le ha proporcionado

b)-Motivo por el que en anexo I, tablas I y II, no se contiene la *clave (...) de la señal* y su *descripción* que se contiene en la tabla de ANEXO II

Respondió que: "*Ha de hacerse nuevamente referencia al alcance del informe al que se refiere esta cuestión, en que cabía diferenciar los logs efectivamente generados en el sistema del Reclamante de los que no se habían generado, de forma que mientras los primeros podían diferenciarse en función del momento en que se produjeron, los segundos únicamente podían referenciarse por una denominación específica. Esa y no otra es la razón por la que las tablas de ambos anexos difieren, del mismo modo que en las tablas contenidas en el anexo I se indica si procede o no incluir el correspondiente log en la respuesta facilitada a la solicitud de ejercicio del derecho de acceso, que por motivos obvios no figura en la tabla del anexo II*."

3.34 En caso de salto de alarma en el domicilio, ¿a qué persona se le trasladaría la información?, ¿al último usuario que figura logado en la conexión de la alarma?, ¿al titular?, ¿bajo qué presupuestos? Y ¿cómo los identifica en los logs? -Detalle en este caso, algún log que considere dato personal y que motivado por el salto de alarma, se haya dado información a esa persona.

Responde que: "*El protocolo de actuación en caso de producirse un salto de alarma, y que se siguió en el caso del Reclamante en el salto de alarma de fecha 27/11/2015, es el siguiente:*

• Llamada a habla/escucha de la central de la alarma. (Verificación por Audio).

• Llamada a teléfono fijo de la vivienda en que se encuentra el sistema, si se dispusiere de ese dato.

• Llamada a los contactos designados en el orden establecido por el titular del contrato en el plan de acción que consta en el Contrato y verificación de la palabra clave.

• Información al contacto en caso de lograrse una comunicación con el mismo y la verificación de la palabra clave.

• Comunicación a las Fuerzas y Cuerpos de Seguridad en caso de existir indicios suficientes de la posible existencia de un delito (en el caso de 27 de noviembre de 2015 no se llegó a ejecutar porque no se consideró una alarma confirmada)."

"*En relación con el concreto supuesto analizado, como se ha descrito en varias respuestas anteriores, el interesado designa en el Contrato hasta cuatro contactos, estableciendo igualmente un orden de prelación en la comunicación a los mismos de una determinada incidencia. Una vez se consigue contactar con uno de los contactos designados, se le solicita la palabra clave, sin la cual no se le proporciona la información sobre el incidente identificado. Así sucedió en el salto de alarma producido el 27 de noviembre de 2015, en cuyos logs puede apreciarse como se intentó el contacto sucesivamente con las personas designadas en primer, segundo y*

tercer lugar, siendo infructuoso, y como la contactada en cuarto lugar no facilitó la palabra clave."

3.35 En sus alegaciones al acuerdo de inicio indicaron que:

"*Presentada la información, la Agencia también hace mención del "salto temporal entre el día 27/11/2015 a las 20:17 y el 4/12/2015 a las 11:05, sin explicar el motivo de esa ausencia de "logs" en ese intervalo de tiempo*". *Sobre esta afirmación no puede esta parte sino manifestar, dicho sin ánimo de ofender a la Agencia, que no se corresponde a la realidad y basta con acudir al escrito presentado por esta parte a la Agencia en fecha 18/06/2021 (páginas 106 y 107 del expediente) donde mi representada pone de manifiesto (citamos textualmente lo manifestado por SECURITAS DIRECT) "ésta generó "logs" hasta las 20:09 horas del día 27/11/2015, hora y fecha en la que se produjo la intrusión en el domicilio del reclamante y durante la cual, dicho sistema de alarma quedó completamente inutilizado. A partir de esa fecha, no pudo generar más logs". Además, y en relación con la memoria interna del dispositivo, también esta parte puso de manifiesto en su escrito de 18/06/2021 (páginas 106 y 107 del expediente) "(…) tras el análisis de la memoria interna de la alarma instalada sólo constaba un "log" generado para ese marco temporal, el cual constaba en nuestro burofax de fecha 26/02/ 2021".*

a) Se hace notar que figuran logs en ese periodo que son considerados no datos personales. Al respecto, se le solicita que indique como se inician tales logs y como finalizan.

Responden que: "*Como ya se ha indicado en reiteradas ocasiones los logs a los que se refiere la pregunta se corresponden con los generados directamente desde un operador de SECURITAS DIRECT en la CRA, y consisten básicamente en los sucesivos intentos de comunicación con los interesados para comunicar la incidencia y verificar el estado de la alarma. No se trata de los comunicados desde la centralita ubicada en el domicilio del reclamante, que al resultar inutilizada no podía generar ningún tipo de log o señal, como ponen de manifiesto los logs que el sistema generó entre las 22:21:18 horas del 28 de noviembre de 2015 y las 11:04:50 horas del día 4 de diciembre de 2015, a los que se ha hecho referencia en un lugar anterior de este escrito."*

a) Igualmente expliquen cómo se liga la interrupción con el primer log de reanudación,(catalogado en verde) 4-12-2015, 11:05:04, que evento la produce y que información personal proporcionaría este.

Responde que: "*El citado log es el resultado de comprobaciones técnicas a través de un sistema automático que se denomina GTI (como aparece en el propio log) que se encarga de llevar a cabo varias verificaciones para conocer el estado técnico del sistema, procediendo a la apertura de un mantenimiento cuando resulta necesario. En este caso, un operador se encarga de llamar al cliente para hacer una revisión con el cliente en línea y si no es posible, concertar una visita de un técnico para verificar el estado del sistema*".

Se aprecia que el día 4/12/2015 como en días anteriores figuran logs en color rojo, mientras que a partir del 28/11/2015 todos están en rojo.

3.36 a) En el documento 2 de alegaciones, -total logs- cuadro Excel de todos los logs, diferenciados en color rojo-no dato-, verde, si, figura:

Con distintas claves de la "***(…)*** *del evento*" distinguidos en rojo los considerados no datos personales, ejemplo, hay dos en rojo, de 27/11/2016 20:09:47, y otro misma fecha y hora, en verde. En qué se asemejan y en qué se diferencian en cuanto las referencias de sus contenidos en lo que a información sobre datos personales que pueden contener.

b) En este caso, por ejemplo detalle la diferencia de estos dos logs (de no datos personales) en cuanto a origen y porque al mismo tiempo, en este caso, uno si se considera dato personal y el otro no.

Igualmente, si desea, comentar otros logs -no datos personales- que coinciden fecha y hora.

Responde que: "*Como se ha expuesto en la respuesta a la pregunta contenida en el punto 4.17"* (3.17 en esta propuesta*)" los logs se refieren a eventos distintos: el primero implica la detección de un salto de alarma detectado por un sensor volumétrico; el segundo implica la generación de un código de desactivación en caso de que sea necesario acudir a la vivienda una vez realizadas las verificaciones correspondientes, que constan igualmente en la tabla de logs; y el tercero se refiere a la cobertura **(...)***."

c)Explique si parece posible que como sucede con las marcas de los logs de no datos personales que puede haber más de uno en la misma fecha y hora, si podría también haber dos de misma fecha y hora para que se registraran logs de los considerados datos personales, algún ejemplo, y si en los del reclamante se da en algún caso.

Responde que:" *La respuesta a esta pregunta sería que sí es posible y un ejemplo de ello son los siguientes logs marcados en verde que se refieren a mantenimientos presenciales de cambio de alarma. Son varios logs que ocurren en el mismo momento temporal. 05/12/2015 18:38:10*:", indicando cuatro movimientos de la misma fecha y hora.

OCTAVO: Con fecha 2/02/2023, se emite propuesta de resolución del literal:

"*Que por la Directora de la Agencia Española de Protección de Datos se sancione a* **SECURITAS DIRECT ESPAÑA, S.A.**, *con NIF* ***A26106013****, por una infracción del artículo 58.2 c) del RGPD, de conformidad con el artículo 83.6 del RGPD, tipificada como muy grave en el artículo 72.1.m) de la LOPDGDD, con una multa de 50.000 euros.*

Con arreglo al artículo 58.2.c) del RGPD se propone que se atienda el cumplimiento del derecho de acceso completo y comprensible, como se explicita en el último fundamento de derecho y se desprende del sentido de esta propuesta."

NOVENO: Con fecha 20/02/2023, la reclamada realiza las siguientes alegaciones:

A) Sobre los logs técnicos y su asimilación con datos de carácter personal, manifiesta:

1-El dispositivo en ningún momento estará bajo la influencia del reclamante, ni tendría capacidad de ejercer una influencia sobre el reclamante ya que no tiene capacidad de configurar o modificar los parámetros técnicos que afectan al modo de funcionamiento y la configuración establecida por SD para su interacción con la central receptora de alarmas.

2-"*Si bien el número que identifica el dispositivo en relación con el contrato celebrado con un determinado cliente ha de ser considerado dato personal al vincularse con la parte en dicho contrato*", la interpretación llevada a cabo por la AEPD en su propuesta desvirtúa el concepto de dato personal, y, en consecuencia, la aplicación del RGPD, al entender que cada actuación técnica sobre ese dispositivo es un dato personal del reclamante, es decir, que constituye información "*sobre*" él, y que, por tanto, ha debido de ser aportado en el derecho de acceso.

- La información de los logs técnicos no tiene incidencia en o sobre el interesado, ni siquiera indirecta, al tratarse de señales y comunicaciones efectuadas entre maquinas que, en todo caso, son ajenas al propietario de la vivienda sobre la que se instale el sistema y no afectan al mismo, ni directa ni indirectamente.

3- Reitera el sentido del Dictamen 4/20007, sobre los requisitos que deberían concurrir en la información para entender que pueda ser considerado dato personal, cuando la misma "*verse sobre una persona identificada o identificable*". "*En el marco de sus debates sobre los problemas de protección de datos planteados por las etiquetas RFID, el Grupo de trabajo señaló que un «dato se refiere a una persona si hace referencia a su identidad, y sus características o su comportamiento o si esa información se utiliza para determinar o influir en la manera en que se la trata o se la evalúa*".

Para considerar que la información referida a un objeto concreto, el dispositivo de alarma, instalado en el domicilio del reclamante pueda ser considerado dato personal, por versar sobre una persona, debe haber un elemento de contenido, o de finalidad, o de resultado. Ya en el informe aportado en el acuerdo de inicio se indicaba:

- La información debe referirse a una persona física específica, por lo que la información en los logs deberá, como mínimo encontrarse en una de las siguientes situaciones:

a.1 Estar vinculada directamente con un individuo determinado, de manera tal que proporcione información directa sobre su forma de actuar, sus características mentales o físicas, sus preferencias, sus habilidades o cualquier otro patrón de conducta que pueda atribuirse directamente a la misma, o

a.2 Pueda utilizarse para evaluar o influir de cualquier forma en un individuo determinado o en su conducta, o

a.3 Pueda repercutir directamente en los derechos e intereses de un individuo determinado.

De dicha conclusión, se infería que los logs técnicos no podían ser considerados datos personales por referirse únicamente a un objeto y no encontrarse en ninguno de los supuestos mencionados.

La valoración de la propuesta solo alude a que los logs técnicos son datos personales por el hecho de que se vinculan al identificador del sistema de alarma, y este, vía contrato al reclamante. Estima que no concurren los requisitos de "*contenido*": No aporta información de manera directa acerca del interesado, de la "*finalidad*": el objetivo de los logs técnicos no es evaluar, tratar de determinada manera o influir en la situación o comportamiento de una persona, ni de "*resultado*": que "*concurriría si el uso de la información repercutiera o pudiera repercutir en los derechos y los intereses del reclamante*" , "*ya que no existe posibilidad de que mediante la información obtenida de los logs técnicos pueda afectarse de manera alguna los derechos e intereses del interesado que no guarda relación alguna con las operaciones que constituyen dichos logs*". El "*uso de esta información podría suponer un trato diferenciado o discriminatorio del interesado o una afectación en su ámbito personal*".

4- La consideración como dato personal de la información contenida en los logs técnicos no se ve afectada porque se refiera a la interconexión CRA-dispositivo de alarma instalado en el domicilio del reclamante, ya que la finalidad de este, en nada puede determinar la naturaleza del dato personal o no de las señales que el mismo emite. Si se sigue este razonamiento cualquier información relacionada con un objeto podría conducir a la consideración del mismo como dato personal, al verse afectada su utilidad o el objeto por el que el mismo ha sido adquirido o se deriva de un servicio contratado por el interesado,

Además, considera que informaciones relacionadas con máquinas o sistemas, no tienen necesariamente la condición de datos personales en caso de que no revelen información sobre una persona identificada.

Pone como ejemplo los datos mixtos (personales y no personales) que pueden vincularse o no inextricablemente, pudiendo entrar en el ámbito del derecho de acceso, o no, lo que supone que solo los datos personales del conjunto sean accesibles para el interesado, según se recoge en las directrices 1/2022 del EDPB sobre el derecho de acceso. Finaliza indicando que estas circunstancias son extrapolables al presente caso, en el que la operación interna del dispositivo y su interacción con la CRA, sin incorporas mas información que la relevante para verificar y analizar el funcionamiento de los sistemas de alarma contratados.

Sobre el cumplimiento y su modo, en cuanto a la solicitud de acceso del reclamante, manifiesta:

1-Al margen de la consideración que se tenga sobre la naturaleza de dato personal de los logs técnicos, que no es el objeto de esta alegación, la información excluida no tiene el carácter de dato personal, habiéndose dado acceso únicamente a lo que se refiere a los datos personales sometidos a tratamiento por el responsable que recibe la solicitud.

2-Ha tratado de dar respuesta al reclamante en los términos que el mismo ha solicitado, e incluso facilitarle la comprensión de la información aportada. Fue el reclamante quien, una vez facilitada información que pretendía clarificar el alcance de cada uno de los logs

facilitados consideró que lo que debía facilitarse eran los logs "en bruto", sin la agrupación y clarificación previamente efectuada, para luego considerar que esa información tampoco le satisfacía, por ser, a su juicio, poco comprensible. Lo que persigue el reclamante es la información generada por el sistema de alarma, dado que entiende que se produjo un fallo en su funcionamiento que dio lugar al robo en su propiedad

B) Sobre la revelación del "*know how*", manifiesta:

1-La Ley 1/2019 de 20/02/2019, de secretos empresariales, pretende garantizar y proteger los conocimientos técnicos y la información empresarial no divulgados contra su obtención utilización y revelación ilícitas. En este caso, tiene encaje como información a la que se está haciendo referencia, que revela los procesos internos y el modo de funcionamiento de los sistemas de alarma instalados y en la consideración del artículo 1.1 de la ciada Ley

2-La información de sus sistemas y procesos constituyen un activo. La seguridad que se puede comunicar con los logs técnicos debe ser adecuadamente protegida para evitar el acceso por terceros que podrían conseguir burlar o eludir el funcionamiento de dichos sistemas.

