- **Expediente Nº: E/03857/2021**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

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

HECHOS

PRIMERO: La reclamación interpuesta por D. ***A.A.A.*** (en lo sucesivo, la parte reclamante) tiene entrada en fecha 19 de octubre de 2020 en la Agencia Española de Protección de Datos. La reclamación se dirige contra ACTURUS CAPITAL, S.L. (en adelante, la parte reclamada).

Los motivos en que basa su reclamación son que ganó un sorteo que realizaba la entidad reclamada y el premio era la remisión de unas prendas a su domicilio. Señala que le enviaron las destinadas a otro ganador, por lo que le dijeron que tramitarían el cambio. Al tramitar el cambio, el reclamante recibió un segundo envío con las prendas correctas. En este segundo envío, el reclamante indica que en el paquete aparece como remitente los datos postales del otro ganador.

Documentación relevante aportada por el reclamante:

Fotografía de la etiqueta de un sobre de un envío, con fecha 30 de septiembre de 2020, en el que el destinatario es el reclamante, y en los datos del remitente aparece un nombre y una dirección de A Coruña y un número de teléfono móvil.

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), con número de referencia E/09115/2020, en fecha 16 de noviembre de 2020, se dio traslado de dicha reclamación a la parte reclamada, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

Con fecha 14 de diciembre de 2020, se recibe escrito en nombre de la parte reclamada como contestación al traslado de la reclamación presentada, en el cual se indica que se adjunta la respuesta, pero no se presenta ningún documento adjunto al escrito.

Con fecha del 2 de febrero de 2021, se envía requerimiento de información, junto con el que se traslada la reclamación a la parte reclamada, constando su recepción el día 3 de febrero de 2021.

TERCERO: Con fecha 6 de abril de 2021, la Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada por la parte reclamante, al no haber recibido contestación al anterior requerimiento de información, en el procedimiento E/09115/2020. A continuación, la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación

para el esclarecimiento de los hechos objeto de la reclamación, teniendo conocimiento de los siguientes extremos:

Con fecha del 14 de abril de 2021, se envía un requerimiento de información, junto con el que se traslada la reclamación a la parte reclamada, y se da un plazo de diez días hábiles para contestar, que consta recibido el mismo día 14 de abril de 2021. Tras enviar un correo electrónico al delegado de protección de datos de la parte reclamada (en adelante, DPD), advirtiendo de que ha transcurrido el plazo de contestación, se recibe un escrito de contestación a este requerimiento de información, en nombre de la parte reclamada, con entrada en la AEPD el 10 de junio de 2021, en el que se aporta, entre otra, la siguiente información:
Manifestación de que el reclamante comunicó los hechos telefónicamente al departamento de marketing de la parte reclamada, y que, posteriormente, en fecha 15 de octubre de 2020, envió una comunicación a la parte reclamada para dar a conocer los hechos. Indicación de que, tras esta comunicación, se dio traslado al DPD.
Manifestación de que el DPD, tras contactar con el otro ganador del premio y con MRW, que es la empresa de mensajería que hizo los envíos, ha llegado a la conclusión de que el otro ganador se deshizo del paquete del envío sin darse cuenta de la presencia de los datos personales del reclamante y de que MRW trató los envíos como un intercambio entre los dos ganadores en vez de tratarlo como dos nuevos envíos.
Manifestación de que los datos de los ganadores del concurso comunicados a MRW se limitaban a nombre, apellidos, dirección y teléfono.
Manifestación de que se ha reflejado esta brecha internamente y se ha modificado el protocolo de envío de premios, para que los envíos pasen siempre por la central para reempaquetarse cuando se tengan que reenviar, informando de ello a los empleados y a los proveedores de mensajería.

