- Procedimiento Nº: PS/00225/2019

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: El 05/02/2019, D. ***A.A.A.***, en representación de FACUA - ASOCIACIÓN DE CONSUMIDORES Y USUARIOS EN ACCIÓN (en lo sucesivo FACUA), interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra HOLALUZ-CLIDOM, S.A., con NIF ***A65445033*** (en adelante HOLALUZ). Los motivos en los que basa la reclamación son, en síntesis, los siguientes: la vulnerabilidad del sitio web *https://www.holaluz.com* titularidad de la empresa al quedar expuestos los datos asociados al CUPS (Código Universal Punto de Suministro), de centenares de usuarios; cualquier persona que acceda a la citada web puede conocer el volumen de consumo eléctrico que se produce en cualquier inmueble con solamente introducir la dirección del inmueble que le interese y tener acceso a datos que únicamente debería conocer el titular del suministro.

Se adjunta como documento único video certificado por la empresa *save the proof.com* (que según su web certifica el contenido de páginas web y ficheros con validez legal), en el que se puede apreciar el funcionamiento de la web en lo que se refiere a lo descrito anteriormente.

Asimismo, el reclamante aporta escrito en el que declara haber enviado un e-mail el 28/01/2019 al reclamado en el que informaba de los hechos manifestados anteriormente, sin que se haya dado respuesta al mismo; adjunta copia del correo electrónico, así como del perfil de la red social twiter de HOLALUZ.

SEGUNDO: Tras la recepción de la reclamación, la Subdirección General de Inspección de Datos procedió a realizar las siguientes actuaciones:

El 26/02/2019 fue trasladada a HOLALUZ la reclamación presentada para su análisis y comunicación a la denunciante de la decisión adoptada al respecto. Igualmente, se le requería para que en el plazo de un mes remitiera a la Agencia determinada información:

- Copia de las comunicaciones, de la decisión adoptada remitida al reclamante a propósito del traslado de la reclamación y acreditación de que el reclamante había recibido la comunicación de dicha decisión.

- Informar sobre las causas que motivaron la incidencia que originó la reclamación.

- Informar de las medidas adoptadas para evitar que se vuelvan a producir incidencias similares.

- Cualquier otra que considere relevante.

En la misma fecha se le comunicaba a la reclamante la recepción de la reclamación y su traslado a la entidad reclamada.

HOLALUZ no ha dado respuesta a la solicitud de información formulada por la Agencia Española de Protección de Datos.

TERCERO: El 21/05/2019, de conformidad con el artículo 65 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada por el reclamante contra HOLALUZ.

CUARTO: Con fecha 04/10/2019, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al reclamado, por la presunta infracción por la presunta infracción del artículo 32.1, 33 y 34 del RGPD sancionada conforme a lo dispuesto en el artículo 83.4.a) del citado Reglamento.

QUINTO: Notificado el citado acuerdo de inicio, el reclamado presentó escrito de alegaciones el 10/07/2019 manifestando, en síntesis, lo siguiente: que en fecha 16/12/2019 la sociedad CLIDON llevo a cabo la transformación de SL a SA y la modificación de su denominación social pasando a denominarse HOLALUZ CLIDON; el error atribuido por la supuesta ausencia de notificación de la brecha de seguridad de datos personales, no siendo cierto ya que fue presentada en fecha 15/02/2019; el cumplimiento de la normativa sobre protección de datos por parte de la entidad habiéndose establecido medidas de seguridad adecuada; la ausencia de vulneración del artículo 32.1 de RGPD; el cumplimiento del deber de notificar la existencia de la brecha de seguridad; la ausencia de obligación en el deber de notificar la brecha de seguridad a los interesados; el cumplimiento del deber de colaboración y de gestión de la brecha de seguridad; la solicitud de archivo del procedimiento.

SEXTO: Con fecha 19/12/2019 se inició la apertura de un período de práctica de pruebas, acordándose las siguientes:

- Dar por reproducidos a efectos probatorios la reclamación interpuesta por FACUA - ASOCIACIÓN DE CONSUMIDORES Y USUARIOS EN ACCIÓN y su documentación, los documentos obtenidos y generados por los Servicios de Inspección que forman parte del expediente E/02128/2019.
- Dar por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio PS/00225/2019 presentadas por CLIDOM ENERGY S.L. (HOLALUZ), y la documentación que a ellas acompaña.
- Mediante diligencia del instructor se incorporan al expediente impresiones de pantalla de la web de HOLALUZ.

