- **Procedimiento Nº: E/04518/2021**

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 ***A.A.A.*** (en adelante, el reclamante) tiene entrada con fecha 7 de septiembre de 2020 en la Agencia Española de Protección de Datos. La reclamación se dirige contra SILMARTEL XXI, S.L***.,*** con NIF ***B47648928*** (en adelante, el reclamado). La reclamación se basa en el envío a todos los miembros de la comunidad de una comunicación por email sin copia oculta, haciendo así visible las direcciones de correo. Junto a la reclamación aporta copia de la comunicación.

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/07935/2020, se dio traslado de dicha reclamación al reclamado, 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 reclamado pese a solicitar una ampliación de plazo, que le es concedida, no remite contestación alguna a esta Agencia.

TERCERO**:** Con fecha 15 de marzo de 2021, la Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada por el reclamante.

CUARTO: 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:

ANTECEDENTES

Fecha de entrada de la reclamación: 7 de septiembre de 2020

Reclamante: ***A.A.A.*** (en adelante, el reclamante)

Reclamado: SILMARTEL XXI, S.L. (en adelante, el reclamado).

Según la información obtenida ("*Diligencia Info Sociedad*") del servicio Axesor su tamaño es *"PYME (Microempresa*)" y las cuentas del último ejercicio presentadas en el Registro Mercantil corresponden al año 2009.

Hechos según manifestaciones del reclamante:

El reclamante pone de manifiesto (número de registro de entrada O00007128e2000001137) que el administrador de fincas "*en nombre de la Asesoría SILMARTEL XXI S.L" envío, con fecha de 29 de mayo de 2020, un correo electrónico a los propietarios de la comunidad sin utilizar el sistema de "copia oculta*"

Documentación relevante aportada por el reclamante:

- Copia del correo electrónico enviado con fecha de 29 de mayo de 2020 y asunto "COMUNICADO PISCINA PUERTA DEL GOLF" desde la cuenta de correo electrónico administracion@silmartel.com en el que se comunican las condiciones de apertura de la piscina de la comunidad. La lista, de 68 destinarios, incluye para cada uno de ellos la dirección de correo electrónico y el nombre asociado en la agenda del remitente a cada destinatario (valor que, para casi todos los casos, comprende el nombre y los apellidos del mismo).

Antecedentes del reclamado en el sistema de información (SIGRID) de la AEPD:

En el marco del procedimiento E/07935/2020 la AEPD, en virtud del artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, dio traslado de la reclamación al reclamado solicitando información en relación con el incidente. No habiendo obtenido la información necesaria para esclarecer los hechos, la AEPD acordó, con fecha de 15 de marzo de 2021, la admisión a trámite de la reclamación presentada.

ENTIDADES INVESTIGADAS

Durante las presentes actuaciones se han investigado las siguientes entidades:

SILMARTEL XXI, S.L. con NIF B47648928 con domicilio en JUAN MARTÍNEZ VILLERGAS, 12, ENTREPLANTA, OFI. 4 - 47014 VALLADOLID (VALLADOLID)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

Sirva este apartado para resumir el resultado de las presentes actuaciones. Toda la información aquí citada obra bajo el número de expediente que titula este informe. En concreto, las referencias al escrito del reclamado han de entenderse realizadas al registrado de entrada en la AEPD el día 9 de junio de 2021 con el número O00007128e2100025795. Así, el reclamado realiza las siguientes manifestaciones en relación con los hechos objeto del presente informe:

Sobre las causas del incidente:

"La razón de porqué se envió el correo sin copia oculta fue un error humano achacable a mi persona, debido a las urgencia [sic] por notificar la apertura de la piscina en la Comunidad."

Sobre el procedimiento establecido:

"El procedimiento usual para este tipo de comunicaciones es copia oculta, en nuestra oficina se envían numerosos correos a varias personas, y es el procedimiento establecido".

Sobre las acciones tomadas para resolver el incidente:

"Las acciones que tomaremos para la próxima vez que ocurra será volver a enviar un nuevo correo a todos con copia oculta, indicando que anulen el correo.

Por otro lado los trabajadores de la empresa lo tienen claro que ese es el procedimiento a seguir."

Sobre el motivo por el que no se ha notificado previamente a la AEPD:

"Entendíamos que no se había producido una brecha de seguridad hasta recibir el requerimiento. Y tampoco tenemos constancia de haber enviado más correos de esta manera."

Sobre la existencia de incidentes análogos:

"No tenemos conocimiento de haber envidado mas [sic] correos de esta forma."

Sobre las medidas técnicas y organizativas para evitar incidentes análogos en el futuro:

"En este sentido, hemos adoptado las siguientes:

- reunión con los empleados, para recordar y reforzar la importancia del tratamiento de datos personales de forma diligente, haciendo especial referencia a la utilización de la opción de copia oculta en el envío de comunicaciones dónde haya más de un destinatario.

- remitir por escrito las instrucciones/procedimiento para el envío de información a las comunidades de propietarios (haciendo especial referencia a la utilización de la opción de copia oculta en el envío de comunicaciones dónde haya más de un destinatario).

- remitir un recordatorio periódico (p. ej. mensual) al personal para recordar la importancia de tratar los datos personales de los comuneros con las adecuadas precauciones.

- formaciones en materia de privacidad o protección de datos personales."

No consta documentación adjunta al escrito O00007128e2100025795.

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

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

Artículo 32

"Seguridad del tratamiento

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".

La empresa afirma que previamente a la brecha, ya tenía establecido, como procedimiento habitual para el envío de este tipo de comunicaciones, el uso de copia oculta. Por ello se puede concluir que contaba con medidas de seguridad razonables.

La brecha se produjo por un error humano motivado por la urgencia para notificar la apertura de la piscina.

En cuanto al impacto, se han visto afectados 68 personas siendo los datos expuestos, la dirección de correo electrónico y el nombre asociado a cada destinatario, en la agenda del remitente (que en la mayoría de los casos se corresponde con el nombre y los apellidos).

Para evitar que estos hechos se repítan la reclamada realiza una reunión con los empleados para reforzar la importancia del tratamiento de datos personales de manera diligente y donde se hace especial referencia al uso de la opción de copia oculta en el envío de comunicaciones. Asimismo se procede a remitir por escrito las instrucciones para el envío de información a las comunidades de propietarios. Así como la emisión de recordatorios periódicos al personal sobre la importancia de tratar los datos personales con las adecuadas precauciones.

En consecuencia, tal como demuestra el hecho de que no exista constancia de que se hayan producidos más envíos sin copia oculta, consta que disponía de medidas técnicas y organizativas razonables para evitar este tipo de incidencia.

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 del reclamado 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 ***A.A.A.*** y a SILMARTEL XXI, 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, 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