- **Expediente N.º: EXP202318720**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

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

HECHOS

PRIMERO: Con fecha 27 de octubre de 2023, se presentó reclamación con número de registro de entrada REGAGE23e00072680877 ante la Agencia Española de Protección de Datos contra ***INSTALFRICA CLIMATIZACIÓN, S.L.*** con NIF ***B73995771*** (en adelante, la parte reclamada).

Los motivos en que basa la reclamación son los siguientes:

El reclamante manifiesta haber sido víctima de un fraude tipo BEC (Business Email Compromised), por el que alguien presuntamente suplantó la identidad corporativa de la entidad reclamada, con la que tenía pendiente la realización de un pago vinculado a la prestación de un servicio.

El 9 de octubre de 2023 recibió un mensaje de correo electrónico remitido desde la dirección ******EMAIL.3*** en la que le informaba de un nuevo IBAN al que realizar la transferencia del pago. Afirma que ese mensaje pudo haber sido enviado por persona interna o por terceros que tuvieron acceso al buzón de correo señalado, y que de este modo estafaron al reclamante, que considera que sus datos personales no han sido protegidos.

Se aporta la siguiente documentación:

- Copia de la denuncia policial efectuada el día 16/10/2023 ante los Mossos d'Esquadra por los mismos hechos.
- Copia de los correos electrónicos de las comunicaciones mantenidas con el reclamado:Correo electrónico de fecha 28/9/2023 17:41 en el que figura como remitente la dirección de correo electrónico del reclamante (******EMAIL.1***) y como destinatario ******EMAIL.3*** y el contenido es relativo a una solicitud de presupuesto para la adquisición de productos.
- Correo electrónico de fecha 28/9/2023 18:08 enviado desde ******EMAIL.3*** a la cuenta de correo electrónico ******EMAIL.1*** informando de los precios solicitados.
- Correo electrónico de fecha 9/10/2023 11:59 remitido desde la cuenta de correo electrónico ******EMAIL.1*** a ******EMAIL.3*** solicitando factura para realizar el pago de los productos adquiridos.
- Correo electrónico de fecha 9/10/2023 11:34 remitido desde ******EMAIL.3*** al reclamante informando de que se adjunta factura y del número de cuenta bancaria en la que tiene que realizar el pago (CUENTA 1).
- Correo electrónico de fecha 9/10/2023 14:50 remitido desde ******EMAIL.3*** al reclamante informando del cambio del número de cuenta bancaria para realizar el pago del producto contratado (CUENTA 2) debido a problemas con la

anterior cuenta. Aporta las cabeceras de internet de este correo en las que consta que el correo ha sido enviado desde un servidor de correo denominado “mail.tuclimatizaciononline.es”.

- Correo electrónico de fecha 16/10/2023 enviado desde la cuenta de correo del reclamante a ***EMAIL.3*** y a ***EMAIL.2*** informando de la incidencia del cambio del número de cuenta y de que la cantidad ha sido abonada en la segunda cuenta indicada.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), el 27 de diciembre de 2023, se dio traslado de dicha reclamación a la parte reclamada, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, 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 recogido en fecha 5 de enero de 2024 como consta en el acuse de recibo que obra en el expediente.

No se ha recibido respuesta a este escrito de traslado.

TERCERO: Con fecha 27 de enero de 2024, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada.

CUARTO: 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 los siguientes extremos:

Con fecha 20/5/2024 la Subdirección General de Inspección de Datos solicita información y documentación al reclamado en relación con los hechos reclamados mediante notificación electrónica que resulta expirada, siendo reiterada el día 9/9/2024. Con fecha 23/9/2024 tiene entrada en la AEPD un escrito del representante de la entidad en respuesta al requerimiento de información.