Con fecha del 22 de julio de 2021, se envía un requerimiento de información a la parte reclamada, y se da un plazo de diez días hábiles para contestar, constando su recepción el mismo día 22 de julio de 2021. Tras enviar un correo electrónico al DPD, advirtiendo de que ha transcurrido el plazo de contestación el día 9 de agosto de 2021, se recibe un escrito de contestación a este requerimiento de información, en nombre de la parte reclamada, con entrada en la AEPD el 18 de agosto de 2021, en el que se aporta, entre otra, la siguiente información:
Manifestación, respecto a las medidas de seguridad implantadas con anterioridad a los hechos denunciados, de que, entre otras, se disponía de las siguientes medidas: los responsables de cada área tienen acceso al software de protección de datos, que incluye, entre otras cosas, el RAT, los protocolos de ejercicios de derecho y brechas de seguridad y el registro de incidentes; sólo el personal autorizado de cada departamento tiene acceso a los datos personales de los ganadores de los premios; existencia de un protocolo para las devoluciones de premios.
Manifestación de que, en este caso, la causa del incidente denunciado fue un error en el cruce de mensajería debido a la intención de agilizar el proceso de envío del premio al ganador, y debido a que este tipo de campañas no se realizan con asiduidad.
Manifestación de que, con el objeto de evitar que se produzcan incidentes similares, se ha ampliado y aclarado el protocolo para las devoluciones de premios, y se ha comunicado a empleados y proveedores.
Informe sobre la brecha de seguridad, en el que se detallan los mismos hechos detallados en el escrito recibido en la AEPD el 10 de junio de 2021 y se detallan las siguientes medidas tomadas:

Dejar reflejada la brecha internamente.
Informar al otro afectado.
Pedir la destrucción de los datos indebidamente comunicados.
Modificar el protocolo de envío de premios y comunicarlo a los empleados correspondientes y al proveedor. Se indica que esta medida se sustanció el día 6 de noviembre de 2020, en una llamada del consejero de la parte reclamada a los empleados de Marketing, Logística y Atención al Cliente, para informar del nuevo protocolo de envíos y la puesta a disposición de un documento con este nuevo protocolo; y en el envío de una copia del nuevo protocolo a la empresa de mensajería MRW el mismo día 6 de noviembre de 2020.
Videollamada de control de la aplicación del nuevo protocolo en el departamento de Marketing en febrero de 2021.
Copia del protocolo para el envío de premios y concursos con fecha de firma el 5 de noviembre de 2020. En este protocolo se observan, entre otras, la medida de que, si ha habido un error, el paquete debe ser devuelto al origen para ser empaquetado y enviado de nuevo.
Copia de una declaración sellada y firmada por la responsable de MRW Boadilla del Monte, con fecha de firma el 17 de agosto de 2021, en la que se confirma la recepción de la actualización del protocolo para el envío de premios del reclamado en la fecha del 6 de noviembre de 2020.
La parte reclamada alega la aplicación de los ejemplos sobre la valoración de la necesidad de notificar a la Autoridad de control que aparecen en el anexo B de las Directrices sobre la notificación de las violaciones de la seguridad de los datos, elaborada por el GT 29, y que también aparecen en las Directrices 01/2021 del Comité Europeo de Protección de Datos. También alega la aplicación del Reglamento General (UE) 2016/679 (en adelante, RGPD), que, en su artículo 33 hace referencia a la notificación de una violación de la seguridad de los datos personales a la autoridad de control. Manifiesta que el RGPD prevé, como excepción a esta obligación, que el responsable pueda garantizar, conforme al principio de responsabilidad proactiva, que sea improbable que dicha brecha constituya un riesgo para los derechos y libertades de las personas.
La parte reclamada alega la aplicación de la Guía para la Notificación de Brechas de Datos Personales, publicada por la AEPD en junio de 2021, en la que se hace referencia a los siguientes factores a tener en cuenta, entre otros en la evaluación del riesgo de una brecha: que el tipo de violación pueda afectar al nivel de riesgo que presente para las personas; la naturaleza, el carácter sensible y el volumen de datos personales; la gravedad de las consecuencias para las personas; y las características particulares.
Manifestación de que, en este suceso concreto, los datos que se han visto comprometidos son cuatro datos personales de contacto (nombre, apellidos, dirección y teléfono), que no pertenecen a categorías especiales ni a personas vulnerables, que la vulneración afecta a dos personas y que la actividad del responsable del tratamiento es el comercio de productos textiles; y, analizando estos tres parámetros, han determinado que no existe un alto nivel de riesgo de que la violación afecte negativamente a las personas y que es improbable que entrañe un alto riesgo para los derechos y las libertades de las personas.
Manifestación de que se mantuvo comunicación vía correo electrónico y teléfono con los dos afectados, en la que se les informó sobre el hecho, las medidas tomadas respecto a la mensajería y se les solicitó la destrucción del sobre donde aparecían los datos del otro afectado como remitente. También manifiestan que la madre del otro

afectado, que no es la parte reclamante, indicó por vía telefónica que ya se había desecho del sobre sin haber notado que apareciesen los datos de otra persona.

