

Expediente N°: EXP202208793

RESOLUCIÓN DE TERMINACIÓN DEL PROCEDIMIENTO POR PAGO
VOLUNTARIO

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

ANTECEDENTES

PRIMERO: Con fecha 18 de septiembre de 2023, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a **SACYR SOCIAL, S.L.** (en adelante, la parte reclamada), mediante el Acuerdo que se transcribe:

<<

Expediente N.º: EXP202208793

ACUERDO DE INICIO DE PROCEDIMIENTO SANCIONADOR

De las actuaciones practicadas por la Agencia Española de Protección de Datos y en base a los siguientes

HECHOS

PRIMERO: **A.A.A.** (en adelante, la parte reclamante) con fecha 15 de julio de 2022 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra SACYR SOCIAL, S.L., con NIF B85621159 (en adelante, la parte reclamada o Sacyr). Los motivos en que basa la reclamación son los siguientes:

En el escrito recibido se informa de lo siguiente:

La reclamante manifiesta que facilitó inicialmente a la entidad reclamada, en la que presta sus servicios, su dirección de correo electrónico personal, consintiendo en un primer momento, dado que era nueva empresa, (subrogación de los trabajadores por adjudicación de concesión de prestación de un servicio público) para que se usara como método de contacto, ya que no disponía de dirección corporativa. No obstante, reclama porque desde hace más de un año que ha solicitado que supriman sus datos (correo electrónico y teléfono personales) para que únicamente se pongan en contacto a través de teléfono o correo de empresa. Sin embargo, siguen contactando con ella a través de su correo electrónico personal.

Manifiesta además que al enviar la empresa mensajes de correo a su dirección personal, se realiza sin copia oculta, revelando dicho correo a los demás destinatarios.

Junto con la reclamación aporta:

- Copia de varios correos enviados por la entidad reclamada a su dirección de correo personal, conteniendo cuestiones relacionadas con la gestión y organización del trabajo (de fechas 25/05/2022 y 3/06/2022)
- Copia de dos correos enviados por la entidad reclamada el 15/06/2022, con contenido sobre acciones formativas remitidas a diversos destinatarios, entre los que se encuentra la dirección de correo personal de la reclamante, sin la opción de copia oculta.

No se aporta documentación alguna acreditativa de la solicitud de supresión de los datos ni de su deseo de que ya no se utilice su teléfono y correo electrónico personales como medio de contacto para cuestiones relacionadas con la gestión y organización del trabajo.

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), se dio traslado de dicha reclamación a Sacyr, 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 29 de agosto de 2022 como consta en el acuse de recibo que obra en el expediente.

Con fecha 21 de septiembre de 2022 se recibe en esta Agencia escrito de respuesta indicando lo siguiente:

-Que el correo electrónico corporativo no se contempla como una herramienta de trabajo de los auxiliares domiciliarios del SAD (Servicio de Ayuda a Domicilio), grupo al que pertenece la reclamante, si no como un canal de comunicación puntual de la compañía con los empleados, habiéndose definido para este grupo de empleados que la herramienta esencial corporativa de comunicación es un terminal de teléfono móvil puesto a su disposición

Este teléfono se encuentra preparado para poder comunicarse con los auxiliares de ayuda a domicilio tanto verbalmente por llamada telefónica como por escrito, a través de la aplicación WhatsApp, con el fin de acoger mediante dicho canal las comunicaciones laborales escritas, además de incorporar otras funcionalidades como el registro horario de la jornada de trabajo.

Que no obstante lo anterior, indica que no todos los auxiliares de ayuda a domicilio tienen actualmente instalada y en funcionamiento la aplicación WhatsApp en sus terminales móviles corporativos, ya que debido al alto volumen de empleados afectados la compañía está experimentando algo de demora en la gestión de estas instalaciones. Con ello señala que, de forma puntual y transitoria, se ha estado usando el correo electrónico personal de los empleados para comunicaciones estrictamente

relacionadas con la ejecución de la relación contractual laboral, junto con, siempre que haya sido posible, la comunicación verbal a través del teléfono móvil corporativo.

Así mismo indica que tanto la reclamante, así como los empleados que comparten su misma categoría profesional dentro de la concesión a la que pertenece están recibiendo una media de 7 correos al mes.

