- **Expediente N.º: EXP202210236**

RESOLUCIÓN DE PROCEDIMIENTO DE APERCIBIMIENTO

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

ANTECEDENTES

PRIMERO: Como consecuencia de la notificación a la División de Innovación Tecnológica de esta Agencia de una brecha de datos personales del responsable del tratamiento ***POZO LIMPIO SL (LAOOAL VECINDARIO)*** (en adelante, la entidad notificante), con número de registro de entrada ******NÚMERO.1*** relativa a un ciberincidente, se ordena a la Subdirección General de Inspección de Datos que realice las oportunas investigaciones previas con el fin de determinar una posible vulneración de la normativa de protección de datos.

En la citada notificación se informaba a la Agencia Española de Protección de Datos que se había producido una sustracción de un dispositivo teléfono móvil de su titularidad que contenía fotografías de partes íntimas de pacientes antes y después de los tratamientos estéticos. Se afirmaba, asimismo, no tener constancia de que se hubiera materializado daño alguno y que dicho dispositivo se encontraba apagado y protegido con su contraseña y patrón de acceso. Manifiesta que en el dispositivo sustraído se encuentran datos de menores, así como de personas físicas de otros países.

SEGUNDO: En virtud de lo mencionado, la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de extremos que seguidamente se exponen.

Por lo que se refiere a los hechos, en los términos indicados por la entidad notificante, se ha producido la sustracción de un dispositivo teléfono móvil de una clínica, el cual contiene fotografías de partes íntimas de pacientes antes y después de los tratamientos estéticos. Al parecer, la empleada que habitualmente desarrolla su labor en la recepción, se encontraba ausente del lugar realizando una gestión, momento en el que un tercero no identificado aprovechó su puntual ausencia para apropiarse del dispositivo móvil.

Los datos comprometidos consistirían en datos identificativos, de contacto, imagen y salud de unos 150 afectados, entre los que se encuentran menores y cuatro afectados de otros países. De forma concreta, se afirma que la brecha ha podido afectar a un interesado en Alemania, otro en Francia, uno en Italia y otro interesado en Países Bajos. Hay cierta probabilidad de que haya afectado a un cliente sito en Brasil.

La entidad manifiesta que no tiene constancia de la utilización de los datos contenidos en el dispositivo y después de un análisis en diversos buscadores de Internet tampoco se han encontrado evidencias de publicaciones al respecto.

Asimismo, consta que se interpuso denuncia ante los Cuerpos y Fuerzas de Seguridad del Estado de tales hechos.

Por lo que se refiere a la naturaleza de la entidad notificante, la misma es una sociedad limitada de nacionalidad española y que figura como filial de grupo y cuya actividad consiste en *"Lavado y limpieza de prendas textiles y de piel"*.

Con fecha 30/09/2022, y en virtud de lo dispuesto en el artículo 34.4 del Reglamento (UE) 2016/679 General de Protección de Datos, (en adelante RGPD se emitió por la presente autoridad una resolución a través de la cual se obligaba a la entidad notificante a comunicar a los afectados la violación de seguridad producida.

En cumplimiento de la mencionada resolución, la entidad notificante informa que la misma se ha producido dentro del plazo indicado, en fechas 18 y 21 de octubre de 2022, vía WhatsApp, de lo cual aporta copia. Afirma que, si bien se estimaban 150 afectados, de forma proactiva y dada la imposibilidad de concretar qué interesados fueron afectados por el incidente, se realizó la comunicación a un total de 1430 interesados. En el texto del mensaje se informa de la sustracción del dispositivo que contenía información de los clientes, afirmando que no hay constancia de que se haya podido acceder a los datos afectados ya que el dispositivo se encontraba protegido con patrón de seguridad y clave PIN. Asimismo, informan que lo han puesto en conocimiento de las Fuerzas y Cuerpos de Seguridad del Estado e incluyen dirección para contactar con el delegado de protección de datos (***infodpo@forlopd.es***).

Respecto de las medidas de seguridad implantadas, la entidad ha aportado los siguientes documentos:

- Un registro de actividad del tratamiento donde figura el tratamiento "Toma y comparativa de imágenes para la comprobación de la efectividad del tratamiento"
- Un análisis de Riesgo del mencionado tratamiento donde figuran los controles aplicar ya que se considera de riesgo ALTO. No obstante, al tener medidas de seguridad para el acceso de los dispositivos (patrón y PIN) afirman que el riesgo es bajo ya que para acceder al contenido "*se precisa su formateo con el consecuente borrado de todos los datos albergados en el mismo"*.

La entidad manifiesta que tiene contratados los servicios de consultoría en protección de datos, así como el asesoramiento y supervisión como Delegado de Protección de Datos externo desde diciembre de 2019 y aporta "*Manual de medidas de seguridad*" relativo a la protección de datos implantada en la entidad con anterioridad al hecho acaecido. En dicho documento define el uso adecuado de los recursos de la organización referentes a dispositivos tecnológicos, incluyendo una serie de medidas de seguridad aplicables a cualquier dispositivo que se utilice con fines laborales.

