- **Expediente Nº: EXP202200399**

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 julio de 2022, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a **BAYARD REVISTAS, S.A.** (en adelante, la parte reclamada), mediante el Acuerdo que se transcribe:

<<

Expediente N.º: EXP202200399

ACUERDO DE INICIO DE PROCEDIMIENTO SANCIONADOR

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

HECHOS

PRIMERO: D. ***A.A.A.*** (en adelante, la parte reclamante) con fecha 27 de noviembre de 2021 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra BAYARD REVISTAS, S.A con NIF A78874054 (en adelante, BAYARD). Los motivos en que basa la reclamación son los siguientes:

La parte reclamante pone en conocimiento de esta Agencia que ha recibido un email por parte del responsable del portal web ******URL.1***, en el que se le informaba sobre el acceso no autorizado a la base de datos por una tercera persona no autorizada, siendo responsable BAYARD.

Según el email, se han visto involucrados datos de localización y contacto de las personas que habían facilitado su información en el sitio web a través del formulario de registro.

El responsable asegura que ha solucionado todas las vulnerabilidades que han posibilitado el ataque, ha implementado los protocolos a seguir en caso de incidencia relacionada con la protección de los datos, y ha adoptado una serie de medidas, entre las que se encuentra el cifrado de la información almacenada.

Se acompaña a esta reclamación la captura de pantalla del correo electrónico recibido en fecha 19 de noviembre de 2021, alertando de la brecha.

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 BAYARD, 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 se remitió con fecha 21 de enero de 2022 mediante notificación electrónica, conforme al artículo 41 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP).

Esta notificación fue rechazada automáticamente tras haber transcurrido diez días naturales desde su puesta a disposición para su acceso según el párrafo 2, artículo 43, de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas; reiterándose el traslado por correo certificado, con fecha 01 de febrero de 2022, resultando esta última con estado “desconocido” sin posibilidad de localizar a dicho responsable.

TERCERO: Con fecha 23 de febrero de 2022, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

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 los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 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, con fecha 01 de marzo de 2022 se requirió información BAYARD, con la finalidad de que aclare los aspectos relacionados con la violación de seguridad que da lugar a la reclamación interpuesta.

El requerimiento de información se remitió mediante notificación electrónica, conforme al artículo 41 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP).

Si bien, esta notificación fue rechazada automáticamente tras haber transcurrido diez días naturales desde su puesta a disposición para su acceso según el párrafo 2, artículo 43, de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas; reiterándose el traslado por correo certificado, con fecha 14 de marzo de 2022, pero utilizándose domicilio fiscal diferente al utilizado en el traslado, domicilio obtenido de la web del responsable, resultando este último requerimiento exitoso con fecha de acuse el 22 de marzo de 2022.

QUINTO: El 6 de abril de 2022 se recibe respuesta a dicha solicitud de información.

SEXTO: En el marco de las citadas actuaciones previas de investigación se dirigió, nuevamente, requerimiento de información con fecha 25 de abril de ese mismo año.

El requerimiento de información se remitió mediante notificación electrónica, conforme al artículo 41 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP).

SÉPTIMO: El 5 de mayo de ese mismo año se recibe respuesta dicho requerimiento de información.

OCTAVO: De las actuaciones previas de investigación practicadas para el esclarecimiento de los hechos en cuestión, se ha tenido conocimiento de los siguientes extremos:

Con relación al responsable de tratamiento de los datos personales tratados por el portal web ****URL.1* así como de la posible existencia de delegado de protección de datos (DPD), por BAYARD se contesta:

- El responsable de tratamiento de este portal es BAYARD REVISTAS S.A.
- El DPD es GRUPO ADAPTALIA LEGAL FORMATIVO S.L, no obstante, en el momento de producirse la violación de seguridad se tenía únicamente un contrato de asesoría en materia de protección de datos, y que este contrato se amplió en fecha de 17 de enero de 2022 por el que se extendían estos servicios para que el grupo anterior actuara como delegado de protección de datos del responsable BAYARD REVISTAS S.A. Esta vinculación también se comunicó ante esta Agencia el 03 de marzo de 2022, a través de la Subdirección General de Promoción y Autorizaciones, se nos aporta copia del documento de inscripción.