-En cuanto al envío de comunicaciones laborales sin el uso de la funcionalidad de copia oculta, la reclamada indica que se ha debido a una falta puntual de diligencia que no se corresponde con el uso y tratamiento habitual de los datos personales de los empleados

Entiende la entidad reclamada que este hecho es puntual no supone una revelación de datos crítica. No obstante, indica que los empleados de la compañía responsables de la coordinación de los empleados adscritos a la concesión a la que pertenece la reclamante han sido objeto de recordatorio e indicación expresa y de forma inmediata por el DPO de la compañía del obligatorio uso de la funcionalidad de copia oculta en envíos que involucren cuentas personales de correo electrónico.

-En relación con la afirmación de la reclamante relativa a que “*tras más de un año solicitando que se le dé una dirección de correo corporativa y se supriman sus datos personales, sigue recibiendo comunicaciones en su correo personal*” indica la reclamada que:

- Revisados los registros de notificaciones recibidas por el DPO de la compañía en referencia al derecho de supresión supuestamente ejercido, no han sido halladas evidencias al respecto, esto es, en el periodo comprendido desde el inicio de la relación laboral a la actualidad la empleada no ha presentado ante el DPO ejercicio de derecho alguno.

- Revisados los registros de notificaciones a los coordinadores del Servicio de Ayuda a Domicilio de la concesión a la que pertenece la reclamante no consta el ejercicio formal del derecho de supresión por su parte ante dichos coordinadores. Sin embargo, sí constan respuestas por escrito de la reclamante, los días 15 de julio y 5 y 6 de agosto de 2022, a dos correos de objeto laboral enviados por los coordinadores instándoles a que no se le envíen más correos electrónicos

Indica la reclamada que ha reaccionado de forma inmediata a la reclamación interpuesta por la empleada, ya que desde el día 30 de agosto de 2022 se ha cesado en el uso del correo electrónico personal de la reclamante, instalándose con prioridad en su terminal móvil corporativo la aplicación WhatsApp a través de la cual está recibiendo actualmente las comunicaciones escritas relacionadas con el desarrollo de sus competencias profesionales.

Aporta la siguiente documentación:

- Copia de escrito en el que se documenta la entrega por la entidad reclamada de un terminal móvil corporativo a la reclamante, de fecha 16 de junio de 2021
- Copia de los correos de respuesta de la reclamante en los que solicita que no se le envíen más correos electrónicos
- Copia de carta de respuesta dirigida a la reclamante.

TERCERO: Con fecha 26 de septiembre de 2022, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: De acuerdo con el informe recogido de la herramienta AXESOR, la entidad SACYR SOCIAL, S.L. es una gran empresa constituida en el año 2009, y con un volumen de negocios de 108.478.379 euros en el año 2021.

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, 64.2 y 68.1 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 registrarán 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 reclamada realiza, entre otros tratamientos, la recogida, registro, conservación, utilización, acceso, supresión de los siguientes datos personales de personas físicas, tales como: nombre, N.I.F, datos de contacto, número de teléfono/ dirección de correo electrónico, etc.

La 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 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."

En el presente caso, consta una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad al haberse enviado por correo electrónico a varios empleados de la reclamada varios

mails sin utilizar la copia oculta, mostrándose direcciones de correo electrónico personales como la de la reclamante.

Dentro de los principios del tratamiento previstos en el artículo 5 del RGPD, la integridad y confidencialidad de los datos personales se garantiza en el apartado 1.f) del artículo 5 del RGPD. Por su parte, la seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD, que reglamentan la seguridad del tratamiento, la notificación de una violación de la seguridad de los datos personales a la autoridad de control, así como la comunicación al interesado, respectivamente.

III

Artículo 5.1.f) del RGPD

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 la parte reclamante fueron indebidamente expuestos a terceros, al enviarse por correo electrónico a 129 empleados de la entidad reclamada varios mails sin utilizar la opción de copia oculta, mostrándose las direcciones de correo electrónico personales de los mismos.

De conformidad con las evidencias de las que se dispone en este acuerdo de iniciación del procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que los hechos conocidos podrían ser constitutivos de una infracción, imputable a Sacyr, por vulneración del artículo 5.1.f) del RGPD.

IV

Tipificación de la infracción del artículo 5.1.f) del RGPD

De confirmarse, la citada infracción del artículo 5.1.f) del RGPD podría suponer 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. (...)”