En este sentido, la entidad manifiesta que, a pesar de las medidas de seguridad implantadas, no se ha podido impedir el robo del dispositivo.

Respecto a las medidas implementadas con posterioridad a la violación de seguridad, afirma haber implantado dispositivo específico para las imágenes con acceso al contenido y formateo de forma remota junto con una contraseña robusta. Este dispositivo se ha almacenado en dependencias no accesibles al público y solo se

utilizará por determinados empleados. Además, se ha reducido el periodo para traspasar las imágenes al Sistema Informático y borrado del contenido en los dispositivos. Asimismo, manifiesta que ya se ha iniciado los trámites para realizar acciones de formación y concienciación.

Por último, por lo que se refiere a la posible la recurrencia de estos hechos y número de eventos análogos acontecidos en el tiempo, la entidad afirma no haber sufrido ningún evento de seguridad que comprometiera los datos personales de los clientes y pacientes.

TERCERO: Con fecha 15 de septiembre de 2023, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento de apercibimiento a la entidad notificante, por la presunta infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD.

CUARTO: La notificación del citado acuerdo de iniciación, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), fue recogida en fecha 13/12/2023 como consta en el acuse de recibo que obra en el expediente.

QUINTO: Una vez transcurrido el plazo otorgado para la formulación de alegaciones, se ha constatado que no se ha recibido alegación alguna por la entidad notificante.

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran hechos probados los siguientes,

HECHOS PROBADOS

PRIMERO: Tal y como se desprende de las actuaciones de investigación, queda acreditada la sustracción de un dispositivo teléfono móvil de un local de la entidad notificante, el cual contenía fotografías de partes íntimas de pacientes antes y después de los tratamientos estéticos. Dicho hecho fue debido a la ausencia temporal de la empleada que habitualmente desarrollaba su labor en la recepción mientras realizaba una gestión, momento que fue aprovechado por un tercero no identificado para apropiarse del dispositivo móvil.

SEGUNDO Los datos comprometidos consisten en datos identificativos, de contacto, imagen y salud de unos 150 afectados, entre los que se encuentran menores y cuatro afectados de otros países. Dada la imposibilidad de determinar de forma concreta los interesados afectados por el incidente, se realizó por la entidad notificante la comunicación de la brecha a un total de 1430 clientes.

TERCERO No se ha tenido constancia hasta la fecha de la utilización de los datos que se contenían en el dispositivo ni evidencias de publicaciones en Internet con relación a dicho contenido.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con los poderes que el artículo 58.2 del RGPD otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1 y 64.3 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, 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
Obligación incumplida

En relación a la seguridad del tratamiento, el artículo 32 del RGPD estipula lo siguiente:

"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."

En el presente supuesto, de las actuaciones investigación realizadas, así como de las propias declaraciones de la entidad notificante, se desprende que no fueron aplicadas las medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad adecuado el riesgo. Dicho riesgo, tal y como ha afirmado la propia entidad, es considerablemente alto, teniendo en cuenta los datos personales que se trataban, que incluían partes íntimas de los pacientes incluyendo entre los afectados a menores de edad.

La no aplicación de las medidas adecuadas se manifiesta en los propios hechos acaecidos, pues la propia sustracción del dispositivo tuvo lugar sin que mediase ninguna fuerza e intimidación; por el contrario, bastó con un simple despiste o abandono temporal del puesto de trabajo para que una persona ajena a la entidad pudiera hacerse con el dispositivo.

III

Tipificación y calificación de la infracción

De conformidad con hechos descritos en la presente resolución se considera que la entidad notificante ha incumplido la obligación prevista en el mencionado artículo 32.1 consistente en adoptar las medidas técnicas y organizativas adecuadas para garantizar un adecuado nivel de seguridad.

El incumplimiento de dicha obligación supone la comisión de una infracción, imputable a la entidad notificante ***POZO LIMPIO SL (LAOOAL VECINDARIO)***, prevista en el artículo 83.4 del RGP, el cual dispone expresamente:

“Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;”

A efectos del plazo de prescripción de las infracciones, la infracción imputada prescribe a los dos años, conforme al artículo 73 f) de la LOPDGDD, que califica de grave la siguiente conducta:

“f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679].