Manifestación de que, teniendo en cuenta estas circunstancias, la parte reclamada consideró que no era necesaria la notificación de la brecha de seguridad a la AEPD, pero sí se registró internamente, junto a las medidas adoptadas, en un registro de incidencias del software de privacidad, que el DPD tiene puesto a disposición de la parte reclamada.
Manifestación de que no han acontecido otros eventos análogos al denunciado en esta reclamación.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

II

El RGPD define, de un modo amplio, las "violación de la seguridad de los datos personales" (en adelante quiebra de seguridad) como "toda violación de la seguridad que ocasione 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."

III

El artículo 5.1.f) del RGPD, que recoge los "*Principios relativos al tratamiento*", dispone:
"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>)".

IV

"La seguridad del tratamiento" viene regulada en el artículo 32 del RGPD, que 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".

V

En el presente caso, consta que se produjo una quiebra de seguridad de datos personales en las circunstancias arriba indicadas (envío de un paquete en el que consta como remitente otro ganador del premio, que no es la parte reclamante).

El DPD, tras contactar con el otro ganador del premio y con MRW, que es la empresa de mensajería que hizo los envíos, ha llegado a la conclusión de que el otro ganador se deshizo del paquete del envío sin darse cuenta de la presencia de los datos personales y de que MRW trató los envíos como un intercambio entre los dos ganadores en vez de tratarlo como dos nuevos envíos. Los datos de los ganadores del concurso comunicados a MRW se limitaban a nombre, apellidos, dirección y teléfono.

La parte reclamada indica que se ha reflejado esta brecha internamente y se ha modificado el protocolo de envío de premios, para que los envíos pasen siempre por la central para reempaquetarse cuando se tengan que reenviar, informando de ello a los empleados y a los proveedores de mensajería.

Respecto a las medidas de seguridad implantadas con anterioridad a los hechos denunciados, entre otras, se disponía de las siguientes medidas: existencia de un protocolo para las devoluciones de premios.

La causa del incidente denunciado fue un error en el cruce de mensajería debido a la intención de agilizar el proceso de envío del premio al ganador.

Se ha ampliado y aclarado el protocolo para las devoluciones de premios, y se ha comunicado a empleados y proveedores.

Informe sobre la brecha de seguridad en el que se detallan las siguientes medidas tomadas:
Dejar reflejada la brecha internamente.
Informar al otro afectado.
Pedir la destrucción de los datos indebidamente comunicados.
Modificar el protocolo de envío de premios y comunicarlo a los empleados correspondientes y al proveedor. Se indica que esta medida se sustanció el día 6 de noviembre de 2020. En este protocolo se observan, entre otras, la medida de que, si ha habido un error, el paquete debe ser devuelto al origen para ser empaquetado y enviado de nuevo.

En este suceso concreto, los datos que se han visto comprometidos son cuatro datos personales de contacto (nombre, apellidos, dirección y teléfono), que no pertenecen a categorías especiales ni a personas vulnerables, que la vulneración afecta a dos personas.

Teniendo en cuenta todas las circunstancias, la parte reclamada consideró que no era necesaria la notificación de la brecha de seguridad a la AEPD, pero sí se registró internamente, junto a las medidas adoptadas, en un registro de incidencias del software de privacidad.

No han acontecido otros eventos análogos al denunciado en esta reclamación.

A la vista de lo expuesto, consta acreditado que los hechos no tienen un carácter continuado. El volumen de los tratamientos efectuados son los datos de dos personas. No hay vinculación de la actividad del investigado con la realización de tratamientos de datos de carácter personal, ya que es una empresa comercializadora al por menor de textiles. No se aprecian beneficios obtenidos como consecuencia de la comisión de los hechos investigados. Tampoco se aprecia intencionalidad. No consta reincidencia de infracciones de la entidad investigada en el último año. Se acredita que, con anterioridad a los hechos, el investigado tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal. Y han procedido a la regularización de la situación irregular de forma diligente.

Finalmente, se ha acreditado que la actuación de la parte reclamada, como entidad responsable del tratamiento, ha sido acorde con la normativa sobre protección de datos personales citada anteriormente.

Por tanto, conforme a lo señalado, la Directora de la Agencia Española de Protección de Datos, ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente Resolución a ACTURUS CAPITAL, S.L. y a D. ***A.A.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, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, los interesados podrán interponer, potestativamente, recurso de reposición ante la 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.

897-150719

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