Posteriormente, con fecha 3/10/2024 la Subdirección General de Inspección de Datos solicita información y documentación adicional al reclamado mediante notificación electrónica, sin que conste acceso o expiración de esta debido a una incidencia en el servicio de notificaciones electrónicas. Con fecha 25/10/2024 se remite nuevamente la solicitud de información mediante notificación electrónica, teniendo entrada en esta Agencia respuesta de la entidad con fecha 25/10/2024, en el que se aporta un escrito en el que se relaciona una serie de documentos que se aportan y una compilación de documentos sin texto explicativo de la descripción de su contenido.

Con fecha 5/11/2024 se solicita información y documentación adicional al reclamado sobre los procedimientos de gestión del correo electrónico, teniendo entrada escrito de respuesta el día 14/11/2024.

De los escritos de respuesta a los requerimientos de información de la Subdirección General de Inspección de Datos aportados por la parte reclamada, se desprende lo siguiente:

Respecto a la cronología de los hechos ocurridos:

En el mes de septiembre de 2023, el reclamante, les escribe desde su dirección de email al email corporativo ******EMAIL.3*** para interesarse sobre unos productos. En varios emails se indican las características de estos y solicita presupuesto de estos. El día 9 de octubre de 2023 a las 12:34 horas, le envían desde la dirección de email corporativa a su email el presupuesto solicitado, donde figuraba detallado los equipos, los importes, en el documento en formato pdf, el número de cuenta bancaria (CUENTA 1) y además en el mensaje del cuerpo del email hacen referencia al mismo número de cuenta bancaria (CUENTA 1). Hasta que el cliente no realiza el pago y facilita por email el justificante, no efectúan el pedido del material para iniciar el proceso compra.

No les consta haber enviado el correo informando del cambio de cuenta bancaria ni haber recibido posteriormente más comunicaciones desde el email del reclamante. Manifiestan que no son conscientes de las acciones realizadas por el reclamante hasta el día 11/10/2023, que tras llamada telefónica a uno de los empleados comerciales, les hace saber que ha realizado el pago del presupuesto. El empleado, consulta con el departamento de administración y le dice que el pago no ha sido recibido en la cuenta bancaria de la entidad.

Respecto a las causas que han hecho posible el incidente:

Manifiestan que el email corporativo ******EMAIL.3*** fue hackeado. Dicha intervención externa, provocó anular las comunicaciones de entrada y salida con el reclamante, para poder realizar los cambios en el IBAN de destino. Una vez que recibieron el dinero y pudieron operar con él, liberaron el email y las comunicaciones entre ambos, a partir del día 16.

Anteriormente no habían sido conscientes ni informados de ninguna acción similar y el email fue utilizado con otros clientes con total normalidad por ello no han sospechado irregularidades de la no entrada ni salida de emails. Tampoco se observó ningún tipo de señal en la que algún cliente pudiera haber tenido retrasos en el envío de presupuestos, confirmaciones de pedido, confirmaciones de entrega y documentos de facturas, etc. Este email sólo se utiliza en la empresa para estos procesos. Dentro del equipo el email ******EMAIL.3*** lo gestiona una sola persona, que, desde hace mucho tiempo en la empresa, sigue los procesos descritos en la gestión de la venta.

Respecto al número de personas afectadas por la violación de la seguridad de los datos personales:

El número de personas afectadas por la brecha es de e una (1), en concreto el reclamante.

Respecto a la categoría de los datos personales afectados:

En el email intervenido, figuraban los datos fiscales de la persona afectada (nombre y apellidos, nº dni, dirección completa), que son los datos obligatorios para poder emitir la factura de los productos solicitados.

Respecto a las posibles consecuencias para el afectado:

Las consecuencias para la persona afectada han sido económicas, ya que el objetivo de los hackers estaba centrado en derivar la cantidad económica del pago de la factura a otra cuenta bancaria.