SEPTIMO: En fecha 29/06/2020 fue emitida Propuesta de Resolución en el sentido de que por la Directora de la AEPD se archivara al reclamado por la presunta vulneración de los artículos 32.1, 33 y 34 del RGPD, tipificadas en el artículo 83.4.a) del citado Reglamento.

Transcurrido el plazo establecido para ello el reclamado no ha presentado escrito de alegaciones al tiempo de dictar la presente resolución.

OCTAVO: De las actuaciones practicadas han quedado acreditados los siguientes hechos probados:

HECHOS PROBADOS

PRIMERO. FACUA mediante escrito de 05/02/2019, interpuso reclamación ante la Agencia Española de Protección de Datos contra HOLALUZ, como consecuencia de la

vulnerabilidad del sitio web *https://www.holaluz.com* al quedar expuestos los datos asociados a la CUPS de centenares de usuarios y que cualquier persona que accediera a la citada web puede tener conocimiento del consumo eléctrico que se produce en cualesquiera de los domicilios con solamente introducir la dirección del mismo.

SEGUNDO. Consta aportado por FACUA video certificado por la empresa *SAVE THE PROOF* en el que se puede apreciar el funcionamiento de la web en el que se especifica paso a paso lo descrito en el punto anterior.

TERCERO. Consta acreditado que FACUA remitió a HOLALUZ el 28/01/2019 correo electrónico informando de los hechos descubiertos, manifestando que no se ha dado respuesta al mismo y desconociéndose si se ha llevado a cabo actuación técnica para subsanar los hechos denunciados.

CUARTO. Consta aportada escritura de transformación de sociedad limitada en sociedad anónima, así como de la modificación de su denominación social a través de escritura pública, de CLIDOM ENERGY S.L. de 16/09/2019 pasando a denominarse HOLALUZ CLIDOM, S.A.

QUINTO. Consta acreditado que HOLALUZ en fecha 15/02/2019 notificó a la AEPD brecha de confidencialidad ocurrida el 14/02/2019, adjuntando el justificante de presentación de la notificación de brecha de seguridad y el anexo a la notificación de la misma en la que se acredita haber adoptado medidas de carácter técnico y organizativas. Asimismo consta que HOLALUZ remitió a FACUA correo electrónico de 18/02/2019 informando de las medidas adoptadas para resolver el incidente de seguridad reclamado.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada autoridad de control, y según lo establecido en los artículos 47 y 48 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para iniciar y para resolver este procedimiento.

II

El artículo 32 del RGPD "*Seguridad del tratamiento",* establece que:

"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros".

El artículo 33 del RGPD, *Notificación de una violación de la seguridad de los datos personales a la autoridad de control,* establece que:

"1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;

c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;

d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo".

Y el artículo 34, *Comunicación de una violación de la seguridad de los datos personales al interesado,* establece que:

"1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;

c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3".

III

El RGPD define las quiebras de seguridad de los datos personales como aquellos incidentes que ocasionan la destrucción, pérdida o alteración accidental o ilícita de datos personales, así como la comunicación o acceso no autorizado a los mismos.

Desde el pasado 25/05/2018, la obligación de notificar a la Agencia las brechas o quiebras de seguridad que pudiesen afectar a datos personales es aplicable a cualquier responsable de un tratamiento de datos personales, lo que subraya la importancia de que todas las entidades conozcan cómo gestionarlas.

Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas.

El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación.

Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continúas o similares.

También hay que señalar, que la notificación de una quiebra de seguridad implica analizar la diligencia del responsable o en su caso encargado/s y las medidas aplicadas.

En el artículo 33 del RGPD establece la forma en que ha de notificarse una violación de la seguridad de los datos personales a la autoridad de control.

Y el artículo 34 del Reglamento mencionado indica cuando es necesario informar de una violación de la seguridad de los datos personales al interesado.

En este mismo sentido se señala en los Considerandos 85 y 86 del RGPD:

(85) *Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión. Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que*

el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida.

(86) *El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación. Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continuas o similares.*

IV

En el presente caso**,** los hechos reclamados sugerían que en la página web titularidad del reclamado habían quedado expuestos los datos asociados al CUPS de centenares de usuarios; manifiesta el reclamante que cualquier persona que accediera a la citada web podía conocer el volumen de consumo eléctrico que se produce en cualquier inmueble con solamente introducir la dirección del inmueble que le interese y tener acceso a datos que únicamente debería conocer el titular del suministro.

Asimismo, se señalaba en el Hecho Segundo del acuerdo de inicio del procedimiento sancionador que el reclamado no había notificado al supervisor la quiebra que se le había puesto de manifiesto por el reclamante, ni había dado respuesta al requerimiento informativo realizado por la AEPD.