La información que se proporciona en los logs contiene una actividad informativa y registrada a través de sus propios sistemas de información (es decir, estado actual de programas, seguridad, accesos, conectividad de redes, etc.), y por ende, dichos resultados de información generan una metodología de trabajo estandarizada y que es propia de SECURITAS DIRECT.

Vincula la revelación de esta información a la seguridad de los usuarios de sus sistemas de alarma, como garantía del interés general y la preservación de la seguridad que afecta a la totalidad de los logs generados. Considera que el derecho individual del reclamante no puede prevalecer sobre la garantía de la integridad y seguridad de todos sus clientes.

3-Los empleados tienen acceso a la información por su vinculación laboral, y carece de relevancia lo que se indica en la propuesta, al quedar al margen de la aplicación de la normativa de secretos empresariales, cuya eficacia es externa a la empresa. "*Los logs utilizados en los dispositivos de su propiedad, proporcionada al Reclamante, contienen información no personal que, utilizada de manera automatizada y en conjunto, proporciona una serie de señales que, estudiadas de forma agregada, proporcionan a SECURITAS DIRECT una información relevante y propia para la mejora de los servicios de seguridad que proporciona, amén de describir, en su reproducción secuencial, los procedimientos internos seguidos por los sistemas de mi representada, cuya revelación a terceros podría producir un menoscabo de sus derechos*."

4-El "*secreto comercial*" a proteger, no proviene del estudio de un único log (recordemos que sin tratamiento de datos), sino que dicho "secreto comercial", proviene del estudio conjunto de todos los logs, que permite que SECURITAS DIRECT sea capaz de anticiparse a los hechos que puedan acontecer y afectar a la seguridad de sus clientes,

pudiendo adoptar las medidas y garantías que se derivan del estudio y análisis de esos logs.

5-De los logs técnicos, solamente se observan medidas técnicas y algorítmicas comunes a todos los dispositivos, utilizadas en su conjunto para proporcionar a los usuarios un nivel elevado de seguridad en el servicio que se proporciona. Considera que "*no procede la revelación de su know how, al proporcionar logs que son utilizados de manera exclusiva para proporcionar el servicio que ofrece a todos sus clientes, ya que de hacerlo, no sólo estaría situándose en desventaja con el resto de sus competidores, sino que, lo que es mucho más grave, se vería afectado el derecho a la integridad personal de sus clientes y quienes residan con los mismos, bien que consideramos cuando menos de similar protección al derecho a la protección de datos personales*."

6-Además, en el fundamento de derecho X de la propuesta, se estima necesario proporcionar la descripción de los procesos a través e la claves que permitan clarificar la citada tabla y sus apartados que hagan comprensibles los cuadros de los datos en formato de línea o en bruto, como los obtiene la reclamada, lo que considera que multiplica el riesgo de perjuicio para todos sus clientes. Estima que para "*garantizar la integridad y adecuado funcionamiento de sus servicios, considera que no puede proporcionar al reclamante la totalidad de los logs, puesto que de hacerlo estaría poniendo en peligro la seguridad del más de un millón y medio de clientes que contratan sus servicios*".

7-Considera que el secreto comercial de sus derechos resulta mucho más relevante, por interés general y la preservación de la seguridad.

C) En virtud de lo anteriormente alegado, solicita el archivo de la imputación. Además, sobre la graduación de la sanción, señala:

1-Sobre la aplicación del artículo 83.2.a) del RGPD, parte de la base de que se confunde lo que es un elemento del tipo sancionador con una circunstancia agravante y las circunstancias señaladas toman en cuenta para delimitar la supuesta infracción, así como para agravarla, "*lo que vulnera toda proporcionalidad*".

2-Considera que la información proporcionada no está ni es incompleta, ni un mero "*resumen con información escasa*", y que se proporcionó de dos maneras diferentes y complementarias.

Solicita que como atenuantes, se tenga en cuenta que atendió en varias ocasiones la solicitud del interesado otorgándosela en diversos formatos, negándose la buena fe en la propuesta.

DÉCIMO: De las actuaciones practicadas en el presente procedimiento y de la documentación obrante en el expediente, han quedado acreditados los siguientes:

HECHOS PROBADOS

1) El reclamante dispone de una residencia vacacional sobre la que desde 30/07/2014, tenía suscrito con la reclamada un contrato de servicio de seguridad que incluía instalación, mantenimiento y explotación de una central de alarmas.

2) El reclamante manifiesta que al acceder a su vivienda, el 4/12/2015 por la tarde, descubrió, que habían sufrido un robo encontró "la central de alarma" destrozada sin haber sido avisado, recibiendo una llamada de la Compañía esa misma mañana indicando la existencia de problemas de conexión.

3) El reclamante ejerció su derecho de acceso ante la reclamada el 7/04/2017 "*respecto a toda la información obrante en los servidores de Securitas Direct relativa a los registros y señales enviadas por el equipo de alarma instalado en su propiedad, así como las copias existentes de los registros contenidos en la memoria interna de la alarma entre los días 26/11 y 18/12/ 2015*". La reclamada contestó que los registros contenidos en la alarma no entran dentro de la categoría de datos personales, acudiendo el reclamante a la AEPD que resolvió en recurso de reposición el 2/01/2018, estimar la pretensión del reclamante e indicando que se le facilitase el derecho. La reclamada impugnó el acuerdo en la vía contencioso-administrativa, resolviendo la Audiencia Nacional, sección primera, el 23/07/2019, en su recurso 146/2018, desestimando su pretensión y confirmando la resolución.

4) Con fecha 23 y 24/03/2021, el reclamante presenta un nuevo escrito ante la AEPD, señalando que ejerció el mismo derecho ante la reclamada el 2/02/2021, recibiendo una respuesta de 23/02/2021, con una tabla Excel que el reclamante estima que no atiende el derecho.

La tabla Excel que contiene el acceso que se proporciona al reclamante comprende un total de 94 líneas de logs, más una de un período de tiempo del día 5/12/2015, relacionado, según la reclamada, con pruebas en el sistema de alarma como parte del mantenimiento de la instalación.

La tabla es una elaboración de la reclamada, de lo que según indica, "*son datos personales*". Se inicia por fecha, no cronológicamente ordenada y se agrupan al nombre, "*nomenclatura del log generado*" junto a una descripción realizada por la reclamada, "*descripción extendida del log*" que pretende informar o definir en que consiste. Esa definición o "*descripción extendida del log*" es genérica en el detalle de la incidencia. La "*nomenclatura del log generado*" también tiene un nombre general como: "*Señal informativa*""***COLUMNA.1*" o dentro de la misma existen variadas, como "*actuación CRA*", sobre la que figuran "*comunicando"*, "*salta buzón de voz*", *LOCSIN*. Por mencionar algunos ejemplos:

a)"*(...) externo perimetral*" "*nomenclatura del log generado*":" "*Central Seguridad prioridad baja*."

b)"*Distintas actuaciones genéricas del operador humano de Securitas ante una incidencia concreta, ejemplo habilitación del habla/escucha, llamada a los distintos contactos listados, comentarios internos en relación a una información que le transmiten los contactos etcétera*"- "*nomenclatura del log generado*":" "*actuación CR*A".

En algunos logs se refiere a "*contacto*", sin identificar o especificar a que contacto se

refiere, como "*contacto no recuerda la palabra clave para acreditar la identidad y cerrar la incidencia*", o "*los contactos a los que el operador de Securitas trata de localizar no contestan*", "*operador consigue hablar con contacto*".

5) La reclamación dio lugar a que la AEPD trámite el procedimiento de ejercicio de derecho TD/00167/2021 en el que la reclamada antes de su admisión a trámite e inicio, el 19/05/2021 manifestó que no todos los logs que registran las señales de los equipos de alarmas, así como los contenidos en la memoria interna de la misma se pueden considerar que contienen datos de carácter personal. Refiere que ha elaborado un informe a través de un despacho de Abogados, firmado el 29/01/2021 titulado "aplicación del concepto de dato personal a los señales o logs generados por los sistemas de alarma" que indicaba los logs que considera "no implican tratamiento de datos personales, y enumera las categorías de los logs que considera, se encontrarían en este supuesto:

1) "*Emisión de señales de carácter puramente técnico de comunicación entre los dispositivos como parte del protocolo de verificación de su correcto funcionamiento o para el registro de algún fallo técnico".* Pone como ejemplos en su escrito de recurso frente a la TD/00167/2021*: "el nivel de batería del dispositivo, desconexión de la red, inhibición, etcétera*". Se trataba de la "*Emisión de señales de carácter puramente técnico de comunicación entre los dispositivos como parte del protocolo de verificación de su correcto funcionamiento o para el registro de algún fallo técnico".*

2) Registro de señales informativas en relación con, entre otras, la versión del sistema, modelo o categoría del dispositivo instalado.

3)Registro descriptivo de procedimientos internos y técnicos ante un evento concreto". Pone como ejemplos en su escrito de recurso frente a la TD/00167/2021*: "tiempos de espera procedimentados ante un evento, recogida y descripción del evento, proceso de captura y puesta a disposición de los operadores de la imágenes o sonidos, modificación de parámetros internos, traslado del evento a un operador etcétera". Se refería a "Registro descriptivo de procedimientos internos y técnicos ante un evento concreto".*

4) Registro de señales técnicas en relación con la configuraciones de los dispositivos que no proporcionan información sobre el interesado o sus hábitos sino que simplemente refleja en calibraciones de los sistemas de Securitas para su correcto funcionamiento.

5) *Información estadística acerca de los dispositivos*." Pone como ejemplos en su escrito de recurso frente a la TD/00167/2021: "*número de fotos captadas, dispositivos activados, calidad de las respuestas de los dispositivos, número de desconexiones, etc.). Se refería a "Información estadística acerca de los dispositivos*".

Además, indica:

-"*dichos logs*" podrían contener información sobre procesos técnicos internos de la reclamada cuya revelación a terceros podría implicar difusión de secretos comerciales. Menciona a tal efecto el considerando 63 del RGPD.

-El acceso de logs proporcionado al reclamante excluía los técnicos o que afectan a terceros.

Copia del citado informe resultó aportado el 6/07/2022 en alegaciones al acuerdo de inicio como documento 1.

1) Con fecha 7/06/2021 se acordó por la Directora la admisión a trámite del procedimiento de "ejercicio de derechos arts. 15 a 22", TD/00167/2021 en el que la reclamada manifiesta el 18/06/2021:

"*En relación con el contenido de la "memoria interna de la alarma instalada en el domicilio del reclamante, esta generó logs hasta el 27/11/2021, 20:09, hora y fecha en la que se produjo la intrusión en el domicilio durante la cual dicho sistema de alarma quedó completamente inutilizado*. Según la reclamada, el sistema registró y envío señales de captación de movimiento a las 20:09 h del 27/11/2015. A partir de esa fecha, no pudo generar más logs de ningún tipo. Por tanto, en el marco temporal entre el 26/11 y 18/12/2015, la memoria interna solo pudo generar logs los días 26 y 27/11/2015, y solo constaba un log generado en ese marco temporal el cual constaba en la respuesta dada *al reclamante el 23/02/2021*. Aportan documento 1, que es el cuadro con columnas del acceso que se le dio al reclamante en esa fecha, en el que *aparece marcado en verde fluorescente ese log:*

"*27/11/2015 20:09:47/CENTRAL PRIORIDAD ALTA/Código generado automática y aleatoriamente por el sistema para que el vigilante desactive la alarma*".

El reclamante manifestó que tampoco se le han dado los datos de los registros contenidos en la memoria a partir de la nueva instalación de 5/12/2015 que se comprende en la petición.

Con fecha 17/09/2021 se resolvió la tutela, acordando estimar la reclamación y se otorga un plazo para atender el derecho, siendo la resolución recurrida por la reclamada en reposición el 18/10/2021, resolviéndose el 27/10/2021 su desestimación, figurando notificado electrónicamente a la reclamada el 28/10/2021.

2) Con fecha 21/12/2021, la reclamada presenta escrito en el que manifiesta haber enviado copia de acceso al reclamante, aportando remisión de escrito de 14/12/2021, en el que figura copia de documentación que se ha enviado al reclamante por burofax. El documento comprende la remisión de los logs en formato "*líneas de código*", el que se recoge en los sistemas de SD de los registros y señales enviados por el equipo de alarma. Según la reclamada, es la "*transcripción literal, en el formato en que se recoge en los sistemas de SD de los registros y señales enviados por el equipo de alarma."*

El reclamante presentó escrito el 7/05/2022 en el que considera que se sigue sin cumplir con lo resuelto ya que el reclamado clasifica los logs que son datos personales de los que no lo son, es un cuadro ininteligible, la expresión de las descripciones imprecisas, la letra muy pequeña.

En el cuadro con hojas "*excel*" proporcionado al reclamante, el 14/12/2021, se contienen los logs por orden cronológico de fecha y hora y figuran en total 19 columnas informativas susceptibles de contener definiciones como: "(...) de la señal", que se correspondería con los cuadros del anexo II aportado por la reclamada en alegaciones al acuerdo de inicio, donde se describe de forma extendida su significado, no proporcionado al reclamante, .

También se comprenden en las hojas de 14/12/2021 campos como descripción y una descripción mas amplia en "descripción ***(...)***", "*event*", "*event (...)*" "*Zone*", "******COLUMNA.3***", "****COLUMNA.4*". "******COLUMNA.1***", "*tiempo de* ***(...)***", por nombrar solo varias con significados y claves que no se dieron al reclamante.

