- **Procedimiento Nº: E/00852/2021**

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: Como consecuencia de la notificación a la División de Innovación tecnológica de esta Agencia de una brecha de seguridad de datos personales por parte del Responsable del Tratamiento A. E. LLORENTE, S.A. con número de registro de entrada O00007128e2100002928 relativa al envío de datos personales a destinatarios erróneos, se ordena a la Subdirección General de Inspección de Datos que valore la necesidad de realizar las oportunas investigaciones previas con el fin de determinar una posible vulneración de la normativa de protección de datos.

SEGUNDO: A la vista de la citada notificación de quiebra de seguridad de los datos personales, la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación, teniendo conocimiento de los siguientes extremos:

ENTIDADES INVESTIGADAS

Durante las presentes actuaciones se han investigado las siguientes entidades:

AE LLORENTE S.A. con NIF A78267457

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1.- Con fecha 11 de febrero de 2021 se solicitó información a AE LLORENTE S.A. De la respuesta recibida se desprende lo siguiente:

Respecto de la cronología de los hechos. Acciones tomadas con objeto de minimizar los efectos adversos y medidas adoptadas para su resolución final.

19 de enero 2021: Un empleado, por error involuntario, envío un email a 509 clientes. En cuanto se dio cuenta activó la función de recuperación de email del Outlook, pero no informó a los responsables.

25 de enero de 2021: Toyota España se puso en contacto con la gerencia de la compañía, porque había recibido un email de una clienta informando de la incidencia. Se realizan las investigaciones internas oportunas y se analiza el alcance y el origen de la incidencia. Finalmente, se enviaron 434 emails que adjuntaban el fichero de clientes con el que estaba trabajando esta persona, tras haber activado la función de recuperación.

26 de enero 2021: Se realiza comunicación preliminar de Brecha de Confidencialidad a la Agencia Española de Protección de Datos.

29 de enero 2021: Se envía email a los clientes que podrían haber recibido el fichero informando de la incidencia y solicitando el borrado del fichero.

28 de enero 2021: Se envía email a los empleados recordando la necesidad de adoptar medidas de seguridad en el tratamiento de datos y realizar curso de formación online.

29 de enero de 2021: Se completa la comunicación realizada a la Agencia Española de Protección de Datos.

Respecto de las causas que hicieron posible la brecha

Error humano.

Respecto de los datos afectados.

El fichero que se envió contenía 6.900 registros con la siguiente tipología de datos: email, número de teléfono, datos del vehículo (matricula, bastidor, marca, modelo), datos sobre el servicio prestado (fecha, avería, importes, etc.).

No tienen constancia que haya habido consecuencias para los afectados. Sesenta y siete clientes que habían recibido el correo han respondido confirmando eliminación del archivo.

No se tiene ningún tipo de constancia y/o evidencia de la publicación de ninguno de los datos motivos de la brecha hayan sido publicados en internet. Se han realizado comprobaciones introduciendo emails de los contenidos en el fichero en Google, comprobando que el fichero no ha sido indexado.

Aportan copia del correo electrónico enviado a los destinatarios del correo que adjuntaba el fichero informando de la incidencia y solicitando el borrado del fichero.

Respecto de las medidas de seguridad implantadas

Aportan copia de un documento en el que se recogen los riesgos detectados en los tratamientos de datos y la valoración final que indica que es aceptable.

Información sobre la recurrencia de estos hechos y número de eventos análogos acontecidos en el tiempo.

Manifiestan que nunca anteriormente había sucedido algo similar en la empresa, no obstante, de manera correctiva, además del email enviado el día 28/02/2021 y de las charlas informales ya dadas a los empleados, se ha programado una nueva jornada de formación y sensibilización en torno a la protección de datos 29 de marzo 2021 a través de una consultora externa.

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 "violaciones de seguridad de los datos personales" (en adelante quiebra 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 que se produjo una quiebra de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como brecha de confidencialidad.

De la documentación aportada por la empresa en el curso de estas actuaciones de investigación (copia de un documento en el que se recogen los riesgos detectados en los tratamientos de datos y la valoración final que indica que es aceptable, copia de las funciones y obligaciones de los usuarios que acceden a datos de carácter personal y a los sistemas de información de la investigada., copia de la política de usos de medios tecnológicos) se desprende que, con anterioridad a producirse la brecha, la entidad investigada disponía de medidas de seguridad razonables en función de los posibles riesgos estimados.

En cuanto al impacto, se han visto vulnerados datos de contacto (email, nº de teléfono, DNI, datos del vehículo y del servicio prestado), siendo el volumen de registros afectados de 6.900. Asimismo, se ha enviado el fichero como adjunto en 434 correos.

No se tiene constancia de consecuencias para los afectados ni de la indexación o publicación en internet del fichero. Se ha enviado un correo electrónico a los receptores del fichero solicitando que procedan a su borrado.

Para evitar que estos hechos se repitan se ha enviado a todos los empleados un correo de recordatorio de usos informáticos GDPR, que llevaba como adjunto, la política de usos de medios tecnológicos, así como la programación de una jornada de formación y sensibilización en torno a la protección de datos.

En consecuencia, consta que disponía de medidas técnicas y organizativas razonables para evitar este tipo de incidencia. No obstante, y una vez detectada ésta, se produce una diligente reacción al objeto de notificar a la AEPD e implementar medias para eliminarla.

Por último, se recomienda elaborar un Informe Final sobre la trazabilidad del suceso y su análisis valorativo, en particular, en cuanto al impacto final. Este Informe es una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos y servirá para prevenir la reiteración de una brecha de similares características como la analizada.

III

Por lo tanto, se ha acreditado que la actuación de la entidad investigada como entidad responsable del tratamiento ha sido acorde con la normativa sobre protección de datos personales analizada en los párrafos anteriores.

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

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a AE LLORENTE S.A. con NIF A78267457

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.

940-0419

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