Hay que señalar que a la luz de los documentos aportados como la propia entidad reclamada ha indicado y así consta en los hechos probados que el 15/02/2019 notificó a la AEPD la incidencia detectada e informada por FACUA, adjuntando el justificante de presentación de la notificación de brecha de seguridad y el anexo a la notificación en la que se acreditaba haber adoptado medidas de carácter técnico y organizativas pertinentes.

También aportaba la respuesta que le fue ofrecida a FACUA mediante correo electrónico de 18/02/2019 informándoles de la situación, a pesar de que FACUA ha señalado que la mercantil no había procedido a atender sus mensajes.

En primer lugar, hay que señalar que la cesión de los datos por los distribuidores de energía y el posterior tratamiento de los mismos por parte de los comercializadores del sector energético se encuentra habilitada en la Ley 54/1997, de 27 de diciembre, del Sector Eléctrico y en la Ley 34/1998, de 7 de octubre, del Sector

de Hidrocarburos. De conformidad con la citada norma, los datos personales de los usuarios podían obtenerse de las bases de datos de puntos de suministro. Las entidades del sector debían contar con una base de datos denominada Sistema de Información de Puntos de Suministro (SIPS) conteniendo una serie de datos técnicos y personales de los titulares de los puntos de suministro de gas y electricidad.

El Real Decreto 1074/2015, de 27 de noviembre, por el que se modifican determinadas disposiciones en el sector eléctrico, estableció una nueva redacción del artículo 7 del Real Decreto 1435/2002, de 27 de diciembre.

De esta forma, ni las empresas comercializadoras ni la CNMC pueden acceder a partir de la modificación a cualquier información que identifique al titular del punto de suministro, y en particular a los datos recogidos c), z) y aa) del apartado 1, es decir:

"c) Ubicación del punto de suministro, que incluye dirección completa (tipo de vía, nombre de la vía, número, piso y puerta). Esta información debe referirse en todo momento al punto de suministro y no a la ubicación, población y provincia del titular de dicho punto de suministro que se exige en la letra aa) de este mismo artículo.

z) Nombre y apellidos, o en su caso denominación social y forma societaria, del titular del punto de suministro.

aa) Dirección completa del titular del punto de suministro. Esta información debe referirse en todo momento al titular del punto de suministro y no a la ubicación, población y provincia de dicho punto de suministro que se exige en la letra c) de este mismo artículo"

Esta información continua en poder de las empresas distribuidoras, que ya no pondrán a disposición de las comercializadoras o de la CNMC desde ese momento.

Por tanto, con la nueva regulación no se podía acceder a cualquier información que directamente identificara al titular del punto de suministro.

El reclamado es una empresa comercializadora de energía eléctrica y gas. En virtud del Real Decreto 1435/2002, de 27 de diciembre, por el que se regulan las condiciones básicas de los contratos de adquisición de energía y de acceso a las redes en baja tensión, y de conformidad con lo anteriormente señalado tiene acceso al Sistema de Información de Puntos de Suministro (SIPS), es decir, conjunto de datos que recoge la potencia, el consumo de los usuarios, etc., para que las comercializadoras puedan realizarles ofertas personalizadas.

En el caso presente para que un cliente pudiera consultar la tarifa a contratar debe incluir en el formulario que figura en la página web la dirección postal del punto de suministro o el Código Unificado de Punto de Suministro y, seleccionada la vivienda o local en el que el cliente quiere solicitar el suministro, la página web procesa una serie de datos sugiriendo al cliente una cuota estimada.

Por tanto, los únicos datos a los que accede el cliente al realizar el cálculo son: la cuota estimada (la cual se calcula teniendo en cuenta ciertos datos de forma interna sin que el cliente pueda conocerlos y utilizando una serie de algoritmos) y la CUPS que se encuentra cifrado; en ningún caso una vez adoptadas las medidas anteriores

se proporciona el volumen de consumo de la vivienda o local, el número CUPS, la potencia actual contratada, etc.

El reclamado ha manifestado que decidió no incluir el dato de la *"potencia actual contratada"* con el fin de proteger la información de los consumidores, aunque haya recibido quejas de sus clientes por no proporcionar dicho dato dado que consideran que necesitan dicha información para la evaluación del proceso de contratación y la simulación de la cuota estimada.

Por tanto, a través de la información proporcionada al realizar dicho cálculo no pueden conocerse los hábitos de consumo, potencia contratada, etc.