Respecto a la tipología de los datos afectados y descripción cronológica de los hechos acaecidos, BAYARD contesta:

Que el 22 de octubre de 2021 se recibe email firmado por una persona externa, que se identificaba como supuesto investigador y divulgador especializado en ciberseguridad web, informando que había conseguido acceder a los datos de la compañía a raíz de una vulnerabilidad del sitio web, aportando como prueba captura de pantalla con los nombres de las tablas de la base de datos, sin aportar prueba sobre la filtración de datos.

Que este ataque no se había realizado con fines maliciosos sino con la intención de hacking ético, por ello del aviso de la vulnerabilidad al responsable de la web sin ningún propósito delictivo.

Que los datos filtrados corresponden a datos identificativos, de contacto, datos de localización aproximada y en algunos casos datos identificativos de hijos menores de edad.

Que a partir de este momento se contrató los servicios de una tercera compañía experta en ciberseguridad (ACUNETIX) para que identificara y subsanara las vulnerabilidades de la web.

Que el número de afectados correspondería al número total de usuarios del portal web, rondando esta cifra los 464762.

Que ningún usuario ha comunicado que sus datos hayan podido ser utilizados.

En cuanto al análisis de riesgos y las medidas de seguridad que se tenían implantadas previamente al incidente, BAYARD contesta que sí tenían análisis de riesgos realizado previamente a través de la herramienta AEPD GESTIONA, aportando anexo como evidencia de este.

No obstante, tras analizarlo, se concluye que este documento hace referencia al reporte generado por la propia herramienta GESTIONA EIPD de esta Agencia y se incluye tanto una descripción del ciclo de vida de los datos como una relación de requisitos de cumplimiento normativo orientados a la gestión de riesgos, pero no se identifican ni analizan otros factores de riesgos con distinto origen al incumplimiento normativo, por ejemplo, los relacionados con la tecnología empleada.

Las medidas de seguridad implantadas con anterioridad a la brecha, y que se habían demostrado como ineficientes, eran:

- (…)

En cuanto a las medidas de contención, se señalan:

- Contratar servicios de ciberseguridad para identificar todas las vulnerabilidades que permitieron la filtración y aplicar medidas de refuerzo para proteger las BD SQL de la compañía.
- Comunicar la brecha a GRUPO ADAPTALIA LEGAL FORMATIVO S.L, proveedor externo especializado en protección de datos (que por aquella fecha prestaba servicios de asesoría sobre protección de datos, para analizar y determinar las necesidades y obligaciones sobre notificación y comunicación tanto a AEPD como afectados.
- Refrescar e implementar a nivel interno el protocolo de actuación en caso de violación de seguridad para que todo el personal sepa cómo actuar en caso de conocimiento de brecha de seguridad.
- Comunicar con los afectados.
- Notificar a la AEPD.

Respecto a la comunicación a los afectados, BAYARD responde que:

Se comunicó vía email a los cerca de 470000 afectados, en fecha de 20 de noviembre de 2021, aportando copia de email enviado a uno de los afectados.
Tras analizar el mismo se determina que este correo se envió el 19 de noviembre de 2021 a uno de los supuestos afectados trasladándole información sobre:

- o La tipología de datos afectados comunicando que se trata de datos de contacto y localización proporcionados a través del formulario de registro del portal web.
- o Las circunstancias en las que se producen los hechos, informando sobre el email recibido por el supuesto hacker.
- o Las posibles consecuencias, como pérdida de confidencialidad de la información proporcionada a través del portal web.

o Las medidas correctivas adoptadas y que corresponden con las mencionadas anteriormente.

En cuanto a la notificación de la brecha ante esta Agencia, BAYARD contesta que inmediatamente después de analizar la brecha por GRUPO ADAPTALIA, se procede a notificar la misma ante esta Agencia, aportándose como prueba copia del registro de entrada de la notificación.

Del análisis de esta podemos extraer la siguiente información:

- Que se detecta el 22 de octubre de 2021 por la notificación de un tercero ajeno y que se da por resuelta el 26 de octubre de 2021.