En pruebas, la reclamada explicó por ejemplo, que los códigos alfanuméricos que aparecen en la columna *"SIGNAL",* se trata del mensaje generado en el propio lenguaje del sistema de alarma *(lenguaje máquina)* que se traduce en la información que aparece en el resto de las columnas y esencialmente en la columna de "****COLUMNA.2* ***(...)***". Para entender el significado del código, hay que ir al campo de esta columna*. El sistema remite mensajes que incorporan códigos alfanuméricos que posteriormente se traducen en las diferentes columnas del Log presentado. La columna "SIGNAL", recoge la parte del mensaje en "bruto" del sistema que luego se traduce en el resto de las columnas.*

A tal efecto, la reclamada explica que:

• La columna "****COLUMNA.2* ***(...)****"* es la traducción del evento de lenguaje de sistema para que el agente/operador entienda de qué trata el mensaje. Esta información se complementa con las columnas "******COLUMNA.1***" y "****COLUMNA.2*", que contienen información complementaria para que el agente/operador pueda entender el evento que se recibe en la CRA*.*

También figura en los logs de carácter personal proporcionados al reclamante.

• La columna "ZONE", identifica el dispositivo de la alarma en el que se produce el evento (eg. (...), identifica un fotosensor grabador en la posición 2 de programación) y la columna "AREA" describe la zona de la instalación que corresponde (eg, Home Sal??n)

*• La columna "*******COLUMNA.3****" indica la prioridad de la señal, siendo los valores inferiores los de mayor prioridad.*

*• La columna "*******COLUMNA.4****", contiene el tipo de señal que representa al evento (e.g. INF es el código que se asocia a "información", que aparece en el ***COLUMNA.2* ***(...)****, SS se asocia a "supervisión", como se recoge también en el ***COLUMNA.2* ***(...)****, CC se asocia a "coacción", SO se asocia a "SOS", AAC se asocia a "corte de corriente", etc.…). De este modo, estos códigos se vinculan directamente con la información contenida en la columna ***COLUMNA.2* ***(...)****."*

En documento 1 (INFORME de 29/01/2021, aportado por la reclamada en alegaciones), ANEXO II se ofrece un análisis general de la consideración como dato personal de las líneas de log genéricas que pueden ser utilizadas en los sistemas de SD durante el desarrollo de su actividad, sin aplicación especifica a ningún interesado. El cuadro relata las distintas "*clases de señal*" a las que se asocian los diferentes tipos de logs, completados con "*descripción*", "*descripción extendida"* explicada por SD, "*vinculación con la persona física*" y "*si se considera una dato persal o no,*

Sin embargo existen 19 columnas que contienen claves e incluso descripciones inespecíficas como "señal informativa" que no resultan comprensibles sin una correlación explicativa.

3) En el contrato se seguridad suscrito entre el reclamante y la reclamada, figuraba que el sistema de alarma contratado por el reclamante disponía, entre otros, de fotodetectores, dispositivo que cuenta con un sensor de movimientos por infrarrojos, una microcámara y un flash, para caso de intrusión, salte la alarma que dispara la cámara y envía el aviso y las imágenes captadas a la Central Receptora de Alarmas (CRA), elemento de verificación por audio, habla-escucha, que se *encuentra en el interior del panel de control y sirve para realizar verificaciones de audio y escucha en caso de salto de alarma, también sirve para hablar con el cliente a través de la centralita o panel de control*

4) El mantenimiento básico incluía para el cliente: los servicios de comprobación remota del funcionamiento de todos los componentes (chequeo técnico según normativa vigente), actualizando el software y los componentes del mismo, con el único fin de prestar los servicios de seguridad.

10) En el contrato, la reclamada indica que dispone de un fichero de gestión de imágenes y sonidos que puede captar a través de sus sistemas de videovigilancia cuando se produce un salto de alarma en los domicilios de los clientes. Se agrega que "*El CLIENTE sólo podrá tener acceso a información sobre cualquier incidencia o grabación realizada con motivo de un salto de alarma, enviando solicitud escrita a través de los medios que así lo permitan indicados en la cláusula 20 de las condiciones generales, en la que deberá constar la identidad del titular del contrato acompañando fotocopia de su DNI, CIF, NIE o pasaporte en vigor, así como la fecha, hora y lugar en el que presumiblemente sucedió la grabación*".

11) Como parte del contrato figura el "*plan de acción*" en el que figuran las definiciones:

-"CLIENTE: Persona física/jurídica que firma el CONTRATO, que es propietaria del sistema de alarma descrito en el citado CONTRATO y que es poseedor de la palabra clave maestra. El CLIENTE podrá tener en cualquier caso la condición de usuario"

USUARIO: Persona física a la que el CLIENTE autoriza el acceso al inmueble y al uso del sistema de alarma, poniendo a su disposición los medios de conexión y/o desconexión del mismo.

"PERSONAS DE CONTACTO: Persona física que puede coincidir o no con el CLIENTE del contrato y que es poseedora de la palabra clave maestra."

- Clave MAESTRA CLIENTE: Identifica al CLIENTE y a los contactos principales. Debe ser proporcionada por estos cuando contacten con SECURITAS DIRECT telefónicamente. Permite y da acceso a todo tipo de gestiones y modificaciones, ya sean administrativas (contrato, plan de acción, etc.), u operativas (verificación de saltos de alarma).Para que ud. Se identifique ante Securitas")

- Clave COACCION: En la llamada de verificación ante un salto de alarma debe facilitarse a SECURITAS DIRECT, por quien se encuentre en el inmueble ante una situación de peligro real para su integridad física y/o patrimonial.

También figura una "*CLAVE SECURITAS*", "*para que Securitas se identifique ante usted*."

Figuran :

-*"lista de contactos*", cuatro personas identificadas por nombre y primer apellidos, numeradas, el reclamante, cliente, con dos teléfonos, el resto con uno, todos con llaves.

Los cuatro figuran en otro listado de "*plan de acción estándar*" en el cuadro, ordenados como "*contacto*" de 1, el reclamante, a 4.

En las condiciones particulares, el reclamante añade su e mail.

12) Preguntada la reclamada en pruebas sobre el modo por el que se identifican en los logs, las distintas acciones de los posibles usuarios en sus distintos roles que puedan asumir: titular, autorizados, contactos y en los distintos elementos del sistema, manifestó que se identifican por la reproducción en el log de la interacción que se pueda producir con cada uno de ellos, aclarando que los "*usuarios con acceso al sistema*" se corresponden con personal de SD que pueden recibir una determinada incidencia con el titular o aquellos contactos designados y en su caso, llevan a cabo las operaciones solicitadas por aquéllos, que dan lugar a logs que fueron consideradas como datos personales del reclamante, al proceder de una acción instada por éste o sus autorizados. Figuran otros logs que responden a esta premisa como los comprendidos entre el 05/12/2015 a las 14:19:04 y las 14:45:45, proporcionados al reclamante, donde ***USUARIO.1 accede a la ficha de cliente para gestionar y acordar un mantenimiento con el cliente asociado al evento que ocurrió el 26/11/2015.

Si se examina el cuadro Excel de acceso proporcionado al reclamante entre el 05/12/2015 a las 14:19:04 y las 14:45:45, solo figura "*el operador visiona las palabras de código bajo demanda*", "*evento (...)*" y que accede a la ficha del cliente, sin figurar que titular o contacto causa la petición.

El de 18/12/2015 a las 20:08:18, como consecuencia de una llamada del cliente a SECURITAS DIRECT en el mismo sentido, sin figurar que titular o contacto causa la petición. Apreciándose que en ese mismo día, existen logs proporcionados al reclamante, que responden a "*evento inyectado servicio APP, conexiones desconexiones remotas*", sin que se correlacione el causante de la petición, fuera titular o alguno de los contactos autorizados.

13) Además, a través de una aplicación instalada en el teléfono móvil, los usuarios o personas de contacto autorizado pueden interactuar con el sistema de alarma, siendo el teléfono móvil un medio de comunicación del personal de seguridad con el reclamante al que remiten SMS o e mails. La reclamada en pruebas manifestó que "con el dispositivo móvil se puede conectar o desconectar el sistema de alarma, y que dicha incidencia se registra en la memoria interna del dispositivo, aunque sólo se transmite a la CRA en caso de que la actuación responda a la existencia de una incidencia de seguridad. En ese supuesto, es decir, cuando se produce una incidencia de seguridad (e.g. desconexión como consecuencia de un salto de alarma) y posteriormente se desconecta el sistema, el log queda registrado en la CRA identificando al usuario (llave, mando o código) que ha realizado la acción. Igualmente, si la desconexión o la conexión se realiza desde la App se transmite el log a la CRA, reflejando que se ha producido una acción a través de un dispositivo Iphone o Android, pero no se refleja el número de teléfono *desde el cual se realiza esta acción*". Añade que en este caso, los registros serían los siguientes:

• 06/12/2015 a las 1:15:27 – Desconexión. ***(…)*** 00 - User: 07 Desconexión por salto de alarma de la 1:15:04 ***(...)***. Este log registra una desactivación del sistema de alarma por medio de un mando a distancia a raíz de un salto de alarma.

En cuanto a logs asociados a interacciones con el sistema de alarma a través de la APP, instalada en el móvil del reclamante, éstos serían los siguientes:

Señala los logs iniciados el 06/12/2015 14:06:47 Petición de Estado desde iPhone hasta las 21:06:08 con distintas peticiones desde iPhone. En los cuadros del acceso proporcionados al reclamante, en dicha fecha y hora no se contiene ni se deduce que la petición se correlacione con el reclamante o pueda serlo por alguno de los contactos autorizados. De tal modo que a la vista del cuadro Excel-acceso proporcionado- se desconoce quien es la persona: titular o contacto autorizado que pide y arma el sistema o las imágenes.

14) El panel de control, también llamado consola de control de alarma, suele estar situado en el interior de la vivienda, es el que recibe las señales de los sensores, y donde se activa (arma) o desactiva (desarma), de modo que si no está activada (armada), no recogerá las señales de los sensores. El dispositivo de alarma de la vivienda está conectado 7/365 con la CRA. La reclamada informó que el sistema de conexión y la CRA, se lleva a cabo mediante una tarjeta SIM integrada en el panel de control.

La reclamada manifestó que el panel de control del sistema de la alarma almacena registros. De hecho, puede almacenar hasta ******NÚMERO.3*** eventos, los cuales se van borrando de manera cíclica, en función de los registros que se vayan generando y grabando continuamente. Según se van generando y grabando registros nuevos, se borran me manera cíclica los más antiguos manteniendo un orden temporal de grabación y borrado siempre dentro de los ***NÚMERO.3 registros que puede albergar.

15) La reclamada manifestó en pruebas ante la cuestión del modo en que se generan y almacenan los logs del funcionamiento del sistema de alarma, que el sistema genera y almacena en el panel de control registros derivados de:

-Interacciones del cliente con el sistema de alarma, por ejemplo: conexión, desconexión.

-Verificaciones internas del sistema: ejemplo cobertura ***(...)***, y

-Actuaciones del sistema de alarma en el desempeño de su función, por ejemplo, salto de alarma.

Además, señaló la reclamada que el catálogo de logs que pueden generarse por la interacción del sistema instalado y la CRA es cerrado, no siendo posible la creación de nuevos logs distintos de los que el sistema genera. Algunos de estos logs previamente configurados sí se generarán como consecuencia de la interacción del sistema con una actividad desarrollada por un operario o usuario autorizado de SECURITAS DIRECT, así como por el propio titular del sistema o las personas autorizadas por éste.

La memoria interna del dispositivo se encuentra alojada en la placa base del panel de control. Según la reclamada, dicha memoria interna registra eventos, entre los que se distinguen:

(i) aquéllos que generan un log, copia de los cuales han sido facilitados en el documento Nº 2 de los aportados juntos con el escrito de alegaciones al acuerdo de Inicio. (logs tal como salen del sistema de SD, juntos, los que contienen datos y los que no, por orden cronológico).

(ii) y otros eventos meramente técnicos y relacionados con la interconexión producida para la remisión de los logs a la CRA de SECURITAS DIRECT (e.g. canal por el que se remite el log, conexión exitosa, acuse de recibo, etc.). Dado que únicamente se refieren a la remisión y no a ningún tipo de actuación concreta, estiman que no formarían parte de lo solicitado por el reclamante.

Según la reclamada, en ambos casos, el destino de dichos registros es la CRA*, "si bien la información mencionada en el punto (ii) así como los logs que no reflejan un evento relevante relacionado con el funcionamiento de la alarma no se comunican y permanecen en la memoria interna de la centralita y sólo son accesibles por el personal de SECURITAS DIRECT en caso de que se produzca un evento que exija la realización de un análisis forense.*

En pruebas, la reclamada indicó que desde la CRA, los operadores tienen la capacidad de activar o desactivar la alarma únicamente a petición del cliente, en el marco de una interacción telefónica con éste. Esa petición queda debidamente registrada, por medio de su correspondiente log. El supuesto se dio en los registros proporcionados al reclamante en el día 18/12/2015.

16) La reclamada sostiene que el dispositivo de la alarma del reclamante generó logs (registros de eventos) hasta las 20:09 h del día 27/11/2015, hora y fecha en la que se produjo la intrusión en el domicilio y durante la cual ,dicho sistema de alarma quedó completamente inutilizado. A partir de esa fecha, ese dispositivo no pudo generar más logs.

17) En los registros, hay un salto temporal en logs considerados dato personal que se dieron al reclamante entre el día 27/11/2015 a las 20:17 y el 4/12/2015 a las 11:05.

18) El primer log de reanudación tras 27/11/2015, (catalogado en verde al considerarse que contiene datos personales y entregado al reclamante es el de 4-12-2015, 11:05:04, que la reclamada explica que se produce a consecuencia de comprobaciones técnicas a través de un sistema automático que se denomina GTI (aparece en el propio log) que se encarga de llevar a cabo varias verificaciones para conocer el estado técnico del sistema, procediendo a la apertura de un mantenimiento cuando resulta necesario. En este caso, un operador se encarga de llamar al cliente para hacer una revisión con el cliente en línea y si no es posible, concertar una visita de un técnico para verificar el estado del sistema.

19) Se aprecia que hasta esa reanudación, así como en días anteriores, figuran logs en color rojo, de no dato personal, a partir del 28/11/2015.

20) El 5/12/2015 ,se colocó un nuevo dispositivo de alarma en el domicilio del reclamante, que sustituyó al destruido, siendo baja en el servicio el 23/12/2016.

21) En cuanto a si es posible que los logs se superpongan, la reclamada señaló en pruebas que "*cada línea de log es un registro único con fecha y hora, e incluso puede*

haber varios en el mismo minuto y segundo, al tratarse de "máquinas" pero ello no supone una "superposición", sino la generación de varios logs simultáneos."