Respecto a las acciones tomadas para solucionar el incidente y minimizar su impacto sobre las personas afectadas

En el momento en el que fueron conocedores de la situación, iniciaron comprobaciones del alcance que pudo tener en materia de protección de datos dicho incidente:

- Comprobación de la estructura informática de la empresa por los proveedores informáticos DIGITALIA SOLUCIONES INFORMÁTICAS SL.
- Conversaciones con el reclamante para poder adoptar una solución al incidente.
- Manifiestan que se realizó una auditoría por parte de la empresa Valegal España SL. Aportan copia del documento "*ANÁLISIS DE RIESGOS SEGÚN RGPD 206/679 Y LEY 3/2018 DE PROTECCIÓN DE DATOS Y GARANTÍAS Y DERECHOS DIGITALES"* de fecha 6/2/2024 elaborado por Valegal España S.L.U.

  El punto 1 del documento denominado "1.- INTRODUCCIÓN" hace referencia a Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en cuanto al tratamiento y la libre circulación de datos personales(RGPD) y su obligatorio deber de cumplimiento de los requerimientos y obligaciones para el responsable y el encargado de tratamiento que este incluye, entre las que destaca, la necesidad de llevar a cabo un análisis de riesgos con el fin de establecer medidas de seguridad y control para garantizar los derechos y libertades de las personas.

  El punto 2 de dicho documento denominado "2.- OBJETIVOS" se habla sobre el análisis de riesgos de protección de datos como herramienta que permite realizar una valoración objetiva de los riesgos inherentes a la actividad, así como los de la propia organización y sistemas de trabajo y decidir las medidas que se pueden utilizar para mitigarlos, pero no se define los objetivos perseguidos por el documento.

  Incluye el registro de actividades de tratamiento entre los que se incluye el tratamiento denominado "*Clientes y proveedores*" y se especifica la finalidad, legitimación, cesiones, periodo de conservación de datos, categoría de datos y derechos de protección de datos de los interesados.

  No se observa que el documento incluya identificación de los riesgos en los tratamientos de los datos.

  El documento incluye un punto denominado "Gestión del riesgo" en el que se describe información teórica sobre la evaluación y tratamiento de los riesgos. Incluye, además, el ciclo de vida de los datos en las operaciones de los tratamientos, incluido el tratamiento "*Clientes y proveedores*".

  El documento incluye un punto denominado "estructura informática" en el que se ha identificado los equipos y periféricos en la estructura informática de la entidad del que se desprende que la entidad cuenta con dos ordenadores de sobremesa

con SO Windows 10, contraseña alfanumérica de más de ocho (8) dígitos y con antivirus.

- Manifiestan que se han llevado a cabo medidas correctoras, sin especificar ni acreditar las mismas.

Respecto a las medidas de seguridad de los tratamientos de datos personales adoptadas con anterioridad al incidente

El reclamado aporta documentación de la que se desprende que es beneficiario del programa "Kit Digital", Convocatoria pública de ayudas de fecha 02 de agosto de 2022 del Ministerio de Asuntos Económicos y Transformación Digital, según la Orden ETD/1498/2021, de 29 de diciembre, por la que se prueban las bases reguladoras de la concesión de ayudas para la digitalización de pequeñas empresas, microempresas y personas en situación de autoempleo, en el marco de la Agenda España Digital 2025, el Plan de Digitalización PYMEs 2021-2025 y el Plan de Recuperación, Transformación y Resiliencia de España -Financiado por la Unión Europea- Next Generation EU.

De acuerdo con las bases de la convocatoria, el reclamado ha suscrito, en calidad de beneficiarios un Acuerdo de Prestación de Soluciones de Digitalización con Codisel 2012, S.L. en calidad de Agente Digitalizador Adherido, del que se desprende lo siguiente:

- Que el Beneficiario desea implantar la solución de digitalización COMUNICACIONES SEGURAS (en adelante, la "Solución"), con una serie de características y funcionalidades específicas determinadas que se detallarán a continuación que corresponden con la categoría Comunicaciones Seguras.