IV

Apercibimiento

Sin perjuicio de lo dispuesto en el mencionado artículo 83 del RGPD, el citado Reglamento dispone en el apartado 2.b) del artículo 58 "*Poderes*" lo siguiente:

"Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

(…)

b) dirigir a todo responsable o encargado del tratamiento un apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento; (…)"

Por su parte, el considerando 148 del RGPD indica:

"A fin de reforzar la aplicación de las normas del presente Reglamento, cualquier infracción de este debe ser castigada con sanciones, incluidas multas administrativas, con carácter adicional a medidas adecuadas impuestas por la autoridad de control en virtud del presente Reglamento, o en sustitución de estas. En caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento. Debe no obstante prestarse especial atención a la naturaleza, gravedad y duración de la infracción, a su carácter intencional, a las medidas tomadas para paliar los daños y perjuicios sufridos, al grado de responsabilidad o a cualquier infracción anterior pertinente, a la forma en que la autoridad de control haya tenido conocimiento de la infracción, al cumplimiento de medidas ordenadas contra el responsable o encargado, a la adhesión a códigos de conducta y a cualquier otra circunstancia agravante o atenuante. La imposición de sanciones, incluidas las multas administrativas, debe estar sujeta a garantías procesales suficientes conforme a los principios generales del Derecho de la Unión y de la Carta, entre ellas el derecho a la tutela judicial efectiva y a un proceso con todas las garantías."

Asimismo, el artículo 64 de la LOPDGDD que regula la "*Forma de iniciación del procedimiento y duración*", en su apartado tercero dispone que:

"3. Cuando así proceda en atención a la naturaleza de los hechos y teniendo debidamente en cuenta los criterios establecidos en el artículo 83.2 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, la Agencia Española de Protección de Datos, previa audiencia al responsable o encargado del tratamiento, podrá dirigir un apercibimiento, así como ordenar al responsable o encargado del tratamiento que adopten las medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos de una determinada manera y dentro del plazo especificado.

El procedimiento tendrá una duración máxima de seis meses a contar desde la fecha del acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones.

Será de aplicación en este caso lo dispuesto en los párrafos segundo y tercero del apartado 2 de este artículo."

De la redacción del mencionado precepto, se desprende que la consideración como leve de la infracción no depende de la calificación que realiza la propia ley, pues la misma, como indica el propio artículo, es únicamente a efectos del plazo de prescripción de la infracción. Por el contrario, para determinar el carácter leve de la misma resulta necesario acudir a los criterios que se contemplan en el artículo 83.2 del RGPD, entre los cuales se encuentran: la naturaleza, gravedad y duración de la infracción, la intencionalidad o negligencia, las medidas adoptadas para paliar los daños, el grado de responsabilidad o el grado de cooperación con la autoridad de control, entre otros.

En el presente caso, tal y como resultó de las actuaciones de investigación, si bien los datos contenidos en el dispositivo sustraído eran sensibles, dicho dispositivo se encuentra protegido con la contraseña y el patrón de acceso, lo que hace poco probable el acceso a los mencionados datos por personas ajenas. Asimismo, destaca la ausencia de intencionalidad por parte de la entidad infractora, pudiendo calificarse el nivel de negligencia como leve. Consta, además, que realizó de forma diligente la comunicación de la violación de la seguridad a los afectados al ampliar el número de destinatarios y aplicar un criterio amplio a la hora de determinar los posibles afectados"

Por las razones expuestas y aplicando los criterios indicados, se considera conforme a Derecho no imponer sanción consistente en multa administrativa y sustituirla por dirigir un apercibimiento a la entidad infractora; todo ello sin perjuicio de la adopción de medidas impuestas en la presente resolución en los términos expuestos seguidamente.

V
Medidas a adoptar

El artículo 58.2 d) del RGPD, permite a cada autoridad de control la posibilidad de "*ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado…".*

En el presente caso, se requiere al responsable para que en el plazo de tres meses notifique a esta Agencia la adopción de las siguientes medidas:

- Adoptar las medidas organizativas y técnicas adecuadas para adecuar garantizar un nivel de seguridad adecuado el riesgo y evitar, en la medida de lo posible, que pueda producirse una nueva violación de seguridad.

Se advierte que no atender la posible orden de adopción de medidas impuestas por este organismo en la resolución del presente procedimiento podrá 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 expuesto, 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: DIRIGIR UN APERCIBIMIENTO a ***POZO LIMPIO SL (LAOOAL VECINDARIO)***, con NIF ***B88318290***, por una infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD.

SEGUNDO: ORDENAR a ***POZO LIMPIO SL (LAOOAL VECINDARIO)***, con NIF ***B88318290***, que en virtud del artículo 58.2.d) del RGPD, en el plazo de tres meses, acredite haber procedido al cumplimiento de las siguientes medidas, comunicándolo a la presente autoridad en dicho plazo:

- Adoptar las medidas organizativas y técnicas adecuadas que resulten necesarias para adecuar garantizar un nivel de seguridad adecuado el riesgo y evitar, en la medida de lo posible, que pueda producirse una nueva violación de seguridad.

SEGUNDO: NOTIFICAR la presente resolución a ***POZO LIMPIO SL (LAOOAL VECINDARIO)***.

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.

1403-21112023

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