- **Expediente N.º: EXP202408273**

IMI S/Ref.: 804000; Case Register: 816468

RESOLUCIÓN DE CADUCIDAD DE ACTUACIONES

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

HECHOS

PRIMERO**:** Con fecha 17 de mayo de 2024, **GEOPOST ESPAÑA, S.L.**, con NIF **B85645349** (en adelante, GEOPOST o SEUR) notificó a esta Agencia una brecha de datos personales.

Los hechos que se pusieron en conocimiento de esta autoridad fueron los siguientes:

"El 13 de mayo a las 01.00h, se detectó un acceso no autorizado a nuestros sistemas. A pesar de contar con medidas de seguridad adecuadas y herramientas que nos permiten parchear vulnerabilidades de manera proactiva y efectiva, hemos sufrido este incidente. Con los análisis forenses realizados, el 15 de mayo a las 17.00h, se tiene la certeza de que ha afectado a datos personales relativos a expediciones internacionales. Los datos comprometidos son los necesarios para la prestación del servicio de transporte: Nombre, apellidos, dirección postal y de correo electrónico y teléfono. En una valoración inicial, se estima que aproximadamente 22.000.000 de registros han sido comprometidos. En cumplimiento con nuestras obligaciones legales y en un esfuerzo por mitigar cualquier impacto negativo, hemos notificado igualmente al Instituto Nacional de Ciberseguridad (INCIBE) y a las Fuerzas y Cuerpos de Seguridad del Estado."

SEGUNDO: Como consecuencia de los hechos conocidos, con fecha 30 de mayo de 2024 la Directora de la Agencia Española de Protección de Datos ordenó a la Subdirección General de Inspección de Datos (SGID) realizar las oportunas investigaciones previas con el fin de determinar una posible vulneración de la normativa de protección de datos.

TERCERO: A través del "Sistema de Información del Mercado Interior" (en lo sucesivo Sistema IMI), regulado por el Reglamento (UE) nº 1024/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012 (Reglamento IMI), cuyo objetivo es favorecer la cooperación administrativa transfronteriza, la asistencia mutua entre los Estados miembros y el intercambio de información, se transmitió la citada cuestión con el resto de las autoridades de control el día 14 de agosto de 2025. El traslado de esta cuestión por la AEPD se realiza, teniendo en cuenta su carácter transfronterizo y que esta Agencia es competente para actuar como autoridad de control principal, de conformidad con lo establecido en el artículo 56 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27/04/2016, 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 (en lo sucesivo, RGPD), dado que SEUR tiene su establecimiento único o principal en España.

Los tratamientos de datos que se llevan a cabo afectan a interesados en varios Estados miembros. Según las informaciones incorporadas al Sistema IMI, de conformidad con lo establecido en el artículo 60 del RGPD, actúa en calidad de "autoridad de control interesada" las autoridades de Finlandia, Países Bajos, Suecia, Austria, Estonia, Eslovenia, Dinamarca, Rumanía, Bélgica, Irlanda, Francia e Italia, y las autoridades alemanas de protección de datos de Hesse, Baja Sajonia, Baden-Wurtemberg, Renania-Palatinado, Berlín, Mecklemburgo-Pomerania Occidental y Baviera. Todas ellas en virtud del artículo 4.22 del RGPD, dado que los interesados que residen en el territorio de estas autoridades de control es probable que se vean sustancialmente afectados por el tratamiento objeto del presente procedimiento.

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 las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del RGPD, y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), teniendo conocimiento de los siguientes extremos:

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

SEUR informa en su escrito de 25 de octubre de 2024 a esta Agencia que, en el momento del incidente, se adoptaron las siguientes medidas:

> ***"(…)"***

E indican en el escrito mencionado que "para garantizar la eficacia de las medidas técnicas y organizativas ya desplegadas y las que se implantaron posteriormente, SEUR ha realizado las siguientes mejoras:

> ***- (…)***

SEUR informa que ha realizado una valoración de brecha inicial con su herramienta corporativa y también con la herramienta Asesora Brecha de la AEPD online para comprobar si era necesario notificar la brecha a la AEPD. Se aporta una copia de este informe fechado el 16 de mayo de 2024 a las 10:41 horas con el siguiente resultado: "EL RESPONSABLE DEBE NOTIFICAR SIN DILACIÓN INDEBIDA LA BRECHA DE DATOS PERSONALES A LA AEPD (O LA AUTORIDAD DE PROTECCIÓN DE DATOS COMPETENTE", y en el que se indica que se deben tomar las siguientes medidas:

> "- Notificar la brecha de datos personales a la AEPD mediante el formulario de notificación de brecha de datos personales en la Sede Electrónica
> - Comunicar la brecha a las personas afectadas conforme al artículo 34 del RGPD si el riesgo a alto. Obtenga asesoramiento sobre la obligación de comunicar a las personas afectadas mediante la herramienta Comunica—Brecha RGPD

- Tomar medidas para mitigar los posibles efectos provocados por la brecha y documentada conforme al artículo 33.5 del RGPD, incluyendo los hechos relacionados con la brecha, sus efectos y las medidas adoptadas."

Sobre estos informes, SEUR manifiesta en su escrito de 25 de octubre de 2024 lo siguiente:

> "se determinó que dado el volumen de afectados la brecha podría suponer un alto riesgo para los derechos y libertades de los interesados y se procedió a notificar de forma inicial la brecha en fecha 17 de mayo de 2024. Por otro lado, tal y como se trasladó a la AEPD en la notificación inicial, el 21 de mayo dado el esfuerzo desproporcionado que supondría para SEUR notificar a cada uno de los interesados dado el alto volumen de afectados, se optó por llevar a cabo un comunicado público a través de la web de SEUR España."