Por otra parte, el reclamado ha señalado que el acceso al CUPS, potencia contratada, etc,. solo era posible con ciertos conocimientos de programación y utilizando mecanismos maliciosos para la obtención de la información.

Sin embargo, el reclamado había establecido determinadas cautelas; asi en la página web los interesados aceptan, al acceder y utilizar la misma, las condiciones establecidas en el *"Aviso Legal"* señalando en su punto 5, que los usuarios de la web se comprometen a utilizar la página web de forma correcta, diligente y lícita, de conformidad con la ley.

Tampoco se tiene evidencia de que se haya accedido a la información de los usuarios habiéndose extraído datos de manera masiva. El propio reclamado ha señalado la imposibilidad de que esto pudiera ocurrir al tener implementadas medidas de seguridad que limitaban en el tiempo el número de veces que una misma IP podía consultar varias ofertas a través de la web e introduciendo diferentes direcciones o CUPS y que dicha comprobación se llevó a cabo analizando la evolución de las visitas a la página web y al formulario de contratación y que comparativamente no había aumentado sino que se había mantenido constante en el tiempo.

Asimismo, hay tener presente la Sentencia de la sala de lo Contencioso-Administrativo de la Audiencia Nacional de 25/02/2010 (Recurso 226/2009), en su Fundamento de Derecho Quinto, dispone:

"En el caso de autos, el resultado es consecuencia de una actividad de intrusión, no amparada por ordenamiento jurídico y en tal sentido ilegal, de un tercero con altos conocimientos técnicos informáticos que rompiendo los sistemas de seguridad establecidos accede a la base de datos de usuarios registrados en www.portalatino.com, descargándose una copia de la misma. Y, tales hechos, no pueden imputarse a la entidad recurrente pues, de otra forma, se vulneraría el principio de culpabilidad.

El principio de culpabilidad, previsto en el artículo 130.1 de la Ley 30/1992, dispone que solo pueden ser sancionadas por hechos constitutivos de infracción administrativa los responsables de los mismos, aún a título de simple inobservancia. Esta simple inobservancia no puede ser entendida como la admisión en el derecho administrativo sancionador de la responsabilidad objetiva, que está proscrita, después de la STC 76/1999, que señaló que los principios del ámbito del derecho penal son aplicables, con ciertos matices, en el ámbito administrativo sancionador, requiriéndose la existencia de dolo o culpa. En esta línea la STC 246/1991, de 19 de diciembre,

señaló que la culpabilidad constituye un principio básico del Derecho administrativo sancionador. Culpabilidad, que no concurre en la conducta analizada de Portal Latino."

Por último, el reclamado creó una comisión formal para formalizar y gestionar un plan de acción adoptando una serie de medidas con el fin de hacer frente a la posibilidad de acceder a la información y cuyo resultado fue la encriptación de los datos con el objetivo de que ni siquiera una persona que actuara maliciosamente y con voluntad de hackear la web pudiera tener acceso al CUPS, potencia contratada y consumo efectivo de una vivienda.

En cuanto a la segunda de las infracciones que habría cometido el reclamado, no haber procedido a cumplir con la obligación de notificar la brecha de seguridad conforme exige el artículo 33 del RGPD, como ya se ha aludido con anterioridad consta acreditado que se procedió a llevar a cabo la notificación a través de la Dirección Electrónica Habilitada de la AEPD. Paralelamente, tras la notificación de la brecha y su análisis, se procedió a dar respuesta por escrito al reclamante, FACUA.

La tercera presunta infracción que habría cometido el reclamado sería la falta de cumplimiento de la obligación de notificación de la brecha de seguridad a los interesados, de conformidad con el artículo 34 del RGPD. Sin embargo, en la notificación de 15/02/2019 el reclamado señala haber realizado un análisis interno determinándose que no concurrían los elementos necesarios para tener que llevar a cabo una notificación de la incidencia a los interesados, comprobarse que no existían evidencias de que se hubiera llevado a cabo extracción de la información y no existir un alto riesgo para los derechos y los intereses de los afectados.

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: ARCHIVAR a HOLALUZ-CLIDOM S.A., con NIF ***A65445033***, por la presunta infracción de los artículos 32.1, 33 y 34 del RGPD, tipificados en el artículo 83.4 del RGPD.

SEGUNDO: NOTIFICAR la presente resolución a HOLALUZ-CLIDOM S.A., con NIF ***A65445033***.

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

Contra esta resolución, que pone fin a la vía administrativa 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 13 de julio, reguladora de la

Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

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 Ley 39/2015, de 1 de octubre. 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.

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