22) Con el salto de alarma de 27/11/2015, la reclamada procedió a la pertinente comprobación del mismo mediante el intento de acceso al módulo habla/escucha del sistema. Al no ser posible, y no recibirse desconexión por parte del usuario, se activó el mecanismo de contacto con las personas y los teléfonos establecidos en el documento "*PLAN DE ACCIÓN",* informándose al "*contacto cuatro"* de lo acontecido hasta ese momento. De estos hechos queda reflejo en los logs con datos personales proporcionados al reclamante.

23) La reclamada también dispone de logs que no considera datos personales generados el 27/11/2015 a las 20:09:47, así como todos los del día anterior, 26. El primer log que se genera al reclamante como dato personal es el de *27/11/2015 20:09:47.* A la misma hora, figuran dos logs como no datos personales, en color rojo ,con distintos códigos que los que figuran en el log del reclamante con nota: "*intrusión volumétrico sísmico puerta de garaje* y *nivel de cobertura panel*, descripción *intrusión volumétrico radio*, y el segundo "*señal informativa*". También figuran distintos logs de color rojo del mismo 27 y todos los del 28 hasta el día 4/12/2015, 1104:50. Entre el 28 y el 4/12 , excepto el 29 se generaron según el comentario que figura test de Logs que informan de la pérdida de comunicación con el dispositivo) hasta 4, uno por día.

Manifestó la reclamada que, los logs de 27/11/2015, 20:09:47, se inician mediante la detección de una alerta de alarma volumétrica a las 20:09:47, generándose un código aleatorio (1155) que se genera con cualquier salto de alarma, para que, si se envía a un vigilante, éste pueda desconectarla (en este caso, no se utilizó para enviar a ningún vigilante, ya que se determinó que no era necesario). A partir de ese instante, constan los logs de verificación del sistema para el traspaso de la información a un operador, que realiza desde ese momento las llamadas pertinentes a quienes aparecen como contactos designados en el contrato por el reclamante. Dichos intentos son infructuosos respecto de los tres primeros contactos, al saltar el buzón de voz, pudiendo efectuarse la comunicación con el cuarto de los contactos que, sin embargo, no facilita la palabra que permite establecer la comunicación, concluyendo la tramitación de la alerta el 27/11/2015 a las 20:17:07 horas, ultimo log de dato de carácter personal que figura anotado y se entregó al reclamante.

Manifestó la reclamada que "*todas las actuaciones relacionadas con el salto de alarma y los intentos de contacto han sido consideradas datos personales y facilitadas al reclamante, no teniendo tal consideración los logs exclusivamente relacionados con el modo en que los sistemas de SECURITAS DIRECT gestionan y encauzan las actuaciones a realizar en estos casos o los que se refieren exclusivamente al operador interviniente. La explicación justificativa de la consideración o no de la información como datos personales se contiene en el informe aportado como Documento Nº 1 en las alegaciones al Acuerdo de Inicio."*

La reclamada indicó que los logs generados a partir del momento de producirse el salto de alarma de 27/11/2015, 20:09 h , y una vez descartados los relacionados con los intentos de comunicación con los contactos designados por el Reclamante, se refieren a sucesivos intentos de comunicación entre SECURITAS DIRECT y el sistema instalado en el domicilio del Reclamante, que resultaron infructuosos y siendo interacciones máquina a máquina de carácter técnico.

Asimismo, existen distintos logs relacionados con saltos de alarma posteriormente desactivados el día 5/12/2015 a partir de las 18:56:37, facilitados al reclamante por considerarse que incorporan datos personales relativos al mismo, dado que se trata de acciones encaminadas a distintas pruebas sobre el funcionamiento del sistema instalado en su vivienda, realizándose distintas pruebas de alarma (volumétricas, sísmicas, por coacción o magnéticas). También se produce un salto de alarma el día 6/12/2015 a las 01:15:04 horas, pudiendo comprobarse los logs generados por el sistema, y que concluye con la comunicación con el titular que indica a las 01:17:22 horas que el salto de la alarma puede haber sido generado por la chimenea.

24) A efectos de iniciar el protocolo de actuación, se considera salto de alarma las señales recibidas en la Central Receptora de Alarmas procedentes de la captación de los elementos de detección de intrusión, del botón SOS, del botón antiatraco, y código de coacción. En el contrato existe un protocolo al respecto que distingue si salta, "*sin desconexión del usuario*", caso en el que SD verifica *"mediante el acceso al módulo habla-escucha del sistema y/o llamada al teléfono fijo del inmueble, siempre que se disponga de este último. Si a través de estos medios:*

- Se obtiene contestación: se procederá a identificar a la persona con la palabra clave maestra o de contacto. Si la palabra clave es correcta, se proporcionará al usuario las instrucciones técnicas precisas para que desconecte el sistema.

- Si la palabra clave no es correcta o no se obtiene contestación: SECURITAS DIRECT procederá a dar cumplimiento a los procedimientos de verificación previstos en la normativa de Seguridad Privada vigente así como a utilizar los medios complementarios de verificación tal como proceder a la llamada de comprobación a los CONTACTOS PRINCIPALES y/o OPERATIVOS establecidos, y/o al Vigilante de Seguridad y/o F.C.S. si se tratara de una alarma real confirmada. En todo caso, la decisión de cursar el aviso corresponderá exclusivamente a SECURITAS DIRECT.

En caso de que se diera "*desconexión de usuario*", es el supuesto en que salta la alarma, y en un tiempo inferior a 20 segundos (desde el salto de alarma), se recibe señal de desconexión en la CRA. En este caso, "*se emitirá de modo automático una locución grabada a través del módulo habla escucha del sistema, en la que se informará al cliente de la señal recibida así como de la ejecución de la desconexión por el usuario o persona autorizada y de la cancelación de la incidencia"*
"En el supuesto de que la señal de desconexión se reciba en un tiempo superior al indicado en el párrafo anterior, SECURITAS DIRECT procederá a verificar el salto de alarma mediante el acceso al módulo habla-escucha del sistema y/o llamada al teléfono fijo del inmueble, siempre que se disponga de este último, para realizar las comprobaciones que entienda oportunas según su diligencia como Empresa de Seguridad y que se hallen ajustadas a la normativa de Seguridad Privada aplicable."

La reclamada en pruebas, a la pregunta de Modo/s de verificación de la alarma aplicable/s en este caso, y que logs se generan y señale los que con este descriptivo figuren en el período solicitado por el reclamante, respondió que *pueden clasificarse en:*

(i) aquéllos que se generan como consecuencia de una interacción del titular del contrato o de un autorizado por el mismo con el sistema de alarma;

(ii) los derivados de una interacción humana producida desde la CRA; y

(iii) los que se generan de forma automática, sin intervención humana de ningún tipo.

Considera que *"únicamente los logs enumerados en los puntos (i) y (ii) implican un tratamiento de datos personales, y de éstos sólo el enumerado en el punto (i) supone el tratamiento de datos del reclamante o las personas autorizadas por el mismo, en el Documento nº 1 (informe de* 29/01/2021, aportado por la reclamada en alegaciones*) aportado por la reclamada junto con su escrito de alegaciones, se aclaraba que el derecho de acceso por el interesado a sus propios datos, únicamente afectaba a los contenidos en el citado punto (i) y no a los relacionados en los puntos (ii) y (iii), que no incorporan datos personales del Reclamante. "*

En concreto, y en lo que respecta a todos los logs aportados a la Agencia*,* encajarían en lo descrito en esta respuesta los siguientes logs que representan verificaciones de alarma:

• *Logs comprendidos entre el 27/11/2015 desde las 20:09:47, hasta las 20:17:07, momento en el que se contacta con un plan de acción.* Se trata de 21 logs en cuya descripción todos se relacionan con actuación de la CRA, con añadidos como llamada, comunicando, salta buzón de voz, se deja mensaje en buzón de voz, operador consigue hablar con contacto 4, palabra incorrecta, u otras menciones a contacto 1, 2, 3, llamada a H/E, audio H/E no se envía a FCS y otras claves en los distintos cuadros, *que como ya se ha mencionado no resultan comprensibles sin una clave y explicación comprensible y breve de su significado.*

• Logs comprendidos entre el 06/12/2015 desde las 01:15:04 hasta las 01:17:40. En la que figuran varios logs, "*indica que puede ser la chimenea",* y en el mismo sentido con claves en los distintos cuadros, que no *resultan comprensibles sin una clave y explicación comprensible y breve de su significado.*

La reclamada informó en pruebas, que, en el caso del periodo de datos solicitado por el reclamante, no se produjo ningún registro de aviso de alarma confirmado que se comunicara a la Policía.

25*)* Manifiesta la reclamada que *"la memoria interna de la centralita (Panel de Control) inicialmente instalada y destruida en los hechos acaecidos el día 27/11/2015, no incorpora, dentro del período temporal respecto del que se ejerció el derecho de acceso, ningún log referido al* ***(...)*** *o des(...) del sistema de alarma, siendo esta, y no otra, la razón por la que la información facilitada al Reclamante no incorpora ningún registro de esta naturaleza en relación con el dispositivo inutilizado.*

Respecto de los logs que constasen en la memoria interna del instalado en fecha 5/12/2015, la reclamada indica que no pudo en ningún momento acceder a la información, por lo que no le resultaba posible facilitarla al interesado. En cuanto al motivo, señala que *la CRA, únicamente puede acceder a los logs que son transmitidos a la misma desde la memoria interna del dispositivo, pero no a los de carácter meramente técnico que se generasen en dicha memoria interna, dado que SECURITAS DIRECT únicamente puede acceder al contenido de dicho dispositivo en caso de que se hubiera producido un*

incidente que exija su análisis forense. En este caso, dado que dicho incidente no tuvo lugar, el dispositivo permaneció en la vivienda del Reclamante hasta la finalización del Contrato, sin que en ningún momento SECURITAS DIRECT pudiera acceder a dicha memoria interna ni fuera necesaria la realización de ningún análisis forense de su contenido, al no haberse producido un incidente que lo exigiera. Como puede comprobarse, en dichas respuestas sí se contiene información referida al período mencionado en la cuestión planteada.

26) La reclamada manifestó en pruebas que tras el acceso a los registros contenidos en la memoria de la alarma se ha comprobado que ésta se encontraba conectada desde el día 22/11/2015 a las 11: 56 y que no presentaba anomalía alguna.

27) Sobre el acceso a los datos personales contenidos en la memoria interna del panel de control, tras la colocación del nuevo el 5/12/2015, no figuran en el acceso proporcionado de 14/12/2021 ni en el precedente de 23/02/2021.

28) En el documento 2 de alegaciones, -total logs- cuadro Excel de todos los logs, diferenciados en color rojo-considerados como no datos personales por la reclamada-, y en color verde, considerados como datos personales por la reclamada, figura sí:

Con distintas claves de la "***(...)*** del evento" distinguidos en rojo los considerados no datos personales, ejemplo, hay dos en rojo, de 27/11/2016 20:09:47, y otro de misma fecha y hora, en verde. La reclamada manifestó que *los logs se refieren a eventos distintos: el primero implica la detección de un salto de alarma detectado por un sensor volumétrico; el segundo implica la generación de un código de desactivación en caso de que sea necesario acudir a la vivienda una vez realizadas las verificaciones correspondientes, que constan igualmente en la tabla de logs; y el tercero se refiere a la cobertura **(...)***." Añade que también pueden coincidir fechas y hora en los logs que tienen dato personal, aportando el ejemplo del 5/12/2015 18:38:10 en que figuran cinco distintos, relacionados con mantenimientos presenciales de cambio de alarma.

29) La reclamada informó en pruebas que las revisiones periódicas del sistema de funcionamiento de alarmas previstas en el artículo 43 del RD 2364/1994 por el que se aprueba el Reglamento de Seguridad Privada y el artículo 5 de la Orden INT/316/2011, son efectuadas desde su CRA en modo remoto, normalmente cada tres meses. Además, realiza test diarios de comunicación y correcta transmisión del sistema de alarma con la CRA de forma automática. Da algunos ejemplos de 5/12/2015 que se hallan incluidos en los logs proporcionados al reclamante y de 6/12/2015, 18:45:42, que no se considera log de dato personal del reclamante, figurando en color rojo.

De las revisiones presenciales queda constancia en el log del sistema de gestión de las alarmas de la CRA, ya que el técnico debe ir comprobando una serie de parámetros del sistema y realizando las distintas comprobaciones de funcionamiento.

Si se realizasen revisiones remotas, estas quedarían reflejadas en la memoria de eventos del sistema de alarma.

Por otro lado, las tareas de mantenimiento son correctivas, destinadas a solventar incidencias puntuales que no permitan el correcto funcionamiento del sistema de la

alarma, y tienen como objeto la subsanación de dichas incidencias, pudiendo realizarse según la naturaleza o la necesidad, de manera presencial o remota.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD) reconoce a cada Autoridad de Control, y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la LOPDGDD, es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: "*Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos*."

II

El artículo 4 del RGPD, bajo la rúbrica "*Definiciones*", dispone lo siguiente:

1) *"datos personales: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;"*

"7*) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros"*

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que SECURITAS DIRECT realiza, entre otros tratamientos, la recogida, conservación, consulta, utilización, acceso de los datos personales de los clientes-usuarios, tales como: nombre, apellidos, correos electrónicos, credenciales…, etc.

SECURITAS DIRECT realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y medios de tal actividad, en virtud del artículo 4.7 del RGPD.

El presente procedimiento sancionador se inicia porque la parte reclamante considera que no se ha atendido su derecho de acceso derivado de la TD/00167/2021, alegando que no se han suministrado todos sus datos personales (logs) y que los que se han

remitido le resultan ininteligibles, en los términos fijados en los antecedentes de esta propuesta de resolución.

Así, en este procedimiento sancionador se trata de dilucidar, a través de la instrucción del mismo y atendiendo a las alegaciones y documentación aportada por la parte reclamada, si se ha atendido el derecho de acceso completamente, y de qué forma se ha llevado a cabo, en los términos fijados en el RGPD, y, por tanto, si se ha producido una infracción de la normativa de protección de datos.

III

Tal y como destaca la Exposición de Motivos de la Ley 5/2014, de 4/04, de Seguridad Privada, la seguridad es uno de los pilares primordiales de la sociedad, se encuentra en la base de la libertad y la igualdad y contribuye al desarrollo pleno de los individuos. Dicha ley considera la seguridad privada como una actividad con entidad propia, pero a la vez como parte integrante de la seguridad pública.