V

Sanción por la infracción del artículo 5.1.f) del RGPD

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone en el presente momento de acuerdo de inicio de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que procede graduar la sanción a imponer de acuerdo con los criterios que establecen el artículo 83.2 del RGPD y el apartado 2 del artículo 76 “Sanciones y medidas correctivas” de la LOPDGDD:

- Artículo 83.2.a) RGPD: Naturaleza, gravedad y duración de la infracción.

☐ Se considera que la naturaleza de la infracción es grave puesto que acarrea una pérdida de confidencialidad y, por tanto, de disposición y control irremediable sobre los datos personales.

☐ Número de interesados afectados: 196

- Artículo 83.2.b) RGPD. Negligencia en la infracción: Se observa la existencia de negligencia a la hora de garantizar la confidencialidad de estos. A este respecto, debe recordarse que Sacyr es una gran empresa que realiza, como responsable y/o encargado, tratamientos que afectan a numerosas personas físicas, tanto de las personas a las que presta sus servicios de asistencia, como de sus empleados (más de 5.000) por lo que se le exige un nivel de diligencia mayor para garantizar la confidencialidad de los datos personales que trata.

Procede recordar, en este sentido, la Sentencia de la Audiencia Nacional de 17/10/2007 (rec. 63/2006), que respecto de entidades cuya actividad lleva aparejado el continuo tratamiento de datos de clientes, indica “...el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha

de insistirse en el rigor y el exquisito cuidado por ajustarse a las previsiones legales al respecto.

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el apartado 2 del artículo 76 “Sanciones y medidas correctivas” de la LOPDGDD:

Como agravantes:

- Artículo 76.2.b) LOPDGDD. Vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal: La reclamada se dedica a la prestación de servicios sociales, sanitarios, educativos y de ocio. El desarrollo de esta actividad supone un tratamiento continuo de datos personales que afectan a numerosas personas (destinatarios de sus servicios y más de 5.200 empleados). Por tanto, se trata de una empresa grande habituada al tratamiento de datos personales, entre los cuales pueden figurar datos relativos a la salud, socioeconómicos, familiares, etc.

Por tanto, teniendo en cuenta las circunstancias del caso y los criterios que establece el artículo 83.2 del RGPD y el artículo 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 5.1.f) del RGPD, procede fijar inicialmente una sanción de 12.000 (doce mil euros).

VI

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”.

De la documentación obrante en el expediente se ofrecen indicios evidentes de que la parte reclamada ha vulnerado el artículo 32 del RGPD, al producirse un incidente de seguridad permitiendo el acceso ilícito a datos personales, en concreto a direcciones de correo electrónico personales, al ser remitidos correos sin utilizar la opción de copia oculta.

Hay que señalar que el RGPD en el citado precepto no establece un listado de las medidas de seguridad que sean de aplicación de acuerdo con los datos que son objeto de tratamiento, sino que establece que el responsable y el encargado del tratamiento aplicarán 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, señalando que la determinación de las medidas técnicas y organizativas deberá realizarse 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 tendrán 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.

En este mismo sentido 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 caso, en el momento de producirse la brecha, no cabe afirmar que la reclamada contase con las medidas adecuadas en función de los posibles riesgos estimados para evitar el incidente, así como que las medidas de formación y concienciación dirigida al personal que debía realizar los tratamientos con datos personales era del todo insuficiente, concretamente respecto del envío de correos electrónicos, puesto que, como se ha señalado, se remitieron varios a los empleados de la reclamada sin utilizar la opción de copia oculta, mostrándose las direcciones de correo electrónico personales de 129 empleados.

La responsabilidad de la parte reclamada viene determinada por la quiebra de seguridad puesta de manifiesto en la reclamación y documentación aportada, ya que es responsable de tomar decisiones destinadas a implementar de manera efectiva las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para asegurar la confidencialidad de los datos.

De conformidad con las evidencias de las que se dispone en este acuerdo de iniciación del procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que los hechos conocidos podrían ser constitutivos de una infracción, imputable a la reclamada, por vulneración del artículo 32 del RGPD

VII

Tipificación 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. (...)

VIII

Sanción por la infracción del artículo 32 del RGPD

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone en el presente momento de acuerdo de inicio de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que la sanción a imponer de acuerdo con los criterios que establecen el artículo 83.2 del RGPD y el apartado 2 del artículo 76 “Sanciones y medidas correctivas” de la LOPDGDD

- Artículo 83.2.a) RGPD: Naturaleza, gravedad y duración de la infracción.