- La solución incluye: ***(…=***

Aportan copia de un documento denominado "MODELO COMPILACIÓN DE EVIDENCIAS 1ª FASE DE JUSTIFICACIÓN" que incluye capturas de pantallas acreditativas de situación de la solución de digitalización COMUNICACIONES SEGURAS de la herramienta ******HERRAMIENTA.1 (…)***, de las que se desprende lo siguiente:

- Aportan captura de pantalla de la consola general en la que se observa que el usuario es Instalftica climatización SL. y que están registrados 9 usuarios con nombre y apellidos y nombre de usuario.

- Aportan captura de pantalla del panel de control la licencia suministrada asociada al cliente, de la que se desprende que la entidad está suscrita al producto Firewall base, con fecha de expiración 31/12/2999 y cuenta con los productos: "protección de correo electrónico", "Protección de redes", "Protección web", "protección de día cero" y "protección de servidores web", todos ellos con fecha de expiración 9/3/2024 (un año desde la contratación).

- Aportan captura de pantalla de la que se deprende que las conexiones web son conexiones seguras SSL.

- Aportan captura de control de ******HERRAMIENTA.2 con ***HERRAMIENTA.1*** desde varios tipos de dispositivos, donde se solicita nombre de usuario, contraseña y verificación.

- Aportan captura de pantalla en la que costa la contratación de las licencias de Microsoft 365 básico y estándar.

Respecto a si la violación de seguridad ha sido notificada a la Autoridad de Control

Manifiestan que no se notificó a la AEPD, ya que no existió ningún tipo de violación de seguridad en materia de protección de datos de carácter personal, salvo el incidente bancario por el que se solicita la información.

Respecto de las medidas previstas para que no se vuelva a producir un incidente similar en el futuro

Manifiestan que la empresa ha realizado una adaptación, con una empresa externa, a la normativa vigente en materia de protección de datos personal según el RGPD Y LOPDGDD 3/2018. Aportan copia del certificado emitido por VALEGAL ESPAÑA SL, empresa especializada en consultoría de protección de datos y E-commerce, en el que CERTIFICA, "*que durante la vigencia del presente certificado, la entidad: INSTALFRICA CLIMATIZACIÓN S.L. CIF: B73995771, Implantó las medidas de seguridad técnicas y organizativas necesarias para garantizar la seguridad de los datos de carácter personal que almacena en sus sistemas de información, de acuerdo con lo dispuesto por el NRGPD 2016/679 y LEY ORGÁNICA 03/2018, de Protección de Datos de Carácter Personal y Garantías y Derechos Digitales LOPDGDD. Se compromete a cumplir con lo dispuesto por la normativa sobre protección de datos anteriormente mencionada, así como a hacer cumplir las medidas de seguridad técnicas y organizativas implantadas al personal a su servicio que trate datos de carácter personal, evitando de esta forma, la pérdida, alteración y acceso no autorizado a los mismos. Dicho personal se halla sujeto al deber de secreto y confidencialidad respecto a los datos que trata en los mismos términos que la entidad."* Consta en el certificado como fecha de vigencia hasta el 6 de febrero de 2025.

La empresa ha registrado y designado a un DPD externo para llevar el control y prevenir situaciones como las reflejadas en este caso y poder controlar de una forma profesional todo lo relacionado con la protección de datos de carácter personal. Aportan copia del documento de alta de la Subdirección General de Promoción y Autorizaciones de la AEPD de fecha 17/9/2024.

La empresa ha impartido formación en materia de Lopdgdd y Ciberseguridad a sus empleados/as para poder ser conocedores de las medidas de seguridad aportadas, las tendencias en ciberataques actuales y las acciones a desarrollar en el caso de que se produzca un incidente de seguridad de la información en la empresa, independientemente del nivel que sea.

Aportan copia del certificado emitido por VALEGAL ESPAÑA SL, Consultoría externa especializada en Protección de Datos, Seguridad de la Información y E-commerce, con fecha 6 /2/2024, en el que consta que la empresa INSTALFRICA CLIMATIZACIÓN S.L. ha realizado con éxito la formación en materia de PROTECCION DE DATOS, LEY DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN (LEY 3/2018 Y LEY 34/2002) Y CIBERSEGURIDAD, según el siguiente detalle:

Número de horas: 4.