La actividad de explotación de un sistema de seguridad a través de una CRA es aquel servicio o actividad exclusivo, complementario, de carácter mercantil y de prevención del delito, subordinado a la seguridad pública, desarrollado y prestado por Empresas de Seguridad homologadas por el Ministerio de Interior, sometido a la normativa de seguridad Privada, que utilizan medios, medidas técnicas, elementos de protección, reglamentadas y homologadas, a través de sistemas de seguridad electrónicos contra riesgos de robo o intrusión con las características funcionales descritas en las Normas UNE para su comercialización, venta, instalación en un ámbito privado demandante de seguridad privada. Ello se materializa a través de la firma de un contrato de arrendamiento de servicios de mantenimiento y conexión de dicho sistema a un Centro de Control integrado en la Central de Alarmas también autorizada, para la recepción, tratamiento, verificación de señales de alarma emitidas por dichos sistemas de seguridad instalados, a través de los procedimientos técnicos y humanos previstos en la Orden 316/2011 de 1/02 sobre funcionamiento de los sistemas de alarma en el ámbito de la seguridad privada, de tal manera que pueda determinarse o no su realidad, y su comunicación en caso de confirmarse como real a la Policía.

El objeto de este contrato es la puesta a disposición o entrega material por la Empresa de Seguridad de un Sistema de Seguridad y su instalación con una finalidad de servicio de Central Receptora de Alarmas, y posteriormente el mantenimiento del sistema en adecuado funcionamiento para la prestación de los servicios contratados en el domicilio (vivienda) del usuario contratante.

Al hallarse la instalación del dispositivo y elementos de seguridad vinculados al mantenimiento del mismo como un sistema o producto que se vincula a un servicio de explotación a través de una central receptora de alarmas, se trata de un contrato de servicio ligado al servicio de mantenimiento del sistema instalado, dedicado exclusivamente a recepción de señales de alarma emitidas por el sistema de seguridad instalado y al tratamiento de dicha señales para la determinación de su origen real o falso mediante el cumplimiento de procedimientos reglamentariamente establecidos.

La citada orden de funcionamiento de los sistemas de alarma establece que la CRA efectué verificaciones a través de reglas contenidas en procedimientos técnicos descritos y complementariamente humanos. Tras completarse dichos requisitos formales y

materiales exigidos, puede ser comunicada dicha señal de alarma confirmada por la CRA como real a la Policía.

La sentencia de la Audiencia Provincial de Madrid, sección 11, 98/2014, de 11/03/2014, analiza la naturaleza del contrato de seguridad en su modalidad de prestación de servicios centrales de alarmas por parte de una empresa dedicada a ello, indicando en su fundamento de derecho segundo:

"*Como ya pusiera de manifiesto esta misma Sala en Sentencia de 30 de junio de 2011 , que se remite a la de 29 de Abril del 2010 , que a su vez lo hace a la dictada el 6 de Junio de 2.007 , citando la Sentencia de la A.P. de Barcelona de 30 diciembre 2004 , "...el contrato suscrito por las partes es un contrato de arrendamiento de servicios y no de obra, y ello en base a criterios doctrinales aceptados en jurisprudencia del Tribunal Supremo (S. 4.2.1950, entre otras), que se apoyan para establecer la diferencia, en el objeto inmediato de la obligación del arrendamiento, de manera, que si éste se obliga a la prestación de un servicio o de trabajo de una actividad en sí misma, no al resultado que aquella prestación produce, que es el caso que nos ocupa, el arrendamiento es de servicio. Y en cambio, si se obliga a la prestación de un resultado, sin considerar el trabajo que lo crea, el arrendamiento es de obra. Pues bien, la obligación de la demandada, hoy apelada, es una obligación de actividad, y no de resultados.*

Resulta evidente que la finalidad del contrato era la de dotar al local comercial de unas medidas de seguridad encaminadas a prevenir la comisión de hechos delictivos y la obligación fundamental de la demandada era prestar los servicios necesarios para que los mecanismos de seguridad instalados funcionasen correctamente.

En virtud del contrato de arrendamiento de servicios de seguridad concertado, la entidad demandada, se comprometía, no a evitar la posible comisión de robos en la finca, ni a asegurar en todo caso la restitución (en especie o en equivalente dinerario) de lo que terceras personas pudieran sustraer, sino exclusivamente a responder del normal funcionamiento de un sistema de seguridad, consistente en una alarma de robo con conexión telefónica con la central de alarmas, efectuándose la detección mediante sensores situados en diversos puntos repartidos por las oficinas, de forma que el sistema debía transmitir -vía telefónica- una señal a la Central de Alarmas, la cual a su vez debía dar noticia del posible delito a las fuerzas de seguridad, para que impidieran su consumación, tenía, pues, una finalidad esencialmente preventiva y protectora, por tanto, como se ha expuesto, el objeto está en la actividad, y en estos términos, son los únicos posibles para exigir una responsabilidad".

El envío y recepción de señales por el dispositivo y la CRA se produce en un domicilio particular, entendiendo como tal, un espacio apto para desarrollar en él la vida privada, sobre el que va a incidir su carácter de inviolable que prevé la CE en su artículo 18.2 vulneración que se puede producir con independencia de que, en el momento de la entrada, se encuentre el titular del derecho dentro o fuera de su domicilio. Además, existe una estrecha relación entre la inviolabilidad de domicilio y el derecho a la intimidad consagrado en art. 18.1, como muy bien señaló la STC 22/1984,*"el domicilio inviolable es un espacio en el cual el individuo vive sin estar sujeto necesariamente a los usos y convenciones sociales y ejerce su libertad más íntima"*.

La inviolabilidad de domicilio garantiza pues esa esfera íntima de privacidad personal y familiar (dentro del espacio limitado que la propia persona escoge), frente a toda clase de

invasiones o agresiones de otras personas o de la autoridad pública no consentidas por el titular del derecho. La protección constitucional del domicilio tiene pues un carácter instrumental.

IV

La reclamada aportó algunos detalles sobre el funcionamiento y componentes de un sistema de alarma.

Básicamente en el domicilio se instala un panel de control, que se suele acompañar de un kit de alarma (elementos adicionales como detectores de movimiento/cámara y que pueden permitir la visualización a través de un dispositivo móvil conectado mediante una aplicación instalada, junto con otros medios como mando a distancia, sirenas, lector de llaves, llaves inteligentes que permiten desconectar la alarma simplemente acercando la llave al lector, detectores magnéticos etc.)

El panel de control que se suele instalar en el interior de la vivienda, en un sitio que no esté muy a la vista, está conectado con la CRA, donde llegan las notificaciones y avisos como los saltos de alarma.

A su vez, la CRA debe efectuar operaciones al comprobar y analizar las anomalías que pueden acontecer, control de cortes de electricidad, salto de alarma por diferentes motivos por poner unos ejemplos. Al mismo tiempo, en modo remoto, la CRA puede activar, configurar y verifica las funciones del sistema de alarma, realizar diagnósticos de conexión, y controlar los detectores de alarma.

El panel de control permite activar el sistema, armar, desarmar la alarma, conecta con los elementos adicionales como los sensores y recibe las señales de los detectores periféricos instalados. Por ejemplo:

-si se activa un contacto de puerta o un sensor de movimiento, el panel dará la señal, si no se desactiva la alarma con un código de usuario válido, el sistema asume que hay una intrusión y dará señal audible o lumínica, a la vez de comunicarse con la CRA.

-si se activa el botón de pánico, SOS o antiatraco, directamente comunica con la CRA Además permite la comunicación bidireccional con la CRA mediante micrófono y altavoz integrado (módulo de habla escucha).

La CRA se encarga de analizar e interpretar los saltos de alarma, es la sede de control de los sistemas de alarma.

Cuando se atiende el salto de alarma, la CRA tiene que analizar la información minuciosamente para determinar de qué tipo de emergencia se trata o si se trata de una falsa alarma.

En cualquier caso, la CRA se pondrá en contacto con el propietario o contactos designados para informarle de lo ocurrido.

La comunicación entre el panel de control y la CRA puede darse por diversos medios y método. De manera general, la comunicación entre los sistemas de alarma y la CRA, se dará a través de dos vías de comunicación diferentes para permitir que la comunicación sea continua, aunque falle o se sabotee una de las vías.

Desde la CRA se permite la comunicación bidireccional con el sistema de alarma, pudiendo acceder al sistema a través del software para el control remoto del sistema, ello también independientemente que el sistema haya perdido la alimentación de corriente de la instalación.

Los sistemas en general, registran la actividad de los usuarios autorizados (cliente y personas de contacto por el designadas), así como operadores de la reclamada, incluyendo las operaciones máquina a máquina generando rastros de acceso: -log in-, origen, tiempo de actividad, acciones, y conexiones.

La información de estos registros es esencial para elaborar informes de gestión y para monitorización. Entre los eventos que los distintos sistemas registran, están por ejemplo el inicio, fin de sesión, el acceso, modificación de ficheros y directorios, cambio en las configuraciones principales, lanzamientos de programas, etcétera.

Los registros de actividad de los distintos sistemas y equipos son los datos a partir de los cuales es posible no sólo detectar fallos de rendimiento o mal funcionamiento, sino también detectar errores e intrusiones. Con ellos, se alimentan sistemas de monitorización que convenientemente configurados pueden generar alertas en tiempo real. Por otra parte, facilitan el análisis forense para el diagnóstico de las causas que originan los incidentes. Por último, son necesarios para verificar el cumplimiento de ciertos requisitos legales o contractuales durante las auditorías.

V

Planteadas así las cosas, la parte reclamada considera que los logs "*técnicos*" o "*internos*", no son datos de carácter personal de la parte reclamante, no teniendo, por tanto, obligación de suministrar dichos datos como parte del derecho de acceso ejercitado por esta última.

Se va a analizar la cuestión excepcionada por la reclamada en cuanto a los datos de carácter personal de los denominados por la reclamada: logs "*técnicos*" o "*internos*", que se caracterizan según defiende, por no referirse a ninguna persona, en concreto ni siquiera al reclamante y por no contener información que verse sobre ninguna persona, ni siquiera al reclamante. Añadiendo además que los considera como confidenciales, dignos de la protección del secreto empresarial.

Se ha de partir del artículo 1 del RGPD en el que se establece como objeto

"1. El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos.

2. El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales."

El ejercicio del derecho de acceso se realiza tanto en el marco de la legislación en materia de protección de datos, de conformidad con los objetivos de la legislación en materia de protección de datos, como, más concretamente, en el marco de los "*derechos y libertades fundamentales de las personas físicas*" y, en particular, su derecho a "*la protección de datos personales*", tal como se establece en el artículo 1, apartado 2, del

RGPD.

Es fundamental comprender que se trata de determinar la manera de aplicar las disposiciones a determinadas situaciones en las que los derechos individuales están en juego por el tratamiento de sus datos personales.

El artículo 8.1 de la Carta de Derechos Fundamentales de la Unión Europea, señala:*"1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.*

El considerando (26) indica:" *Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por lo tanto los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación."*

El Dictamen 4/2007 del Grupo de Trabajo del artículo 29 sobre el concepto de datos personales, indica que es: *toda información sobre una persona física identificada o identificable*.

La definición refleja la intención del legislador de mantener un concepto amplio de "*datos personales*", lo que exige una interpretación amplia que abarque toda información que pueda vincularse con una persona, o referirse a una persona identificable, con el objetivo de proteger las libertades y derechos fundamentales de las personas físicas, entre otros, particularmente su derecho a la intimidad en lo que respecta al tratamiento de los datos personales.

Esta amplitud en cuanto a la extensión del término "*dato de carácter personal*", como la diversidad de campos en los que se puede manifestar, se confirma en diversas sentencias del TJUE, a título de ejemplo en la de 20/12/2017, asunto C-434/16, párrafos 33 a 35:

"33. Como ya ha señalado el Tribunal de Justicia, el ámbito de aplicación de la Directiva 95/46 es muy amplio, y los datos de carácter personal a los que se refiere son heterogéneos (sentencia de 7 de mayo de 2009, Rijkeboer, C-553/07, EU:C:2009:293, apartado 59 y jurisprudencia citada).

34 En efecto, el empleo de la expresión «toda información» en la definición del concepto de «datos personales», que figura en el artículo 2, letra a), de la Directiva 95/46, evidencia el objetivo del legislador de la Unión de atribuir a este concepto un significado muy amplio, que no se ciñe a los datos confidenciales o relacionados con la intimidad, sino que puede abarcar todo género de información, tanto objetiva como subjetiva, en forma de opiniones o apreciaciones, siempre que sean «sobre» la persona en cuestión.

35 Este último requisito se cumple cuando, debido a su contenido, finalidad o efectos, la información está relacionada con una persona concreta..." (El subrayado es nuestro).

La doctrina elaborada por el TJUE respecto a la amplitud con la que debe interpretarse el concepto de dato personal se ha ido adaptando, atendiendo a los diversos avances tecnológicos. De este modo, en la sentencia de 24/11/2011, asunto C-70/10, en su párrafo 51 consideró que las direcciones IP son datos protegidos de carácter personal, ya que permiten identificar concretamente a tales usuarios. Este criterio se mantiene y se amplía a los supuestos en los que incluso se trata de las direcciones IP dinámicas, aquellas asignadas de manera temporal por los proveedores de acceso a la red a sus clientes, considerando que seguían constituyendo un dato personal cuando el encargado de almacenarlas, en este caso el titular de un sitio web, no disponía de los datos adicionales necesarios para la identificación del usuario concreto, sino que estaban en posesión de un tercero, recogiendo este criterio, de nuevo favorable a una interpretación amplia del concepto de dato personal, en la STJUE de 19/10/ 2016, en el asunto C-582/14, Patrick Breyer y Bundesrepublik Deutschland, al aseverarse que la IP es un dato de carácter personal para el proveedor de servicios: "*el artículo 2, letra a), de la Directiva 95/46 debe interpretarse en el sentido de que una dirección IP dinámica registrada por un proveedor de servicios de medios en línea con ocasión de la consulta por una persona de un sitio de Internet que ese proveedor hace accesible al público constituye respecto a dicho proveedor un dato personal, en el sentido de la citada disposición, cuando éste disponga de medios legales que le permitan identificar a la persona interesada gracias a la información adicional de que dispone el proveedor de acceso a Internet de dicha persona*" (párrafo 49).