Se reporta por una persona externa que ha podido tener acceso a los datos enviando como prueba únicamente una captura de pantalla con el nombre de las tablas de la base de datos, sin aportar los datos.
- Que los datos afectados son datos básicos, de localización y de contacto.
- Indican que entre las personas afectadas hay datos identificativos de menores.
- Que se ha actualizado el registro de incidentes.
- Que entre las nuevas medidas de seguridad está la realización de auditorías periódicas y el cifrado de los datos.

En relación con la existencia de terceras compañías que pudieran actuar como encargados de tratamiento de la información personal, responden que el único tercero es Amazon Web Services (AWS) con quienes tienen contratado el alojamiento web, firmándose las condiciones generales de contratación en materia de protección de datos publicadas por AWS en la dirección ******URL.2***

FUNDAMENTOS DE DERECHO

I
Competencia

En virtud de los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 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 (RGPD) reconoce a cada autoridad de control, y según lo establecido en los artículos 47 y 48 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para iniciar y resolver este procedimiento.

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 BAYARD, entre otros tratamientos, realiza la recogida, registro, conservación…etc, de los datos de contacto y localización proporcionados por los usuarios, a través del formulario de registro del portal web.

BAYARD 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 accedido a los datos de los usuarios del portal web, por una vulnerabilidad del sitio web.

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.

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 los afectados, obrantes en la base de datos de BAYARD, fueron indebidamente expuestos a un tercero.

El 22 de octubre de 2021 BAYARD recibe email firmado por una persona externa, que se identificaba como supuesto investigador y divulgador especializado en ciberseguridad web, informando que había conseguido acceder a los datos de la compañía a raíz de una vulnerabilidad del sitio web, aportando como prueba captura de pantalla con los nombres de las tablas de la base de datos y sin aportar prueba sobre la filtración de 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 BAYARD, 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 la infracción en cuestión es grave a los efectos del RGPD y que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Como agravantes:

- g) las categorías de los datos de carácter personal afectados por la infracción.

En el presente caso, los datos filtrados corresponden a datos identificativos, de contacto, datos de localización aproximada y en algunos casos datos identificativos de hijos menores de edad.

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:

- b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

  BAYARD colabora con sus publicaciones en la difusión de la cultura y el fomento de la lectura, disponiendo de una base de datos de los usuarios del portal web.

- f) La afectación a los derechos de los menores.

  Tal y como consta en el expediente los datos filtrados corresponden a datos identificativos, de contacto, datos de localización aproximada y en algunos casos datos identificativos de hijos menores de edad.

El balance de las circunstancias contempladas en 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, permite fijar inicialmente una sanción de IMPORTE DE 30.000 € (treinta 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".

En el presente caso, BAYARD como responsable del tratamiento de datos, está obligado a aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que presente el tratamiento de datos.

"(…)".

Si bien, el análisis de riesgos que aportan es el reporte de salida generado por la herramienta GESTIONA EIDP de esta Agencia.

Esta herramienta sirve, únicamente, de guía para establecer los elementos básicos que deben ser tenidos en cuenta en los análisis de riesgos de los tratamientos y evaluaciones de impacto, sin embargo, no es válida para identificar de forma exhaustiva los posibles factores de riesgo que deben ser evaluados para proteger los derechos y libertades de los interesados presentes en el tratamiento de datos.

El análisis de riesgos proporcionado carece de la identificación de factores que hagan referencia a posibles amenazas de ataques web relacionadas con la pérdida de confidencialidad, disponibilidad o integridad de los datos personales tratados a través del propio portal ******URL.1***.

El artículo 32 del RGPD 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 organizati-vas 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 verifica-ción (que no auditoría), evaluación y valoración de la eficacia de las medidas.

En relación con las medidas preventivas implantadas de forma previa a la brecha, no existe vinculación alguna entre estas medidas y el propio análisis de riesgos realizado, por lo que no se puede demostrar que dichas medidas se desplegaron para mitigar un determinado nivel de riesgo inherente del tratamiento para los derechos y libertades de las personas cuyos datos personales se trata.

Es de resaltar que con ***(…)".***

(…).