Número de asistentes: 3.

Índice del contenido:

- Informe de Registro de Actividades del Tratamiento
- Redacción de Documento de Seguridad
- Redacción de Manuales de Confidencialidad, Uso de Dispositivos Digitales y Desconexión Digital para empleados/as.
- Redacción de Cláusulas de Seguridad informativas
- Adaptación online de web según Lssice Ley 34/2002
- Introducción al concepto de transformación digital.
- Entornos digitales seguros.
- Análisis de eficiencia en los procesos de comunicación y producción de la organización.
- Gestión de riesgo.
- Ciberseguridad y Hacking Ético.
- Herramientas Digitales.
- Políticas de compliance IT.

La empresa ha contratado los servicios de una empresa de Ciberseguridad para monitorizar cualquier acción de seguridad de la información, trabajar de forma continua y coordinada con la empresa y dar una pronta respuesta ante cualquier indicio de violación de seguridad, aportando para ello medidas de seguridad escalables y programadas en el tiempo.

Aportan "*Copia del contrato de ET y documentos de facturas con la empresa que gestiona el* correo *electrónico, servidores, web, etc.*" de encargado del tratamiento suscrito con DIGITALIA SOLUCIONES INFORMÁTICAS S.L. de fecha 6/2/2024, para la prestación de Servicios Informáticos y Ciberseguridad, de cuyo contenido se desprende lo siguiente:

- El objeto del contrato es regular el tratamiento de determinados datos personales del RESPONSANBLE DEL TRATAMIENTO, por el ENCARGADO DEL TRATAMIENTO, con motivo de la relación de prestación de servicios que vincula a ambas partes, dando cumplimiento a las obligaciones establecidas en el artículo 28 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), y en la normativa española de protección de datos de carácter personal.
- El ENCARGADO DEL TRATAMIENTO tratará por cuenta del RESPONSABLE DEL TRATAMIENTO los datos personales necesarios para la prestación de servicios derivada de la relación que vincula a ambas partes, de conformidad con las instrucciones documentadas en el ANEXO I al contrato.
- El ENCARGADO DEL TRATAMIENTO tratará por cuenta del RESPONSABLE DEL TRATAMIENTO la información sobre personas físicas identificadas o identificables documentada en el ANEXO II al contrato.

- Incluye las OBLIGACIONES DEL ENCARGADO DEL TRATAMIENTO, entre las que se encuentran, entre otras: tratar los datos de acuerdo con las instrucciones del responsable del tratamiento, deber de información, deber de confidencialidad, subcontrataciones, atención a los derechos de protección de datos personales.

- Descripción de la forma de prestación del servicio: El servicio será prestado en los locales del RESPONSABLE DEL TRATAMIENTO, que facilitará al ENCARGADO DEL TRATAMIENTO el acceso a sus sistemas. El servicio será prestado a través de acceso remoto, prohibiéndose expresamente al ENCARGADO DEL TRATAMIENTO incorporar los datos objeto de tratamiento a sistemas o soportes distintos de los del RESPONSABLE DEL TRATAMIENTO. El servicio será prestado por el ENCARGADO DEL TRATAMIENTO en sus propios locales y con sus sistemas, ajenos a los del RESPONSABLE DEL TRATAMIENTO.

- El contrato incluye como ANEXO III las Medidas de seguridad que debe implementar el encargado del tratamiento, entre las que se incluye:

  - Adecuación al Esquema Nacional de Seguridad (ENS) (AA.PP.)
  - Sistema de identificación y autenticación de usuarios.
  - Sistema de gestión de privilegios de acceso.
  - Cortafuegos (Firewall)
  - Sistema de análisis y gestión de vulnerabilidades y amenazas / Sistema de protección contra código malicioso y descargable (vgr. antivirus)
  - Servidor propio X Certificado SSL en página web (protocolo HTTPS)

<u>Respecto a la gestión del correo electrónico</u>

Con anterioridad al incidente la entidad había adoptado Microsoft 365 como proveedor de correo electrónico. Este sistema cuenta con herramientas avanzadas de protección contra ataques de phishing y autenticación multifactor (MFA), la cual, manifiestan, que se exige a todos los usuarios con acceso a cuentas corporativas.

