- **Expediente N.º: EXP202301218**

RESOLUCIÓN DE PROCEDIMIENTO DE APERCIBIMIENTO

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

ANTECEDENTES

PRIMERO: Con fecha 30 de enero de 2023, la Subdirección General de Inspección de Datos (SGID) recibió para su valoración un escrito de notificación de brecha de seguridad de los datos personales remitido por ***A.A.A..*** con NIF ******NIF.1*** (en adelante, CDIS S.L.), recibido en fecha 20/01/2023, en el que informa a la Agencia Española de Protección de Datos de lo siguiente:

El escrito ponía en conocimiento de la presente autoridad el hecho de que una trabajadora del propio centro, por error, entregó un informe de seguimiento al padre de un paciente menor de edad donde figuraban datos parciales relativos a la dirección del domicilio de la madre, así como de su teléfono y dirección de correcto electrónico. Afirma que se trataba de una pareja separada legalmente en la cual existía la necesidad de no desvelar el domicilio actual de la madre.

En virtud de tales hechos, con fecha 24/01/2023, la Directora de la presente autoridad firmó resolución ordenando al responsable la comunicación de la brecha a los afectados, recibiendo en fecha 27/01/2023, por parte de dicho responsable, justificante de la comunicación de la brecha a la afectada, la cual es madre y representante legal del menor. En la citada comunicación se le informaba a la persona afectada el hecho consistente en la entrega al padre, por parte de una empleada y de forma accidental, del informe de seguimiento del menor y en el cual constaban datos parciales de su dirección y de contacto (teléfono y mail). Consta firmada la recepción de la comunicación por la afectada.

SEGUNDO: Como consecuencia de la notificación a la División de Innovación Tecnológica de esta Agencia de una brecha de seguridad relativa a la entrega de un informe con datos de un menor, se ordena a la Subdirección General de Inspección de Datos que valore la necesidad de realizar las oportunas investigaciones previas.

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 extremos que seguidamente se exponen.

En la información que figura en ASEXOR, CDIS S.L es una sociedad limitada de tipo "Autónoma" y consta como "*Actividades de cuidado diurno de niños*" con el objeto

social de *"Intermediación en la prestación de servicios integrales de asistencia social mediante personal cualificado"*

En la web de dicha empresa consta que son un equipo de profesionales "*para apoyar el desarrollo integral de los niños y niñas de nuestra comunidad*".

Con fecha 17/02/2023 se solicitó información y documentación a CDIS S.L no obteniéndose respuesta, reiterándose con fecha 26/04/2023, recibiendo respuesta de la entidad de la cual se manifestaba lo siguiente:

Respecto a la respuesta frente a la brecha:

- El 30 de diciembre de 2022 fue la fecha en la que la trabajadora de CDIS S.L hizo entrega del informe de seguimiento donde constaba el teléfono de contacto y la dirección parcial de su madre y representante legal.
- El 20 de enero de 2023, fecha en la que se personó el menor para seguir su tratamiento, la trabajadora tuvo conocimiento de que el último informe de diciembre entregado al padre constaban los datos de la madre. Ese mismo día se presentó la notificación de la brecha a la Agencia Española de Protección de Datos.
- Al día siguiente, 21 de enero del mismo año, se contactó telefónicamente con la afectada para informarle de los hechos procediendo el 26 de enero, fecha de la cita para el tratamiento del menor, a hacer entrega de un escrito donde se informaba formalmente de lo sucedido. A tal respecto, se aporta copia del mencionado escrito, de fecha 26/01/2023 en el que se informa la entrega de un informe a su exmarido donde constan sus datos de domicilio de forma parcial, teléfono y dirección e-mail, el cual consta firmado por la afectada.
- Asimismo, comunican la apertura de un expediente disciplinario a la trabajadora con fecha 25 de enero, en virtud de los hechos acaecidos.

Respecto de los datos afectados:

- Se afirma que en el informe entregado constaban los datos de domicilio sin especificar la población, el teléfono de contacto y el mail de la afectada.
- Se indica que la afectada les ha manifestado que su exmarido ya conocía su domicilio con anterioridad a los hechos acaecidos. Asimismo, manifiestan que la afectada no ha sufrido ninguna incidencia por el error cometido y que, en consecuencia, no se han utilizado por terceros los datos obtenidos a través de la brecha.