Y por último, en cuanto a las medidas de contingencia, BAYARD en su escrito de respuesta dice literalmente:

"(…)."

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 BAYARD, 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 infracción en cuestión es grave a los efectos del RGPD y que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Como agravantes:

- g) las categorías de los datos de carácter personal afectados por la infracción.

  En el presente caso, los datos filtrados corresponden a datos identificativos, de contacto, datos de localización aproximada y en algunos casos datos identificativos de hijos menores de edad.

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:

- b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

  BAYARD colabora con sus publicaciones en la difusión de la cultura y el fomento de la lectura, disponiendo de una base de datos de los usuarios del portal web.

- f) La afectación a los derechos de los menores.

  Tal y como consta en el expediente los datos filtrados corresponden a datos identificativos, de contacto, datos de localización aproximada y en algunos casos datos identificativos de hijos menores de edad.

El balance de las circunstancias contempladas en 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 20.000 € (importe de veinte mil euros).

IX
Artículo 33 del RGPD

El Artículo 33 "*Notificación de una violación de la seguridad de los datos personales a la autoridad de control*" del RGPD establece:

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

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

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

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

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

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

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

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

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

En el presente caso, consta que BAYARD tiene constancia de haber sufrido una brecha de seguridad de los datos personales en fecha 28 de octubre de 2021 y no ha informado a esta Agencia, hasta la fecha el 11 de noviembre de ese mismo año.

El 28 de octubre ya se tenía constancia de la existencia de vulnerabilidades web que hubiera posibilitado la pérdida de la confidencialidad en datos personales, y es en ese momento cuando se traslada a la empresa asesora en protección de datos para que se le indicara cómo actuar en consecuencia.

Para valorar las necesidades de notificación utilizaron la fórmula que aparece en la "Guía para la gestión y notificación de las violaciones de seguridad": Riesgo = P (Volumen) x I (Tipología x Impacto), utilizando los siguientes parámetros:

- o Volumen = 4 (Más de 100.000)
- o Tipología = 1 (Datos no sensibles)
- o Impacto = 8 (Público, accesible en internet)

No obstante, y teniéndose en cuenta que el 28 de octubre ya se tenía constancia de la posible brecha que afectara a datos personales, existe dilación temporal en relación con la notificación de la brecha a esta Agencia, ya que se realiza el 11 de noviembre de 2021.

De igual forma ocurre con la comunicación a los afectados, que se realiza en fecha aproximada de 20 de noviembre 2021.

Por ello, se decide realizar a BAYARD nuevo requerimiento de información en fecha 24 de abril de 2022 para que se aclare las siguientes cuestiones:

- Motivos que justificarían la dilación en la notificación a la Agencia.

- Motivos que justificarían la dilación en la comunicación con los afectados.

Con relación a la dilación a la notificación de la brecha de seguridad a la Agencia, indican que, en el momento del conocimiento de esta, BAYARD no podía asegurar que dicha brecha fuera real, y por lo tanto desconocía el riesgo existente para los derechos y libertades de los interesados.

Aportando lo siguiente**: "*(…)*."**

Si bien, no se han encontrado pruebas de esta notificación realizada el 2 de diciembre ni tampoco de la afirmación anteriormente referida; en consecuencia, no se pueden admitir dichos motivos de dilación.

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 BAYARD, por vulneración del artículo 33 del RGPD.

X
Tipificación de la infracción del artículo 33 del RGPD

De confirmarse, la citada infracción del artículo 33 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:

(…)

> *r) El incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679. (…)"*

XI
Sanción por la infracción del artículo 33 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 infracción en cuestión es grave a los efectos del RGPD y que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Como agravantes:

- g) las categorías de los datos de carácter personal afectados por la infracción.

En el presente caso, los datos filtrados corresponden a datos identificativos, de contacto, datos de localización aproximada y en algunos casos datos identificativos de hijos menores de edad.

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:

- b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

  BAYARD colabora con sus publicaciones en la difusión de la cultura y el fomento de la lectura, disponiendo de una base de datos de los usuarios del portal web.

- f) La afectación a los derechos de los menores.