Procedimiento de alta y baja de usuarios: La creación de cuentas de correo electrónico se realiza exclusivamente por el administrador de sistemas autorizado, quien también es responsable de la gestión de usuarios, que es el gerente de la empresa. El alta de usuarios se lleva a cabo tras una solicitud formal de la dirección a la empresa externa que gestiona el servicio DIGITALIA, verificando que cada cuenta esté asignada a un trabajador/a específico. Al recibir la solicitud, el administrador crea la cuenta y envía los datos de acceso de forma segura mediante whatsapp, correo seguro y llamada telefónica. Se realiza esté proceso de 3 pasos para la verificación de la recepción y custodia de las mismas. Una vez que están verificados los tres pasos, la información enviada a través de la plataforma whatsapp, se elimina completamente para no dejar ningún rastro de la información. En el caso de las bajas, aunque no se ha procedido todavía a ninguna de ellas, está definido el mismo proceso, pero únicamente entre gerencia y la empresa que gestiona el servicio DIGITALIA, siempre tras petición por escrito.

Control de acceso, identificación y autenticación: Cada usuario debe iniciar sesión con un identificador único y contraseña personalizada. La autenticación de dos factores

(2FA) es obligatoria para todos los usuarios para añadir una capa adicional de seguridad. Las contraseñas se renuevan periódicamente, y se les exige a los usuarios cambiarlas en el primer acceso. Asimismo, estas cumplen criterios de complejidad (mínimo de caracteres, combinación de letras y números) para minimizar vulnerabilidades. Se utiliza un gestor de contraseñas para el control de las mismas y además un formulario en papel que incluye el documento de seguridad de Lopdgdd.

Asignación de contraseñas y política de renovación periódica: La asignación de contraseñas está regulada y los usuarios reciben instrucciones detalladas para su creación y cambio, así como pautas de seguridad. Las contraseñas son configuradas por diseño propio cumplimiento como se ha indicado anteriormente los criterios de complejidad idóneos. Se ha establecido un calendario para el cambio de las mismas. Dicho calendario, avisará mediante recordatorio a la gerencia de la necesidad del cambio de las mismas y se procederá a comunicar a cada usuario la gestión. Una vez que se produzca se actuará modificándolo en los gestores y documentos físicos de control.

Política de cancelación de cuentas de correo electrónico: La baja de cuentas de correo de usuarios (por cambio de funciones o baja en la plantilla) se ejecuta inmediatamente tras la notificación del responsable de recursos humanos a gerencia y desde gerencia a la empresa prestadora del servicio DIGITALIA, utilizando los canales habituales de comunicación con ellos. Este procedimiento incluye la desactivación y eliminación de la cuenta tras una revisión de la información contenida. En los casos de cuentas compartidas, se reestablecen las credenciales y se revisan los accesos asignados.

La cuenta de correo electrónico ***EMAIL.3 está gestionada exclusivamente por un número restringido de usuarios previamente identificados en documento interno.

En la actualidad hay tres (3) personas, el gerente y dos empleados/as con acceso a dicha cuenta, con diferente atribución y permisos en la misma.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) confiere a cada autoridad de control y según lo dispuesto en los artículos 47 y 48.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Presidencia 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

Cuestiones previas

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 la parte reclamada realiza, entre otros tratamientos, la recogida y registro de los siguientes datos personales de personas físicas, tales como: nombre, número de identificación, dirección de correo electrónico.

La parte reclamada 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 citado artículo 4.7 del RGPD.