Se considera que la naturaleza de la infracción es grave puesto que supone que Sacry no cuenta con medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad adecuado al riesgo, o bien, existentes estas, no han sido observadas o correctamente implementadas, lo que, además, en el caso concreto, ha supuesto una pérdida de confidencialidad y, por tanto, de disposición y control sobre los datos personales.

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el apartado 2 del artículo 76 “Sanciones y medidas correctivas” de la LOPDGDD:

Como agravantes:

- Artículo 76.2.b) LOPDGDD. Vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal: La reclamada se dedica a la prestación de servicios sociales, sanitarios, educativos y de ocio. El desarrollo de esta actividad supone un tratamiento continuo de datos personales que afectan a numerosas personas (destinatarios de sus servicios y alrededor de 5.200 empleados, según manifiesta). Por tanto, se trata de una empresa grande habituada al tratamiento de datos personales, entre los cuales pueden figurar datos relativos a la salud, socioeconómicos, familiares, etc.

Por tanto, teniendo en cuenta las circunstancias del caso y los criterios que establece el artículo 83.2 del RGPD y el artículo 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 32 del RGPD, permite fijar inicialmente una sanción de 3.000 € (tres mil euros).

IX

Imposición de medidas

De confirmarse la infracción, podría acordarse 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...”*. La imposición de esta medida es compatible con la sanción consistente en multa administrativa, según lo dispuesto en el art. 83.2 del RGPD.

Se advierte que no atender la posible orden de adopción de medidas impuestas por este organismo en la resolución sancionadora 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, a tenor de lo anteriormente expuesto, por la Directora de la Agencia Española de Protección de Datos, SE ACUERDA:

PRIMERO: INICIAR PROCEDIMIENTO SANCIONADOR a SACYR SOCIAL, S.L., con NIF B85621159, por la presunta infracción de los artículos 5.1.f) y 32 del RGPD, tipificadas, respectivamente, en los artículos 83.5 y 83.4 del RGPD.

SEGUNDO: NOMBRAR como instructora a **B.B.B.** y, como secretaria, a **C.C.C.**, indicando que podrán ser recusadas, en su caso, conforme a lo establecido en los artículos 23 y 24 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP).

TERCERO: INCORPORAR al expediente sancionador, a efectos probatorios, la reclamación interpuesta por la parte reclamante y su documentación, así como los documentos obtenidos y generados por la Subdirección General de Inspección de Datos en las actuaciones previas al inicio del presente procedimiento sancionador.

CUARTO: QUE a los efectos previstos en el art. 64.2 b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la sanción que pudiera corresponder sería de:

DOCE MIL EUROS (12.000 euros) por la presunta infracción del artículo 5.1.f) del RGPD, tipificada en el Artículo 83.5 del RGPD.

TRES MIL EUROS (3.000) por la presunta infracción del 32 del RGPD, tipificada en el artículo 83.4 del RGPD

QUINTO: NOTIFICAR el presente acuerdo a SACYR SOCIAL, S.L., con NIF B85621159, otorgándole un plazo de audiencia de diez días hábiles para que formule las alegaciones y presente las pruebas que considere convenientes. En su escrito de alegaciones deberá facilitar su NIF y el número de expediente que figura en el encabezamiento de este documento.

Si en el plazo estipulado no efectuara alegaciones a este acuerdo de inicio, el mismo podrá ser considerado propuesta de resolución, según lo establecido en el artículo

64.2.f) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP).

De conformidad con lo dispuesto en el artículo 85 de la LPACAP, podrá reconocer su responsabilidad dentro del plazo otorgado para la formulación de alegaciones al presente acuerdo de inicio; lo que llevará aparejada una reducción de un 20% de la sanción que proceda imponer en el presente procedimiento. Con la aplicación de esta reducción, la sanción quedaría establecida en **12.000 euros**, resolviéndose el procedimiento con la imposición de esta sanción.

Del mismo modo podrá, en cualquier momento anterior a la resolución del presente procedimiento, llevar a cabo el pago voluntario de la sanción propuesta, lo que supondrá la reducción de un 20% de su importe. Con la aplicación de esta reducción, la sanción quedaría establecida en **12.000 euros** y su pago implicará la terminación del procedimiento, sin perjuicio de la imposición de las medidas correspondientes.