En relación a la finalidad del tratamiento de datos.

- Se aportó escrito firmado por la madre del paciente donde se le informa del tratamiento de los datos y la finalidad de los mismos. En este mismo documento se informa de los derechos de los afectados y de la posibilidad de interponer reclamaciones ante la Agencia Española de Protección de Datos.
- Se aporta consentimiento sobre el tratamiento y almacenamiento de los datos en un fichero de Historia Clínica firmado por la madre del paciente con la finalidad de detectar de forma precoz la aparición de cualquier alteración en el desarrollo o riesgo de padecerlo***,*** *así como recoger información necesaria para el diseño de mapa de recursos necesarios para atender a la población a la que va dirigida.*

Respecto a las medidas de seguridad implantadas, se aporta como anexo las siguientes:

- En relación con el puesto de trabajo:
  - Ubicación en lugares que garantizan la confidencialidad
  - Protector de pantalla que impide visualización y se desactiva con contraseña.
  - Configuración fija en los puestos y solo es modificable con autorización del DPD.
  - Correo electrónico puede ser revisado por el Centro.
  - Acceso a internet solo para las aplicaciones Alborada (Responsabilidad de la Junta de Andalucía) y a Dasi Clinic (Responsabilidad del Centro).
- Entre las prohibiciones a los usuarios:
  - Enviar mensajes con fines comerciales
  - Instalar copias ilegales de cualquier programa
  - Compartir las credenciales de usuarios.
- Dispositivos de seguridad:
  - Antivirus, Firewall
  - Control de acceso a las páginas web.
  - Acceso a los locales con llave y solo personal autorizado por el DPD. A este respecto se ha adjuntado creación del Registro General de Accesos Físicos) en el que consta el nombre de las personas autorizadas con llave de las instalaciones, la fecha de entrega de las llaves, el número de copias existentes con la asignación de un código a cada una de ellas y las posibles incidencias detectadas en relación con el uso de las mismas.
  - Acceso a aplicaciones con código usuario y contraseña cifrada.
  - Gestión de usuarios y gestión de contraseñas. Como anexo 4 han aportado documento de “uso de contraseñas y accesos físicos, dispositivos digitales, internet e imagen” firmado por la mencionada trabajadora.
  - Salidas de soporte con datos personales únicamente con autorización y manteniendo las medidas de seguridad.
  - Copias de seguridad diarias y mensual.
  - No se permiten soportes USB, CD…
  - Acuerdo de Confidencialidad. Se ha aportado como Anexo 3 copia del acuerdo de confidencialidad suscrito por la trabajadora de fecha 19 de septiembre de 2022.

Asimismo, manifiesta que todos los trabajadores reciben formación periódica conforme a las obligaciones derivadas del tratamiento de datos de carácter personal. Con relación a estas manifestaciones se aporta listado de formación en el RGPD y LOPDGDD de fecha 16/09/2022. Entre ellos se encuentra la trabajadora que hizo

entrega del informe. De la misma forma, se aportan formularios disponibles en el Centro para el ejercicio de los derechos.

Por último, se manifiesta que tanto para el acceso a la plataforma Alborada (Responsabilidad de la Junta de Andalucía) y a Dasi Clinic (Responsabilidad del Centro), donde se almacenan todos los informes de los pacientes, se solicita credenciales (usuario y contraseña) los cuales son personales de cada empleado. Indica que al acceder a la historia del paciente, el sistema visualiza la última información, a quién se le hizo entrega y en qué fecha. Fue en dicho momento en el que la trabajadora puso en conocimiento de los responsables del centro lo que entendía había sido un error por su parte.

En relación a la posible concurrencia de eventos análogos acontecidos en el tiempo, afirmaron que no se ha producido hasta la fecha una situación similar.

CUARTO: Con fecha 12 de diciembre de 2023, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento de apercibimiento a la parte reclamada, por las presuntas infracciones del artículo 5.1.f) del RGPD y del artículo 32 RGPD, tipificadas en los artículos 83.5 y 83.4 del RGPD respectivamente.

QUINTO: 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.