Más recientemente, en su sentencia de 17/06/2021 (asunto C-597/19), analizando un supuesto de carga, desde el equipo terminal de un usuario de una red entre pares (peer-to-peer) y hacia los equipos de otros usuarios de dicha red, de partes, previamente descargadas por el usuario antes citado, de un archivo multimedia que contiene una obra protegida, aunque esas partes solo sean utilizables por sí solas a partir de un determinado volumen de descarga y en las que sea el propio software el que automáticamente dé lugar a la carga mencionada, en su párrafo 97 recuerda que "*Con carácter preliminar, es preciso puntualizar que en el asunto principal se contemplan dos tratamientos de datos personales diferentes; a saber, uno que ya realizó inicialmente Media Protector por cuenta de Mircom, en el contexto de las redes entre pares (peer-to-peer), consistente en registrar las direcciones IP de usuarios cuyas conexiones de Internet supuestamente se utilizaron, en un determinado momento, para cargar obras protegidas en las referidas redes, y otro que, según Mircom, debe llevar a cabo Telenet en una fase posterior, consistente, por una parte, en identificar a esos usuarios cotejando las referidas direcciones IP con las que, en ese mismo momento, Telenet había atribuido a los mencionados usuarios para efectuar dicha carga y, por otra parte, en comunicar a Mircom los nombres y direcciones de esos mismos usuarios*".

A la luz del amplio alcance de la definición de datos personales, una evaluación restrictiva de dicha definición por parte del responsable del tratamiento conduciría a una determinación errónea de lo que son datos personales y, en última instancia, a una violación de los contenidos por el RGPD a los interesados entre los que se encuentra el derecho de acceso.

La AEPD, dentro de su función de supervisión de la aplicación de la legislación sobre protección de datos, debe interpretar las excepciones a la aplicación del concepto de datos personales como la que defiende la reclamada, ya que si se validara su teoría sobre una parte los logs del sistema de la alarma, tal vez quedarían fuera del ámbito de aplicación del RGPD.

La citada amplitud en la definición de dato personal, se define por:

-"*toda información*", incluyendo todos aquellos datos que proporcionan información, cualquiera que sea la clase de esta que ha de tener una interpretación amplia, abarcando información subjetiva u objetiva, incluyendo evaluaciones, diagnósticos u opiniones.

-"*sobre*" una persona física, relacionando pues cualquier tipo de información sobre una persona física. Aquí es imprescindible conectar la finalidad de la información con el "sobre" quien se trata la misma y los efectos que puede tener para esa persona.

-"identificada" o *"identificable".* Alude a toda persona cuya identidad pueda determinarse, directa o indirectamente, en el sentido de que, para calificar una información de dato personal, no es necesario que dicha información permita por si sola, identificar al interesado. En este caso, la información que le hace identificable son los logs, que tanto los llamados técnicos por la reclamada, como los que considera datos de carácter personal del reclamante, figuran en relación a un dispositivo, estructurado en un único y conjunto bloque compacto y unitario cronológicamente ordenados para reflejar los eventos del dispositivo referido a dicho reclamante que es identificable.

El Dictamen 4/2007 añade: "*En los casos en que, a primera vista, los identificadores disponibles no permiten singularizar a una persona determinada, ésta aún puede ser «identificable», porque esa información combinada con otros datos (tanto si el responsable de su tratamiento tiene conocimiento de ellos como si no) permitirá distinguir a esa persona de otras".* En este caso, no todo el mundo le puede identificar, pero el personal de Securitas sí, y con que haya alguien que lo pueda hacer sería suficiente,

-independientemente del contenido o carácter de procedencia de la información.

-Tal como ya ha reproducido la reclamada en su informe de 29/01/2021, aportado por la reclamada en alegaciones, respecto a la información "*sobre*" una persona, el Dictamen 4/2007, ejemplifica su significado con: "*los datos incluidos en el fichero personal de una persona guardado en el departamento de personal de su empresa, que están claramente relacionados con su situación como empleado de dicha empresa. Aunque no siempre resulte tan evidente establecer que la información versa «sobre» una persona concreta. En algunas ocasiones, la información que proporcionan los datos se refiere no*

tanto a personas como a objetos. Esos objetos suelen pertenecer a alguien, o pueden estar bajo la influencia de una persona o sus autorizados, o ejercer una influencia sobre ella o pueden tener una cierta proximidad física o geográfica con personas o con otros objetos. En esos casos, sólo indirectamente puede considerarse que la información se refiere a esas personas u objetos. Un análisis similar puede aplicarse cuando los datos se refieren en primera instancia a procesos o hechos, como por ejemplo el funcionamiento de una máquina cuando es necesaria la intervención humana. Bajo determinadas circunstancias, esta información también puede considerarse información «sobre» una persona."

- "*Estamos ante una tercera categoría de «sobre» cuando existe un elemento de «resultado». A pesar de la ausencia de un elemento de «contenido» o de «finalidad» cabe considerar que los datos versan «sobre» una persona determinada porque, teniendo en cuenta todas las circunstancias que rodean el caso concreto, es probable que su uso repercuta en los derechos y los intereses de determinada persona. Basta con que la persona pueda ser tratada de forma diferente por otras personas como consecuencia del tratamiento de tales datos."*

Cabe destacar que el alcance del concepto de datos personales y, por tanto, la diferenciación entre datos personales y otros datos, formaría parte integrante de la evaluación realizada por el responsable del tratamiento para determinar el alcance de los datos a los que el interesado tiene derecho a obtener acceso, elementos que se tendrían que incluir en la configuración de la "*privacidad desde el diseño*". En este caso, la reclamada señala que no fue hasta 2020, cuando comenzó a analizar el tratamiento de los logs, de los dispositivos de alarma conectados a la CRA, sirviendo el informe de 29/01/2021 también como instrumento de gestión, de las solicitudes de ejercicio de derechos.

En este caso, se trata de la instalación de una alarma, un dispositivo que controla permanentemente las veinticuatro horas de todos los días del año la seguridad de la vivienda en un domicilio privado, que se instrumenta mediante un contrato de seguridad y que tiene un dispositivo instalado en el domicilio del reclamante conectado con elementos adicionales de verificación, y que, para su correcto funcionamiento, además, precisa mantenimiento y seguimiento, debiendo estar conectada. De la configuración del sistema se correlaciona que, de su uso, interacciones y saltos de alarma se generan logs que se corresponden inequívocamente con datos personales de personas identificadas, identificables e información que versa sobre unos y otros, los identificados y los que pueden resultar identificables.

Centrándonos en la negativa de la reclamada en clasificar como logs que son datos de carácter personal, a los logs llamados técnicos, sea, porque no recogen información sobre un interesado, ni pretende conocer información, y no se ven afectados sus derechos y libertades, se ha de recordar que estos logs que descarta del ámbito de aplicación del RGPD la parte reclamada los clasifica en categorías, que consistirían resumidamente, en:

-señales técnicas de comunicación entre dispositivos con el objeto de verificar el correcto funcionamiento o registros de algún fallo.

-recoger información por medio de señales informativas,

-registros internos ante un evento concreto.

Se observa en el informe de 29/01/2021, aportado por la reclamada en alegaciones**,** en la tabla I, que constan como descripciones de este tipo de logs técnicos, y que se encontrarían pues en alguna de las tres categorías explicadas anteriormente, supuestos como: "*información sobre saltos de alarma*", "*salto de alarma en los sensores*", o "*períodos en los que se produce una perdida de conexión entre servidores de SD y el dispositivo instalado en el domicilio del interesado*", la "*cancelación de la incidencia*", "*señal relevante que se transmite a un operador para iniciar el proceso de gestión*", "*emisión de señales técnicas periódicas para confirmar que efectivamente se encuentra conexión y disposición de realizar la actividad*". Todas, según la reclamada responden a protocolos internos de comunicación-verificación, sin explicar cómo considera que estos logs tanto por su contenido, como por sus efectos, no estima que pueden afectan a los derechos e intereses del interesado o cómo considera que no son referidos a él, si, además, al extraerlos del sistema aparecen agrupados y relacionados con la persona del reclamante y su vivienda para utilizarlos con fines de control de seguridad de eventos y correcto funcionamiento del sistema, y que constituiría información que le concierne.

La consideración de datos personales que le "*conciernen*" no debe ser interpretada de manera demasiado restrictiva. Así lo interpretan las Directrices 1/2022, sobre los derechos de los interesados, derecho de acceso, versión 1.0, adoptada el 18/01/2022, por el Comité Europeo de Protección de Datos y que figura en su web, si bien en consulta pública desde 28/01 a 11/03/2022. En su numeral 103 ,indica que " *la clasificación de los datos como datos personales relativos al interesado no depende del hecho de que dichos datos personales se refieran también a otra persona*. Por lo tanto, es posible que los datos personales se refieran a más de una persona al mismo tiempo y en su numeral 104, que "*Las palabras «datos personales que le conciernan» no deben ser interpretadas de manera «demasiadamente restrictiva» por los responsables del tratamiento, como ya declaró el Grupo de Trabajo del artículo 29 en relación con el derecho a la portabilidad de los datos. Transpuesta al derecho de acceso, el CEPD considera, por ejemplo, que las grabaciones de conversaciones telefónicas (y su transcripción) entre el interesado estar comprendidas en el derecho de acceso, siempre que estos últimos sean datos personales".*

La citada Directriz 4/2007, establece como ya se ha mencionado, que: "*en algunas ocasiones, la información que proporcionan los datos se refiere no tanto a personas como a objetos. Esos objetos suelen pertenecer a alguien o estar bajo la influencia de una persona o ejercer una influencia sobre ella*", y que en esos casos, existe la posibilidad de que la información se refiera a esas personas, si bien de modo indirecto.

Pues bien, en el supuesto que estamos examinando, todos los logs, incluyendo aquellos generados y almacenados en los que no interviene el titular-usuarios, sea operado por empleados de SD en procesos en que no interactúe el titular, sea en operaciones técnicas de carácter interno que revelan información sobre la eficacia y funcionamiento, al tratarse de la alarma instalada en su vivienda, ligada al contrato de prestación de servicios suscrito, establecen una conexión entre el objeto (la alarma) y el afectado,

puesto que la alarma está identificada con un identificador único (una numeración específica para cada dispositivo de alarma) para ese servicio que liga indefectiblemente al interesado con el dispositivo y todo lo que se genera y registra en relación con el mismo. Si tomáramos aisladamente cualquiera de los logs remitidos, estos identificarían a esa persona.

Conforme a la SAN 3091/2019, de 23 de julio de 2019, "*De un lado, se trata de una persona física, y por tanto plenamente identificable, que firma un contrato de instalación y mantenimiento de una alarma para la protección de su vivienda con la empresa de seguridad actora. Firma del contrato del que necesariamente derivan una serie de derechos respecto de la custodia y seguridad de dicha vivienda. De otra parte, y esto resulta importante remarcarlo, el derecho de acceso se ejercita respecto de registros y señales captadas y enviadas por el equipo de alarma instalado en un domicilio privado, ejerciéndose precisamente por parte de quien es titular de dicho domicilio".*

Así, en este caso, existiendo este vínculo entre la alarma y el interesado, a través del identificador único que liga la alarma al contrato y al interesado, sistema de alarma que puesto en funcionamiento o programado, genera información sobre dicha persona, por lo que todos los logs discutidos tienen la consideración de datos de carácter personal.

Aparte de que la información puede versar sobre el reclamante de forma directa, por quedar identificado o poder ser identificable como lo es en las interacciones activas o pasivas, también resulta identificado de forma indirecta por estar la información de los logs, todos, también los técnicos, asociada al objeto o dispositivo, que apuntaría a que la información va a versar sobre el reclamante por estar afectado en su derecho a la seguridad de su propia vivienda y en su propia vivienda, incidiéndole esos logs.

Tanto los logs técnicos llamados así por la reclamada, como el resto, permanecen almacenados y custodiados por la reclamada, documentan y contienen información directa o indirecta sobre el funcionamiento seguro de su sistema contratado, es su objeto, por lo que se refieren al reclamante o le concierne, cuanto menos. Su interpretación no sería completa si se considera separar esta información que la reclamada denomina "*logs técnicos*" que considera no deben permanecer sino almacenados en su poder, sin que hayan de ser usados como instrumento aportado al reclamado para su conocimiento.

Además, todos los logs como registros de acontecimientos, tanto los denominados técnicos por la parte reclamada como los que no lo son, están incluidos en un mismo formato "en bruto" o "en línea", porque aparecen interrelacionados y condicionados, de forma cronológica, con la dificultad de su comprensión sino es de forma completa, y aconsejándose su protección en cuanto a integridad en su seguridad de forma conjunta. No se debe olvidar que una de las funciones de los logs puede ser evitar las modificaciones o su seguimiento para conocer los acontecimientos. Por otro lado, por ejemplo, un acceso debido a una brecha de seguridad obtendría plena información al aparecer ordenados en función de una finalidad única. Por otro lado, que el software utilizado o sus opciones configure a los logs como "técnicos" no puede servir para extender la exclusión total y automática de todo el log, sino exclusiva y excepcionalmente, de los datos que en base las cualidades descriptivas o claves que ostenten, incidan sustancialmente en el secreto comercial.

Piénsese a título de ejemplo en los logs técnicos recopilados el día de la intrusión y los

días posteriores, que relacionan operaciones internas por las que la reclamada puede deducir lo sucedido, y las consecuencias extraídas de la conexión de los días posteriores, días de falta de conexión, todos ellos afectan al derecho del reclamante porque se relacionan con el derecho a la seguridad de sus bienes y propiedad que el intenta proteger mediante el funcionamiento permanente del dispositivo y la garantía mediante la suscripción de un contrato con obligaciones y derechos para ambas partes. De este modo, solo la reclamada podría entender lo acontecido sobre el sistema contratado por el reclamante, cuando los logs técnicos, que se encuentran ligados a la persona del reclamante, también se consideran que afectan de modo directo o no a los derechos del reclamante. Además, se ha de añadir que ante los mismos eventos, acontecidos en los mismos momentos, como por ejemplo, los saltos de alarma, o los cortes de corriente, se generan ese otro tipo de logs que la reclamada considera han de tener un tratamiento diferenciado por ser técnicos.

En resumen, el tratamiento de los datos de los logs tiene como finalidad la ejecución del contrato de seguridad, resultando que uno de los objetos del mismo es el registro de logs, que todos están relacionados con la seguridad de la vivienda. La relación entre el sistema, las señales y el titular del sistema de la alarma dada la finalidad del tratamiento de los logs y el objeto sobre el que recae es evidente, pues los logs técnicos que identifican al reclamante también conciernen en su derecho que ostenta como titular y responsable del uso correcto del sistema contratado, frente al que se despliega dicho registro de eventos, fundamentales medios para el derecho afectado del reclamante.