El artículo 4 apartado 12 del RGPD define, de un modo amplio, las *"violaciones de seguridad de los datos personales" (en adelante brecha de seguridad)* como *"todas aquellas violaciones de la seguridad que ocasionen 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."*

Hay que señalar que la identificación de una brecha de seguridad no implica la imposición de una sanción de forma directa por esta Agencia, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

III

Principios relativos al tratamiento

El artículo 5.1.f) "*Principios relativos al tratamiento*" del RGPD establece:

"1. Los datos personales serán:
(…)

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)."

En el presente caso, consta que los datos personales de los afectados, obrantes en la base de datos de la parte reclamada, fueron indebidamente expuestos a un tercero.

No obstante, cabe recordar que la mera identificación de una brecha de seguridad por parte de esta Agencia no implica la comisión de una infracción en materia de protección de datos, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

Tal como se ha expuesto anteriormente, de los hechos que se deducen del expediente administrativo, no se desprende que, con anterioridad a la brecha de seguridad, la parte reclamada/alias, careciera de medidas de seguridad razonables en función de los posibles riesgos estimados ni que no se hubiera actuado de forma diligente una

vez conocida la brecha de seguridad, ni que las medidas adoptadas con posterioridad al incidente aquí analizado no fueran adecuadas.

Al respecto, el artículo 28 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público dispone que: "*Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, (…) que resulten responsables de los mismos a título de dolo o culpa*".

En el presente caso, no ha quedado acreditado que la parte reclamada hubiera actuado de forma negligente ni, mucho menos, con dolo por su parte, por tanto, no cabe entender que se hubiera producido una infracción del artículo 5.1.f) RGPD.

IV
Conclusión

En el presente expediente, la parte reclamante manifiesta haber sido víctima de un fraude de tipo *Business Email Compromise* (BEC), mediante el cual, presuntamente, terceros suplantaron la identidad corporativa de la entidad reclamada, desviando el pago de un pedido a una cuenta bancaria fraudulenta tras manipular la comunicación por correo electrónico.

A lo largo de la investigación se ha verificado que la entidad reclamada sufrió un acceso ilícito a su cuenta de correo electrónico corporativa, lo que permitió la manipulación de los mensajes intercambiados con el reclamante. No obstante, de las actuaciones realizadas no se desprende que el acceso se debiera a una negligencia o incumplimiento directo de la normativa de protección de datos personales por parte de la entidad reclamada, la cual disponía previamente de medidas técnicas y organizativas implementadas, tales como autenticación multifactor, políticas de contraseñas, protocolos de gestión de usuarios, contratación de servicios de ciberseguridad, así como procedimientos definidos de alta, baja y control de accesos a sus cuentas de correo.

Asimismo, la entidad reclamada ha acreditado haber adoptado medidas adicionales tras el incidente, revisando su estructura de seguridad, ampliando sus controles de ciberseguridad y reforzando la formación interna en materia de protección de datos y ciberseguridad.

En este contexto, no se ha constatado que existiera una vulneración previa de los principios previstos en el artículo 5 del RGPD imputable a una deficiente actuación de la entidad, tratándose en este caso de un acceso ilegítimo externo no atribuible a un incumplimiento de sus obligaciones como responsable del tratamiento. En consecuencia, y al no acreditarse infracción de la normativa de protección de datos, procede el archivo de las actuaciones.

Todo ello sin perjuicio de las posibles actuaciones posteriores que esta Agencia pudiera llevar a cabo, aplicando los poderes de investigación y correctivos que ostenta.

Así pues, al no haber sido posible atribuir la responsabilidad por el tratamiento de acuerdo con lo señalado, por la Presidencia de la Agencia Española de Protección de Datos, SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a ***INSTALFRICA CLIMATIZACIÓN, S.L.*** y a la parte reclamante.

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

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

1245-240125

Lorenzo Cotino Hueso
Presidente de la Agencia Española de Protección de Datos