SEXTO: En fecha 20 de diciembre de 2023 se recibe escrito de alegaciones de CDIS S.L en el que, en síntesis, se recogen las siguientes consideraciones:

1º. Que, desde el inicio de su actividad, ha tenido como objetivo primordial cumplir de manera escrupulosa con los requisitos establecidos por la normativa de Protección de Datos. Inicialmente, se rigió bajo la Ley 15/1999 de Protección de Datos de Carácter Personal, y a partir de 2018, se adaptó al Reglamento Europeo de Protección de Datos (RGPD) R.UE 2016/679 y a la Ley 3/2018 de Protección de Datos y garantías de los derechos digitales (LOPDGDD 3/2018).

2º. Que, debido a la naturaleza de la actividad desarrollada, se tiene muy claro la importancia de garantizar la seguridad, integridad, confidencialidad y correcto uso de la información tratada. Esto se refleja en todas las medidas de seguridad implementadas, tal como se justifica en la comunicación de la brecha de seguridad.

3º. Que, tras la situación descrita en la brecha de seguridad, y en atención a la responsabilidad proactiva, así como a una nueva evaluación de riesgos, en su calidad de responsable del tratamiento, y después de consultar con la Consejería de Salud y Consumo de la Junta de Andalucía decidió eliminar cualquier información relacionada con teléfono, dirección postal y correo electrónico de todos los informes generados para su entrega a los interesados (se adjunta modelo junto al mencionado escrito). Considera esta medida adecuada y proporcionada para evitar que se repita la situación comunicada, incluido el error humano.

En base a lo expuesto, la parte reclamada solicita que se proceda al archivo de actuaciones en el plazo previsto.

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: El 30 de diciembre de 2022, una trabajadora de CDIS S.L entregó al padre de un paciente menor de edad un informe de seguimiento que contenía datos parciales relativos a la dirección del domicilio, teléfono y correo electrónico de la madre, representante legal del menor. La madre y el padre del menor están separados legalmente y existía la necesidad de no comunicar el domicilio actual de la madre al padre.

Estos hechos se desprenden de la notificación de dicha brecha de datos personales que realizó CDIS S.L. a la Subdirección General de Inspección de Datos (SGID) de la presente autoridad el 20 de enero de 2023.

SEGUNDO: El día 26 enero de 2023 CDIS S.L comunicó la mencionada brecha de datos personales a la persona afectada, madre y representante legal del menor, informándole de la entrega accidental del informe de seguimiento al padre, que contenía datos parciales de su dirección, teléfono y correo electrónico.

Este hecho queda acreditado a través del justificante de dicha comunicación aportada por CDIS S.L a esta autoridad el 27 de enero de 2023 y en el cual consta firmada la recepción de la misma por la afectada.

TERCERO**:** De las actuaciones de investigación y los documentos aportados por CDIS S.L ha quedado constatada, posteriormente al acaecimiento de la brecha, la implementación por parte de dicha entidad de medidas reactivas con el fin de proteger los datos personales de las personas cuyos datos van a ser tratados.

CUARTO Tal y como consta en la información que figura en ASEXOR, la empresa CDIS S.L. es una sociedad limitada dedicada a las “Actividades de cuidado diurno de niños” con el objeto social de “Intermediación en la prestación de servicios integrales de asistencia social mediante personal cualificado”.

II

FUNDAMENTOS DE DERECHO

I

Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante 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."*
[Introduzca el texto correspondiente a [Texto fundamento I régimen aplicable].]

II
Vulneración del artículo 5.1.f) del RGPD

El artículo 5 del RGPD establece los principios relativos al tratamiento, indicando, entre otras cuestiones, que 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»)."

De la misma forma, el Considerado 39 RGPD dispone que: "*Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento."*

El principio de confidencialidad, según el mencionado artículo 5.1 f) del RGPD, exige la protección de datos personales contra accesos, usos y divulgaciones no autorizados. Dicho principio resulta esencial para garantizar la seguridad de los datos personales, constituyendo un pilar clave en la protección de la privacidad y los derechos individuales en dicho ámbito. Por el contrario, la violación de este principio puede tener consecuencias no deseadas, reflejando su importancia en el marco normativo de la protección de datos.

En el presente supuesto, en los términos expuestos en el HECHO PROBADO PRIMERO, la entrega accidental de determinados personales de la madre y representante legal de un paciente, como la dirección parcial, el número de teléfono y el correo electrónico a una parte no autorizada (en este caso, el padre del menor) manifiesta una vulneración del citado principio.