Esos datos de registro de logs, que en este caso la reclamada niega sean de carácter personal, definiéndolos como técnicos, agrupados por responder a protocolos internos de comunicación-verificación, registro de señales o de procedimientos internos, pueden emplearse en realidad por ejemplo también con una finalidad forense en un caso de responsabilidad por el funcionamiento del sistema del que el titular es el reclamante.

Indudablemente se identifica el sistema con todos sus registros con el reclamante, repercutiendo en sus derechos e intereses. No se puede deducir que esos datos no sean información sobre una persona identificada o identificable y además parte de sus derechos afectados, como por ejemplo por el robo sufrido, se relacionan con los logs, incluyendo los que la reclamada considera técnicos y que en realidad identifican al reclamante y le afectan directamente en sus derechos.

En conclusión:

1. El RGPD determina qué es un dato de carácter personal en su artículo 4: "*datos personales: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;"*

2. La parte reclamante ha suscrito un contrato de seguridad con la parte reclamada. Para ello se instala en el domicilio de la parte reclamante un dispositivo de alarma.

3. El dispositivo de alarma ubicado en la vivienda del reclamante está identificado con un

identificador único y permanente (una numeración específica para cada dispositivo de alarma) para ese concreto contrato de prestación de servicios.

4. A través del sistema de alarma se generan logs ligados al dispositivo de alarma instalado en el domicilio de la parte reclamante, unidos a su vez al contrato suscrito por este último con Securitas Direct. La SAN 3091/2019, de 23 de julio de 2019, define a los logs como "*registros y señales captadas y enviada por el equipo de alarma instalado en un domicilio privado".*

5. Cada uno de los logs sin distinción ligan indefectiblemente, por tanto, al interesado con el dispositivo, con todo lo que se genera y registra en relación con el mismo, y con el contrato suscrito. Cada uno de logs identifica unívocamente al interesado.

6. Además, todos los logs conciernen al interesado en relación con sus derechos, puesto que los logs se encuentran conectados con la seguridad de la vivienda, afectando al reclamante en cuanto a su derecho a la seguridad de su vivienda y de la seguridad en su propia vivienda.

7. Los logs identifican al reclamante, pues es información sobre una persona física identificada.

Por tanto, en este caso concreto y en atención al contexto, y examinadas todas las circunstancias concurrentes, el contenido de acceso ha de incluir todos los logs generados por el sistema de alarma, incluyendo los que la parte reclamada denomina como logs "técnicos", por ser considerados datos de carácter personal en los términos del artículo 4 del RGPD, incluyendo los que no se han entregado por ser catalogados como técnicos por la reclamada.

Se concluye, en este caso concreto, que todos los logs son datos de carácter personal, incluyendo los denominados técnicos por la reclamada, que identifican al reclamante y afectan de un modo u otro al reclamante, por lo que entrarían en el derecho de acceso que se debería proporcionar.

VI

Sobre la manifestación por parte de la reclamada de que los "*logs que no implican tratamiento de datos*", esto es, los logs "técnicos", podrían contener información sobre procesos técnicos internos, cuya revelación a terceros implicaría la cesión a terceros de su "*know how*" o secretos comerciales, el considerando 63 del RGPD señala:

"*Los interesados deben tener derecho a acceder a los datos personales recogidos que le conciernan y a ejercer dicho derecho con facilidad y a intervalos razonables, con el fin de conocer y verificar la licitud del tratamiento. Ello incluye el derecho de los interesados a acceder a datos relativos a la salud, por ejemplo los datos de sus historias clínicas que contengan información como diagnósticos, resultados de exámenes, evaluaciones de facultativos y cualesquiera tratamientos o intervenciones practicadas. Todo interesado debe, por tanto, tener el derecho a conocer y a que se le comuniquen, en particular, los fines para los que se tratan los datos personales, su plazo de tratamiento, sus destinatarios, la lógica implícita en todo tratamiento automático de datos personales y, por*

lo menos cuando se base en la elaboración de perfiles, las consecuencias de dicho tratamiento. Si es posible, el responsable del tratamiento debe estar facultado para facilitar acceso remoto a un sistema seguro que ofrezca al interesado un acceso directo a sus datos personales. Este derecho no debe afectar negativamente a los derechos y libertades de terceros, incluidos los secretos comerciales o la propiedad intelectual y, en particular, los derechos de propiedad intelectual que protegen programas informáticos. No obstante, estas consideraciones no deben tener como resultado la negativa a prestar toda la información al interesado. Si trata una gran cantidad de información relativa al interesado, el responsable del tratamiento debe estar facultado para solicitar que, antes de facilitarse la información, el interesado especifique la información o actividades de tratamiento a que se refiere la solicitud." (El subrayado es nuestro).

Se alude a los límites en cuanto a la modalidad de obtención del derecho de acceso que se contiene en el artículo 15.3 y 4 del RGPD, que indica:

"3. El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento...

4. El derecho a obtener copia mencionado en el apartado 3 no afectará negativamente a los derechos y libertades de otros."

Así pues, el derecho a obtener copia respecto del derecho de acceso "*no debe infringir los derechos o libertades de terceros, incluido el secreto de las empresas o la propiedad intelectual, incluido el software de protección de los derechos de autor".* Sin embargo, se reitera, estas consideraciones no deben dar lugar a la denegación de toda la información al interesado.

La Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo de 8/06*/* 2016 relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas, que se ha transpuesto a nuestro ordenamiento por la Ley de Secretos Empresariales 1/2019 de 20/02, indica en sus considerandos 34 y 35:

"(*34) La presente Directiva respeta los derechos fundamentales y observa los principios reconocidos, en particular, en la Carta, en especial el derecho al respeto de la vida privada y familiar, el derecho a la protección de los datos de carácter personal, la libertad de expresión y de información, la libertad profesional y el derecho a trabajar, la libertad de empresa, el derecho a la propiedad, el derecho a una buena administración, en particular al acceso a los expedientes, al mismo tiempo que se respeta el secreto comercial, el derecho a la tutela judicial efectiva y a un juez imparcial y el derecho de defensa.*

(35) Es importante que se respete el derecho al respeto de la vida privada y familiar y a la protección de los datos personales de toda persona cuyos datos personales puedan ser tratados por el poseedor de un secreto comercial cuando se tomen medidas para la protección del secreto comercial, o de toda persona implicada en un proceso judicial relativo a la obtención, utilización o revelación ilícitas de secretos comerciales, con arreglo a la presente Directiva, y cuyos datos personales sean objeto de tratamiento. La Directiva 95/46/CE del Parlamento Europeo y del Consejo regula el tratamiento de los datos personales efectuado en los Estados miembros en el contexto de la presente Directiva y bajo la supervisión de las autoridades competentes de los Estados miembros, en particular las autoridades públicas independientes designadas por estos. Así pues, la presente Directiva no debe afectar a los derechos y obligaciones previstos en la Directiva 95/46/CE, en

particular los derechos del interesado de acceder a aquellos de sus datos personales que sean objeto de tratamiento y de obtener la rectificación, supresión o bloqueo de los datos debido a su carácter incompleto o inexacto y, en su caso, la obligación de tratar los datos de carácter sensible de conformidad con el artículo 8, apartado 5, de esa misma Directiva."

Similar limitación a la prevista en el artículo 15.4 del RGPD se aplica al derecho a la portabilidad que se desarrolla en el artículo 20 del RGPD, estableciendo su número 4 que "*El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros*". Teniendo en cuenta que el derecho de acceso a la copia, como el derecho a la portabilidad de los datos se encuentran entre los componentes fundamentales del RGPD, sería aplicable en este sentido el razonamiento que para esta limitación señala el Grupo de Trabajo 29 en las directrices sobre el derecho a la portabilidad de los datos, adoptadas el 13/12/2016 determinan que:" *Puede entenderse, aunque no están directamente relacionados con la portabilidad, que esa mención incluye también «los secretos comerciales o la propiedad intelectual y, en particular, los derechos de propiedad intelectual que protegen los programas informáticos». No obstante, aunque estos derechos deben tomarse en consideración antes de responder a una solicitud de portabilidad de datos, «estas consideraciones no deben tener como resultado la negativa a proporcionar toda la información al interesado*".

Como conclusión a las alegaciones de la reclamada, ponderando el derecho de acceso del interesado y los derechos de la parte reclamada, se ha de atender a la conciliación de derechos de ambas partes conforme marca el párrafo 4 del artículo 15 del RGPD en la ejecución la ejecución de parte del contenido de la copia de los logs que integran el derecho de acceso.

De esta forma, la condición prevista el artículo 15.4 del RGPD se restringiría no a la copia de los logs, que son todos los logs como se ha motivado, sino a la parte de la copia de datos del log que pueda denotar información afectada por el secreto comercial en los términos que en el siguiente fundamento de derecho explicitaremos.

VII

Cualquier persona disfruta, en virtud de su artículo 15 del RGPD, del derecho de acceso a los datos personales que le conciernan y sean objeto de tratamiento, que establece:

"1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales…"

"3. El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.

4. El derecho a obtener copia mencionado en el apartado 3 no afectará negativamente a

los derechos y libertades de otros."

El derecho de acceso denominado habeas data o "*habeas scriptum"* constituye núcleo esencial del derecho regulado en el art.18.4 de la Constitución -STC 292/2000 y consiste en que el afectado puede exigir al responsable una prestación de hacer. El alcance del derecho de acceso está determinado por el alcance del concepto de datos personales definido en el artículo 4, apartado 1, del RGPD.

El derecho de acceso no debe considerarse aisladamente, ya que está estrechamente relacionado con otras disposiciones del RGPD, en particular con los principios de protección de datos, incluida la equidad y la legalidad del tratamiento, la obligación de transparencia del responsable del tratamiento y otros derechos de los interesados previstos en el capítulo III del RGPD. Especial importancia cobran en este procedimiento los artículos 5.1 b) a d), que recuerdan:

1. Los datos personales serán:

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

La protección del derecho fundamental al respeto de Protección de Datos de carácter personal implica, en especial, que toda persona física pueda cerciorarse de que los datos personales que le conciernen son exactos y se utilizan de manera lícita. El citado derecho de acceso puede ser indispensable, en particular, para permitir al interesado obtener, en su caso, del responsable del tratamiento de los datos, una rectificación, supresión o el bloqueo de esos datos y, en consecuencia, ejercer otros derechos que se relacionan con los fines para los que fueron recabados.

En tal sentido, si bien aludiendo a la entonces vigente, Directiva 95/46 del Parlamento Europeo y del Consejo, de 24/10/1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, se pronunció el Tribunal de Justicia de la Unión Europea, en el asunto "*Rijkeboer*", C/553/07, de 7/05/2009:

51"El citado derecho de acceso es indispensable para que el interesado pueda ejercer los derechos que se contemplan en el artículo 12, letras b) y c), de la Directiva, a saber, en su caso, cuando el tratamiento no se ajuste a las disposiciones de la misma, obtener del responsable del tratamiento de los datos, la rectificación, la supresión o el bloqueo delos datos [letra b)], o que proceda a notificar a los terceros a quienes se hayan comunicado los datos, toda rectificación, supresión o bloqueo efectuado, si no resulta imposible o supone un esfuerzo desproporcionado [letra c)].

52 El derecho de acceso es, igualmente, condición necesaria para el ejercicio por el interesado del derecho de oposición al tratamiento de sus datos personales, contemplado en el artículo 14 de la Directiva, como lo es para el derecho a recurrir por los daños sufridos, previsto en los artículos 22 y 23 de ésta."

El objetivo general del derecho de acceso es proporcionar a las personas información suficiente, transparente y fácilmente accesible sobre el tratamiento de sus datos personales para que puedan conocer y verificar la legalidad del tratamiento y la exactitud de los datos tratados.

Salvo que se indique expresamente lo contrario, la solicitud debe entenderse en el sentido de que se refiere a todos los datos personales relativos al interesado.

"*Así pues, si no se da el pleno acceso, se debe informar al interesado de las razones y circunstancias concretas que permitan conocer los motivos por si el reclamante desea tomar medidas contra esa consideración*", tal como se señala en el punto 172 de las citadas Directrices 1/2022.El responsable del tratamiento deberá buscar datos personales en todos los sistemas informáticos y en los ficheros no informáticos sobre la base de criterios de búsqueda que reflejen la forma en que se estructura la información.

En caso de que el responsable vaya a aplicar excepciones o restricciones al derecho de acceso deberá comprobar cuidadosamente a qué partes de la información se refiere la excepción y facilitar toda la información que no esté excluida por la excepción. Esta previsión formaría parte del tratamiento de datos desde el diseño, teniendo establecido previamente dicho aspecto suficientemente desarrollado, explicitado y documentado.

La comunicación de datos y otra información complementaria sobre el tratamiento debe facilitarse de forma concisa, transparente, inteligible y fácilmente accesible, utilizando un lenguaje claro y sencillo. Los requisitos más precisos a este respecto dependen de las circunstancias del tratamiento de los datos, así como de la capacidad del interesado para comprender la comunicación.

En tal sentido, además, el acceso proporcionado el 23/02/2021, no es adecuado, por incompleto, no es el formato de origen, sino un resumen, con información escasa y desordenada cronológicamente en el contenido del relato de los eventos que figuran registrados, limitándose en un modo no ordenado a la agrupación de fechas y denominación de logs, añadiendo una explicación propia que dada la diversidad y el carácter de las situaciones que se pueden presentar no satisface mínimamente el contenido del derecho de acceso.

Difiere del proporcionado el 14/12/2021 en cuanto a que este último es el formato original y que contiene todos los rasgos del log. Ahora bien, la parte reclamada no ha incluido todos los logs, puesto que faltan los que denomina logs "técnicos", resultando además que son incomprensibles en atención a las claves y abreviaturas que constan en documento cuyo significado se desconoce.

Así pues, y no obstante lo anterior, si los datos consisten en "*códigos*" como en este caso, u otros "*datos brutos*" del servicio, deben explicarse para que tengan sentido para el interesado. Tal explicación no se ha suministrado en el acceso proporcionado el 14/12/2021.

El acceso a los datos personales significa el acceso a los datos personales reales, no solo una descripción general de los datos ni una mera referencia a las categorías de datos personales tratados por el responsable del tratamiento.