La reducción por el pago voluntario de la sanción es acumulable a la que corresponde aplicar por el reconocimiento de la responsabilidad, siempre que este reconocimiento de la responsabilidad se ponga de manifiesto dentro del plazo concedido para formular alegaciones a la apertura del procedimiento. El pago voluntario de la cantidad referida en el párrafo anterior podrá hacerse en cualquier momento anterior a la resolución. En este caso, si procediera aplicar ambas reducciones, el importe de la sanción quedaría establecido en **9.000 euros**.

En todo caso, la efectividad de cualquiera de las dos reducciones mencionadas estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

En caso de que optara por proceder al pago voluntario de cualquiera de las cantidades señaladas anteriormente (12.000 ó 9.000 euros) deberá hacerlo efectivo mediante su ingreso en la cuenta nº **IBAN: ES00 0000 0000 0000 0000 0000** abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A., indicando en el concepto el número de referencia del procedimiento que figura en el encabezamiento de este documento y la causa de reducción del importe a la que se acoge.

Asimismo, deberá enviar el justificante del ingreso a la Subdirección General de Inspección para continuar con el procedimiento en concordancia con la cantidad ingresada.

El procedimiento tendrá una duración máxima de doce meses a contar desde la fecha del acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones, de conformidad con lo establecido en el artículo 64 de la LOPDGDD.

En cumplimiento de los artículos 14, 41 y 43 de la LPACAP, se advierte de que, en lo sucesivo, las notificaciones que se le remitan se realizarán exclusivamente de forma electrónica, a través de la Dirección Electrónica Habilitada Única (dehu.redsara.es), y que, de no acceder a ellas, se hará constar su rechazo en el expediente, dando por efectuado el trámite y siguiéndose el procedimiento. Se le informa que puede

identificar ante esta Agencia una dirección de correo electrónico para recibir el aviso de puesta a disposición de las notificaciones y que la falta de práctica de este aviso no impedirá que la notificación sea considerada plenamente válida.

Por último, se señala que conforme a lo establecido en el artículo 112.1 de la LPACAP, contra el presente acto no cabe recurso administrativo alguno.

935-290523

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

>>

SEGUNDO: En fecha 3 de octubre de 2023, la parte reclamada ha procedido al pago de la sanción en la cuantía de **9000 euros** haciendo uso de las dos reducciones previstas en el Acuerdo de inicio transcrito anteriormente, lo que implica el reconocimiento de la responsabilidad.

TERCERO: El pago realizado, dentro del plazo concedido para formular alegaciones a la apertura del procedimiento, conlleva la renuncia a cualquier acción o recurso en vía administrativa contra la sanción y el reconocimiento de responsabilidad en relación con los hechos a los que se refiere el Acuerdo de Inicio.

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, 64.2 y 68.1 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 registrarán 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

Terminación del procedimiento

El artículo 85 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP), bajo la rúbrica

“Terminación en los procedimientos sancionadores” dispone lo siguiente:

“1. Iniciado un procedimiento sancionador, si el infractor reconoce su responsabilidad, se podrá resolver el procedimiento con la imposición de la sanción que proceda.

2. Cuando la sanción tenga únicamente carácter pecuniario o bien quepa imponer una sanción pecuniaria y otra de carácter no pecuniario pero se ha justificado la improcedencia de la segunda, el pago voluntario por el presunto responsable, en cualquier momento anterior a la resolución, implicará la terminación del procedimiento, salvo en lo relativo a la reposición de la situación alterada o a la determinación de la indemnización por los daños y perjuicios causados por la comisión de la infracción.

3. En ambos casos, cuando la sanción tenga únicamente carácter pecuniario, el órgano competente para resolver el procedimiento aplicará reducciones de, al menos, el 20 % sobre el importe de la sanción propuesta, siendo éstos acumulables entre sí. Las citadas reducciones, deberán estar determinadas en la notificación de iniciación del procedimiento y su efectividad estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

El porcentaje de reducción previsto en este apartado podrá ser incrementado reglamentariamente.”

De acuerdo con lo señalado,
la Directora de la Agencia Española de Protección de Datos **RESUELVE:**

PRIMERO: DECLARAR la terminación del procedimiento **EXP202208793**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

SEGUNDO: NOTIFICAR la presente resolución a **SACYR SOCIAL, S.L.**

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, los interesados podrán interponer 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.

936-040822

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