En primer lugar, conviene indicar que el artículo 4 define como datos personales "*a 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."*

En este contexto, la manifestación realizada por la entidad de que la indebida entrega fue consecuencia de una negligencia de una trabajadora no exime de su presunta responsabilidad ante tales hechos. Debe de recordarse que, en virtud del principio de responsabilidad proactiva reconocido en el propio artículo 5, el responsable del tratamiento es responsable del cumplimiento de los principios enunciados en el citado artículo, así como capaz de demostrarlo. Por tanto, garantizar los principios de protección de los datos personales y asegurar su correcto tratamiento recae en el responsable del tratamiento.

En el presente supuesto, no es posible ignorar el potencial impacto que puede tener una divulgación no autorizada de información personal. Asimismo, la divulgación de datos adicionales, como el correo electrónico o el número de teléfono, aumenta el riesgo de posibles usos indebidos de dichos datos en un futuro.

Por otro lado, la existencia de la necesidad de no comunicar al padre del menor información personal de la madre, como queda acreditado en el HECHO PROBADO PRIMERO, es un factor clave a tener en cuenta en el presente caso. La relevancia de dicho hecho se encuentra en la obligación que posee el responsable del tratamiento de respetar las preferencias de aquellas personas respecto a aquellos datos personales que van a ser objeto de tratamiento. En el caso que nos ocupa, la entrega de determinada información personal de la madre al padre, a pesar de la existencia de la necesidad de no hacerlo, implica una manifestación de la vulneración del mencionado principio de confidencialidad, lo que conlleva una infracción en los términos indicados más abajo.

Por último, la alegación por CDIS S.L consistente en el hecho de haber comunicado la brecha de seguridad tanto a la autoridad como a la afectada, no exime tampoco de la responsabilidad de haber infringido el principio de confidencialidad. Debe de recordarse que dichas comunicaciones no son potestativas, sino que resultan de obligado cumplimiento por el RGPD. La notificación de dicho incidente, aunque demuestra un cumplimiento reactivo de dicha norma, no puede eliminar la responsabilidad inherente por no haber evitado la exposición de los datos personales afectados desde un principio. En consecuencia, la entidad que comunica la brecha sigue siendo responsable de la infracción del principio de confidencialidad y debe afrontar las consecuencias legales y administrativas correspondientes.

III
Tipificación y calificación de la infracción del artículo 5.1.f) del RGPD

El incumplimiento del artículo 5.1.f) del RGPD como principio básico del tratamiento supone la comisión de las infracciones tipificadas en el artículo 83.5 del RGPD que bajo la rúbrica “Condiciones generales para la imposición de multas administrativas” dispone:

“Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, 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:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9; (…)"

A este respecto, la LOPDGDD, en su artículo 71 "Infracciones" establece que *"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, el artículo 72 "Infracciones consideradas muy graves" de la LOPDGDD indica:

"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:

a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679. (…)"

IV
Incumplimiento del artículo 32 del RGPD

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

"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".

Resulta necesario señalar que el citado precepto no establece un listado de medidas de seguridad concretas de acuerdo con los datos objeto de tratamiento, sino que establece la obligación de que el responsable y el encargado del tratamiento apliquen medidas técnicas y organizativas que sean adecuadas al riesgo que conlleve el tratamiento, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, alcance, contexto y finalidades del tratamiento, los riesgos de probabilidad y gravedad para los derechos y libertades de las personas interesadas.

Asimismo, las medidas de seguridad deben resultar adecuadas y proporcionadas al riesgo detectado, determinando aquellas medidas técnicas y organizativas adecuadas teniendo en cuenta la seudonimización y el cifrado, la capacidad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia, la capacidad para restaurar la disponibilidad y acceso a datos tras un incidente, proceso de verificación (que no auditoría), evaluación y valoración de la eficacia de las medidas.

En todo caso, al evaluar la adecuación del nivel de seguridad se debe tener particularmente en cuenta los riesgos que presente el tratamiento de datos, 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 y que pudieran ocasionar daños y perjuicios físicos, materiales o inmateriales.