Los datos brutos podrían explicarse como datos no analizados subyacentes a un tratamiento. Los datos brutos pueden existir en diferentes niveles, donde el nivel más bajo de datos solo puede ser legible por máquina (como «bits»). Cabe destacar que la información facilitada al interesado debe estar siempre en un formato legible por el ser humano.

Debido a que todos los logs figuran en un único bloque referido al dispositivo del reclamante, tanto los llamados logs técnicos como los que si se consideraron datos personales por la parte reclamada, tienen para su completa comprensión diversas columnas con diversos descriptores que precisan para ser descifrados, la traducción de las claves para todos los logs.

Al facilitar datos en un formato bruto, es importante que el responsable del tratamiento adopte las medidas necesarias para garantizar que el interesado comprenda los datos, por ejemplo, facilitando un documento explicativo que traduzca el formato bruto en un formulario fácil de usar. Además, podría explicarse en tal documento lo que significan las abreviaturas y otras siglas.

En cuanto a la aplicación del artículo 15.4 del RGPD, se alude al condicionante en cuanto a la modalidad de atención del derecho de acceso con el fin de conciliar los derechos en pugna con la parte reclamada, dado que no debe afectar al derecho de acceso mismo como hemos indicado anteriormente.

Debe tenerse en cuenta que el RGPD ha establecido que el derecho acceso comprende suministrar la información completa.

La condición prevista el artículo 15.4 del RGPD, se restringiría sólo a la entrega de copia a la parte reclamante de los datos que puedan estar afectados por el secreto comercial, es decir a parte de su contenido. Así, el reclamante puede recibir la respuesta del ejercicio del derecho de acceso en otra modalidad que no sea la copia, o incluso combinando varias modalidades si las circunstancias lo requieren como es este caso de derechos que pueden confluir en divergencias de intereses.

Se deduce que siendo el contenido de todos los logs el que se completa con las claves, descripciones de las tablas, comentarios, eventos, etc., el secreto se puede desvelar de todos los logs según la tesis de la reclamada. El contenido sensible a la seguridad a la hora de afrontar las circunstancias que surjan con los dispositivos puede afectar a ambos tipos de logs.

Figura una clave de "***(...)*** de la señal", una descripción, y otra algo más amplia en el campo "****COLUMNA.2* ***(...)***", "****COLUMNA.1*" , "*event*" etc elementos comunes con los datos personales, pero no se aprecia cual sería tal secreto comercial, o "*know how*" en forma de conocimiento de la actuación de los eventos que podría poner en peligro la seguridad de las medidas de la reclamada. En todo caso, ello debe ser objeto de interpretación restrictiva. Así, el riesgo para los secretos comerciales, o más en concreto, el que por el log se desvele la forma de actuar de la parte reclamante, debe estar suficientemente demostrado caso a caso a que afecta, o puede afectar. Puede haber ocasiones en que un solo indicativo de indicios de tal conocimiento o puede ser que aún con varias claves no se revela secreto alguno.

Como forma de respetar el "*know how*" de la reclamada, puede, excepcionalmente, caso a caso, justificar el motivo por el que información conjunta adicional complementaria de cada log que forma la tabla del acceso, o las claves conjuntas del mismo no deban proporcionarse en la modalidad de copia. Ello en relación a considerar que si se acreditase que se revela una especifica forma de actuar ante un evento que pudiera repercutir que el "*know how*" se pudiera conocer de forma injustificada.

En conclusión,

1. La parte reclamante tiene derecho a acceder a todos los logs, que son sus datos personales.

2. Se establecen dos modalidades combinadas y complementarias de acceso. Y ello en atención a la ponderación de los derechos e intereses concernidos, teniendo en consideración también el derecho de la parte reclamada al secreto comercial.

3. Una modalidad de acceso es la copia.

Teniendo en consideración el derecho de la parte reclamada al secreto comercial, en virtud del art. 15.4 del RGPD, se limita el contenido de la copia conteniendo todos los logs.

La limitación a la modalidad del derecho de acceso a la copia, implica, en este caso, no suministrar al reclamante los datos del contenido de los logs en aquellos casos en que puedan estar afectados por el secreto comercial. La parte reclamada deberá motivar tal afectación.

4. En la otra modalidad, y complementaria, a la anterior, la parte reclamada tendrá que habilitar una forma de acceso a todos los datos personales del reclamante, afectados o no por el secreto comercial, sin perjuicio de lo establecido para la copia.

5. En ambas modalidades de acceso, los datos personales han de suministrarse en formato original, comprensibles e inteligibles, con información complementaria para su comprensión.

VIII

Del análisis del supuesto concreto examinado y atendiendo a las circunstancias concretas puestas de manifiesto a lo largo del expediente administrativo, de lo que se entregó al reclamante, de su contenido y alcance, Securitas ha proporcionado en virtud de lo resuelto previamente por la AEPD, los "*logs*" en bruto, sin tratar, pero habiendo filtrado previamente los "*logs*" y excluyendo la información que considera que no son datos personales "*al tratarse de información exclusivamente técnica*" y ateniéndose a secreto comercial.

Asimismo, de los logs que considera contienen datos de carácter personal del reclamante no proporcionó los indicativos y claves que permitirían conocer por completo su significado.

Se considera que la parte reclamada ha incumplido la resolución de la Agencia Española de Protección de Datos con relación a las medidas que se le impusieron.

Los hechos se estiman constitutivos de una infracción, imputable a la parte reclamada, por vulneración del artículo 58.2.c) del RGPD, que dispone lo siguiente:

"2*. Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación*:

"c*) ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado en virtud del presente Reglamento*

Esta infracción se tipifica en el artículo 83.6 del RGPD, que estipula lo siguiente:

"*El incumplimiento de las resoluciones de la autoridad de control a tenor del artículo 58, apartado 2, se sancionará de acuerdo con el apartado 2 del presente artículo con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía*."

Que faculta a la AEPD a proceder conforme la facultad que le concede el artículo 58.2

"*i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular*;"

En este caso, procede por la falta de atención en cumplir en sus términos, alcance y contenido el contenido esencial del derecho de acceso, y por el impedimento que supone privar de los datos que son objeto de tratamiento, una multa administrativa.

El artículo 71 de la LOPDGDD indica:

"*Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 , así como las que resulten contrarias a la presente ley orgánica*."

A efectos del plazo de prescripción de las infracciones, la infracción imputada prescribe a los tres años, conforme al artículo 72.1 de la LOPDGDD, señala:

"1*. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes*:"

"*m) El incumplimiento de las resoluciones dictadas por la autoridad de protección de datos competente en ejercicio de los poderes que le confiere el artículo 58.2 del Reglamento (UE) 2016/679*."

IX

La multa que se imponga deberá ser, en cada caso individual, efectiva, proporcionada y disuasoria, conforme a lo establecido en el artículo 83.1 del RGPD. En consecuencia, se deberá graduar la sanción a imponer de acuerdo con los criterios que establece el artículo 83.2 del RGPD, y con lo dispuesto en el artículo 76 de la LOPDGDD, respecto al apartado k) del citado artículo 83.2 del RGPD.

Se tienen en consideración las siguientes circunstancias:

-artículo 83.2.a) ”*la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido*;”

En las ocasiones que se proporcionó el acceso, las dos primeras con el mismo contenido, y una tercera tras la resolución del procedimiento de ejercicio de derechos fue incompleto, no parcial, ya que no se refleja ni todo su contenido ni tampoco se facilita su comprensión. Se trata de operaciones de tratamientos de datos, en una materia como la relacionada con la seguridad de una vivienda. Tales elementos operarían como agravantes. El incumplimiento de la obligación de atender el derecho no puede tener las mismas consecuencias en función de la duración, persistencia de las razones negativas o reiteradas respuestas, acreditándose en este caso una mayor gravedad que cualifica la respuesta sancionadora.

-artículo 83.2.b) del RGPD, “*la intencionalidad o negligencia en la infracción*” que se manifiesta en que el 17/09/2021 se resolvió el procedimiento sobre ejercicio de derechos, TD/00167/2021, si bien recurrido en reposición, el 27/10/2021 confirma la resolución del TD, notificada al día siguiente a la reclamada. No consta que cumpliera la atención del derecho en el plazo que se le otorgaba en la resolución, que rebasa ampliamente, y que solo tras hacer el reclamante la preceptiva manifestación de no haber recibido nada al respecto, tuvo la AEPD que dirigirse a la reclamada que solo entonces, se aviene a remitirle el último escrito de 14/12/2021, que continua sin satisfacer el contenido del derecho. La actuación denota una clara negligencia en el cumplimiento del deber que le corresponde.

Manifiesta la reclamada que actúa con diligencia al contratar a una entidad para estudiar los logs en su relación con los datos personales con el fin de atender la petición del reclamante

Respecto esta afirmación, parece contradecir otra que la reclamada señaló en alegaciones al mismo acuerdo de inicio, de que la contratación del servicio jurídico que se plasmó en el informe del documento 1, se hizo principalmente al efecto de cumplimiento normativo que prevé valorar que datos se están tratando. Siendo los logs datos comunes a todos los productos derivados de una alarma, que gestiona la reclamada, desde la entrada en vigor del RGPD debería haber implementado el tratamiento desde el diseño que se ha mencionado en la resolución, con el objeto de que el responsable ponga en funcionamiento las medidas técnicas y organizativas para implementar los principios y salvaguardas de los derechos individuales. En esencia, esto significa que debe integrar la protección de datos en sus actividades de tratamiento y prácticas comerciales, desde la etapa de diseño y durante el ciclo de vida. Ayuda a asegurarse de cumplir con los principios y requisitos fundamentales del RGPD, y forma parte del enfoque de responsabilidad. Esa supuesta diligencia no es ni más ni menos que el cumplimiento que la normativa establece.

-artículo 76.2 b) de la LOPDGDD:” *La vinculación de la actividad del infractor con la realización de tratamientos de datos personales*”. La reclamada dispone de productos que oferta para los que son imprescindibles su gestión habitual de tratamiento datos que aparecen relacionados en contratos junto a sus dispositivos.

En cuanto a las alegaciones con las que la reclamada pretende atenuar la sanción por manifestar que atendió, si bien parcialmente el derecho, en tres ocasiones, se debe indicar que el acceso de 23/02/2021, reproducido el 18/05/2021 son meros accesos formales reiterados, elaboraciones propios con una descripción de log con explicación genérica, atención que es incompleta, no parcial. No solo no procede del original, es una elaboración de la reclamada, le faltan las claves para su comprensión y la descripción de los eventos, sino que tampoco comprende los logs que la reclamada denomina impropiamente "*técnicos*". Además, deduciendo que ha sido un cumplimiento parcial, trata de anudar la consecuencia de que el acceso es un incumplimiento de tipo leve a los efectos de la prescripción del artículo 74.c) de la LOPDGD. Por el contrario, la infracción de tal modo, tanto de resultas de los accesos con el mismo contenido, como el que tiene lugar con el proporcionado el 14/12/2021, se ha de calificar de sustancial, descartando su carácter siquiera formal, cuanto menos "*meramente formal*", repercutiendo en que no tuvo ni ha tenido acceso a toda la información y la repercusión que tiene para el afectado.

Sobre la buena fe alegada, "*se ha dado cumplimiento hasta en tres veces*", se considera que no es importante las veces en que se de el cumplimiento, porque con una sería suficiente, estimando que las ocasiones en que se ha proporcionado, han sido con contenido incompleto, no parcial como estima la reclamada. Por otro lado, la buena fe no acredita la ausencia de culpabilidad y antijuricidad.

Se considera que en función de los factores mencionados, por la infracción del artículo 58.2 del RGPD, se acuerda imponer una sanción de multa de 50.000 euros.

X

Como poder correctivo, corresponde a esta AEPD: "*ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado en virtud del presente Reglamento*".(artículo 58.2.c) del RGPD)

La reclamada ha de completar el acceso solicitado, proporcionando todos los logs que ha excepcionado hasta la fecha, comprendiendo la totalidad de los logs contenidos por orden cronológico en el documento 2 del cuadro aportado en las alegaciones al acuerdo de inicio, que se marcaban en color rojo, en el que se complementan y suceden lógicamente los registros del dispositivo.

La información habrá de contener las claves que permitan clarificar la citada tabla y sus apartados que hagan comprensible los cuadros de los datos en formato de línea o en bruto como los obtiene la reclamada.

Las especificidades del fundamento de derecho VI y VII se tendrán en cuenta como modalidad de cumplimiento de la medida impuesta.

La imposición de esta medida es compatible con la sanción consistente en multa administrativa, según lo dispuesto en el art. 83.2 del RGPD.

Se advierte que no atender a los requerimientos de este organismo puede ser considerado como una infracción administrativa conforme a lo dispuesto en el RGPD, tipificada como infracción en su artículo 83.5 y 83.6, pudiendo motivar tal conducta la apertura de un ulterior procedimiento administrativo sancionador.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada,

la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER a **SECURITAS DIRECT ESPAÑA, S.A.**, con NIF ***A26106013***, por una infracción del aartículo 58.2 c) del RGPD, tipificada en el artículo 83.6 del citado RGPD, y calificada, a efectos de prescripción como grave en el artículo 72.m) de la LOPDGDD, una sanción administrativa de 50.000 euros.

SEGUNDO: En virtud del artículo 58.2.c) del RGPD que faculta para "*ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado en virtud del presente Reglamento*;" se le requiere para que en el plazo de quince días atienda el derecho objeto de esta reclamación en la forma señalada.

El incumplimiento de lo dispuesto podría dar lugar el ejercicio de la potestad sancionadora de acuerdo con lo señalado en el artículo 83.6 del RGPD.

TERCERO: NOTIFICAR la presente resolución a **SECURITAS DIRECT ESPAÑA, S.A.**

CUARTO: Advertir al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el art. 98.1.b) de la LPACAP en el plazo de pago voluntario establecido en el art. 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29/07, en relación con el art. 62 de la Ley 58/2003, de 17/12, mediante su ingreso, indicando el NIF del sancionado y el número de procedimiento que figura en el encabezamiento de este documento, en la cuenta restringida nº ***IBAN: ES00-0000-0000-0000-0000-0000***, abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A.. En caso contrario, se procederá a su recaudación en período ejecutivo.

Recibida la notificación y una vez ejecutiva, si la fecha de ejecutividad se encuentra entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si se encuentra entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, 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 13707, 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.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado

manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada LPCAP. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-181022

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