  Tal y como consta en el expediente los datos filtrados corresponden a datos identificativos, de contacto, datos de localización aproximada y en algunos casos datos identificativos de hijos menores de edad.

El balance de las circunstancias contempladas en 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 33 del RGPD, permite fijar inicialmente una sanción de 2.000 € (dos mil euros).

XII
Imposición de medidas

Entre los poderes correctivos que dispone el artículo 58 "*Poderes*" del RGPD, en el apartado 2.d) se establece que 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 Agencia Española de Protección de Datos en la resolución que ponga fin al presente procedimiento podrá ordenar la adopción de medidas, según lo establecido en el artículo 58.2.d) del RGPD y de conformidad con lo que se derive de la instrucción del procedimiento, si fuera preciso, de manera adicional a sancionar con una multa.

Por lo tanto, por la Directora de la Agencia Española de Protección de Datos, SE ACUERDA:

PRIMERO: INICIAR PROCEDIMIENTO SANCIONADOR a BAYARD REVISTAS, S.A con NIF A78874054, por la presunta infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5 del RGPD.

INICIAR PROCEDIMIENTO SANCIONADOR a BAYARD REVISTAS, S.A con NIF A78874054, por la presunta infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 del RGPD.

INICIAR PROCEDIMIENTO SANCIONADOR a BAYARD REVISTAS, S.A con NIF A78874054, por la presunta infracción del artículo 33 del RGPD, tipificada en el artículo 83.4 del RGPD.

SEGUNDO: QUE a los efectos previstos en el artículo 64.2 b) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP), la sanción que pudiera corresponder, sin perjuicio de lo que resulte de la instrucción, sería de:

TREINTA MIL EUROS (30.000 €), por la presunta infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5 del RGPD.

VEINTE MIL EUROS (20.000 €), por la presunta infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 del RGPD.

DOS MIL EUROS (2.000 €), por la presunta infracción del artículo 33 del RGPD, tipificada en el artículo 83.4 del RGPD.

CUARTO: NOMBRAR como instructor a ***B.B.B.*** y, como secretario, a ***C.C.C.***, indicando que cualquiera de ellos podrá ser recusado, 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).

QUINTO: 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.

SEXTO: NOTIFICAR el presente acuerdo a BAYARD REVISTAS, S.A con NIF A78874054**,** 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 procedimiento 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).

Conforme dispone el artículo 85 de la LPACAP, iniciado un procedimiento sancionador, si el infractor reconoce su responsabilidad, se podrá resolver el procedimiento con la imposición de la sanción que proceda.

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 CUARENTA Y UN MIL EUROS (41.600€), resolviéndose el procedimiento con la imposición de esta sanción.

Del mismo modo podrá, en cualquier momento anterior a la resolución de este 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 CUARENTA Y UN MIL EUROS (41.600€) y su pago implicaría la terminación del procedimiento.

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 se ponga de manifiesto dentro del plazo concedido para formular alegaciones a la iniciación 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 TREINTA Y UN MIL DOS CIENTOS EUROS (31.200 €).

En todo caso, la efectividad de cualquiera de las citadas reducciones estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción impuesta, conforme dispone el artículo 85.3 de la LPACAP.

En caso de que optara por proceder al pago voluntario de cualquiera de las cantidades señaladas anteriormente (CUARENTA Y UN MIL EUROS (41.600€) o TREINTA Y UN MIL DOS CIENTOS EUROS (31.200 €), deberá hacerlo efectivo mediante su ingreso en la cuenta nº ***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 SGID para continuar con el procedimiento en concordancia con la cantidad ingresada.

El procedimiento tendrá una duración máxima de nueve meses a contar desde la fecha del acuerdo de inicio o, en su caso, del proyecto de acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones, conforme con lo establecido en el artículo 64.2 de la LOPDGDD.

935-110422

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

>>

SEGUNDO**:** En fecha 27 de julio de 2022, la parte reclamada ha procedido al pago de la sanción en la cuantía de **31200 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

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 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

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 **EXP202200399**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

SEGUNDO: NOTIFICAR la presente resolución a **BAYARD REVISTAS, S.A.**.

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.

936-020822

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