Por su parte, el considerando 83 del RGPD señala *que "(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como 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, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales".*

En el presente supuesto, el incumplimiento del contenido del citado artículo 32 del RGPD se fundamenta en un análisis detallado de las circunstancias que rodean el incidente de la brecha de datos producida. En este sentido, como se deduce del propio artículo, la normativa vigente requiere que las entidades encargadas del tratamiento de datos personales apliquen medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

Conviene mencionar que el incumplimiento de dichas obligaciones en este caso no es consecuencia de la brecha comunicada por la entidad, sino que la misma supone un indicio o manifestación de no haber evaluado adecuadamente los riesgos asociados con el tratamiento de datos o implementado medidas de seguridad acordes con estos riesgos.

Ello es particularmente relevante en el presente supuesto dado que, teniendo en cuenta el objeto social de CDIS S.L, indicando en el HECHO PROBADO CUARTO, el tratamiento puede afectar a datos de menores. Como resulta lógico, la naturaleza sensible de tales datos requiere un mayor nivel de protección debido a los riesgos potencialmente mayores para los derechos de este colectivo más vulnerable.

La alegación presentada por CDIS S.L. consistente en que, tras la situación descrita en la brecha de seguridad, se decidió eliminar cualquier información relacionada con teléfono, dirección postal y correo electrónico de todos los informes generados para su entrega a los interesados, manifiesta de hecho la citada vulneración del artículo 32 del RGPD. Este artículo exige que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo de una forma previa y continua. Por el contrario, las medidas señaladas se adoptaron de forma reactiva tras la brecha de seguridad y no con anterioridad a la misma, lo que evidencia que las medidas preventivas iniciales fueron insuficientes para proteger adecuadamente los datos personales y cumplir el mandato del artículo infringido.

De igual forma, las medidas de seguridad deben ser especialmente rigurosas y revisadas en entornos donde se tratan datos sensibles como en ocurre en el caso de menores, con el fin de asegurar su confidencialidad, así como su integridad y disponibilidad. La entidad no debe solo implementar medidas de seguridad, sino también asegurarse de que estas medidas se mantengan efectivas ante los distintos riesgos en el tratamiento de datos personales, incluidos un posible error o negligencia humana, especialmente cuando dichos datos son sensibles.

En conclusión, la imputación de la infracción se sustenta en una inadecuación e ineficacia de las medidas de seguridad implementadas lo que conlleva el incumplimiento del artículo 32 del RGPD.

V
Tipificación y calificación de la infracción del artículo 32 del RGPD

De confirmarse, la citada infracción del artículo 32 del RGPD podría suponer la comisión de las infracciones tipificadas en el artículo 83.4 del RGPD que bajo la rúbrica “Condiciones generales para la imposición de multas administrativas” dispone: “*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 este respecto, la LOPDGDD, en su artículo 71 "Infracciones" establece que *"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, el artículo 73 "Infracciones consideradas graves" de la LOPDGDD indica: "*En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:*

(…) 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.

VI

Apercibimiento

Sin perjuicio de lo dispuesto en el apartado 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; (…)"*

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."

En el presente caso, siguiendo los criterios del mencionado artículo y teniendo en cuenta la ausencia de efectos directos negativos para la persona afectada por la brecha tal y como resulta de los hechos probados, se estima que por la presunta infracción de los mencionados artículos procede **dirigir un apercibimiento.**

VII
Adopción de medidas

Procede, asimismo, imponer al responsable la adopción de medidas adecuadas para ajustar su actuación a la normativa mencionada en este acto, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá "*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 técnicas y de seguridad adecuadas al riesgo con el fin de evitar cualquier tipo de quiebra de seguridad, incluidas aquellas derivadas de error o negligencia humana.

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 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: DIRIGIR UN APERCIBIMIENTO a ***A.A.A.***, con NIF ******NIF.1***, por la comisión de las infracciones del artículo 5.1.f) del RGPD y del artículo 32 RGPD, tipificadas en los artículos 83.5 y 83.4 del RGPD respectivamente

SEGUNDO: ORDENAR a ***A.A.A.***, con NIF ******NIF.1***, que en virtud del artículo 58.2.d) del RGPD, en el plazo de 3 meses desde que la presente resolución sea firme y ejecutiva, acredite haber procedido al cumplimiento de las siguientes medidas:

- Adoptar las medidas técnicas y de seguridad adecuadas al riesgo con el fin de evitar cualquier tipo de quiebra de seguridad, incluidas aquellas derivadas de error o negligencia humana.

TERCERO: NOTIFICAR la presente resolución a ***A.A.A.***.

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.

1403-16012024

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