Con fecha de 12 de junio de 2024, se publicó en el sitio web de SEUR, dentro de la sección "Información de interés" ((...)) el siguiente comunicado:

> "*Geopost anuncia haber identificado un incidente de ciberseguridad consistente en un acceso reciente no autorizado a una base de datos operada por su filial en España.*
> *Tras tener conocimiento del incidente, la compañía informó proactivamente al Instituto Nacional de Ciberseguridad (INCIBE) y a la Agencia Española de Protección de Datos (AEDP) e inició rápidamente una investigación junto con los expertos en ciberseguridad.*
> *Esta investigación permite confirmar que los datos comprometidos se limitan a los necesarios para la prestación del servicio de transporte, es decir, nombre, apellidos, dirección postal, dirección de correo electrónico y, en determinados casos, número de teléfono.*
> *Geopost también confirma haber tomado, con su filial española, todas las medidas necesarias para gestionar el incidente y mitigar su impacto, garantizando que nuestra respuesta ha sido inmediata y nuestro sistema de seguridad reforzado. Más específicamente, estas medidas incluyen una variedad de acciones de seguridad como renovaciones de contraseñas, formateo de dispositivos afectados, mejoras en la seguridad de la red, monitoreo en tiempo real y mejoras en la automatización de la respuesta a eventos sospechosos para proteger nuestros sistemas e información.*
> *Este hecho, que no es una situación de ransomware, puede dar lugar al uso de los datos robados para intentos de spam o phishing. Por lo tanto, invitamos a nuestros clientes remitentes o receptores a aumentar su nivel de precaución con respecto a correos electrónicos o llamadas telefónicas sospechosas de contactos desconocidos.*
> *Los interesados pueden contactar con el Delegado de Protección de Datos de Geopost España SL a través de la dirección de correo electrónico (...) para resolver sus dudas, ampliar la información disponible o recibir consejos útiles*."

SEUR, en su escrito presentado ante la AEPD el 14 de junio de 2024, indica que su intención es realizar este comunicado en los sitios web de sus filiales en los siguientes países de la Unión Europea (además de España): Francia, Alemania, Italia, Países Bajos, Bélgica, Portugal, Polonia, Austria, Irlanda, República Checa, Luxemburgo, Hungría, Lituania, Eslovaquia, Eslovenia, Grecia, Rumanía, Letonia, Estonia, Croacia y

Bulgaria. Y se aportan evidencias de esta publicación traducida al idioma local en sitios web de Francia, Italia, Austria, Polonia, Eslovenia, Eslovaquia, República Checa, Lituania y Croacia.

Respecto a la forma de comunicación realizada por un comunicado publicado en su sitio web, y no mediante comunicación directa con los afectados a través de correo electrónico o llamada telefónica, SEUR declara los siguiente:

> "*El motivo acerca del cual no se ha comunicado la brecha a los afectados vía correo electrónico o teléfono es porque no se disponía de los datos de contacto de todos los afectados y, dado el volumen de los mismos se consideró que era un esfuerzo desproporcionado para SEUR realizar dicha comunicación de forma individualizada. Por este motivo, SEUR optó por llevar a cabo un comunicado público a través de la web de SEUR España realizado con fecha 21 de mayo de 2024. También es necesario destacar que, el 30 de mayo de 2024, SEUR recibió una resolución de la AEPD instándole a hacer extensible la medida de publicar el comunicado en la web de SEUR al resto de interesados afectados en otros países, para dar cumplimiento a la obligación de notificación del incidente a los afectados conforme al artículo 34 del RGPD. Por tanto, el 14 de junio de 2024, se procedió a dar respuesta a la resolución de la AEPD, evidenciando el texto del comunicado, el enlace al comunicado final efectuado en la web de SEUR España, así como las evidencias de comunicaciones efectuadas en las diferentes webs de las filiales del Grupo en los países de la UE, en el propio idioma del país, para que la medida fuera igualmente efectiva para todos los interesados afectados*."

SEUR también declara que "se han recibido varios comunicados de clientes solicitando información sobre la brecha y, SEUR con aras de cumplir con sus obligaciones y como muestra de su responsabilidad proactiva, ha respondido a cada uno de ellos con la información relativa a la brecha." Y aporta una impresión de la respuesta dada a dos empresas clientes de SEUR en las que, a una se la informa de que no ha tenido afectados debido a que no ha realizado ningún envío internacional, y a la otra se la informa de que ha tenido 5000 destinatarios afectados, de los que se han visto comprometidos lo datos nombre, apellidos, dirección postal, dirección de correo electrónico, y en determinados casos, número de teléfono, y se informa de las medidas de seguridad aplicadas para intentar evitar ataques similares en un futuro, las cuales incluyen las siguientes medidas:

> ***"(…)"***

2) Respecto de las causas que hicieron posible la brecha, en el apartado primero, "*Copia del informe elaborado y documentación acreditativa en relación con la brecha notificada*", del escrito de SEUR de 25 de octubre de 2024 a esta Agencia, se señala lo siguiente:

> ***(…)***

3) Respecto de los datos afectados:

En su escrito de 25 de octubre de 2024, SEUR señala que corresponden a datos de envíos realizados al extranjero, de los que se han obtenido los siguientes datos de los destinatarios: Nombre, apellidos, dirección postal y de correo electrónico y, en algunos casos, número de teléfono.
Y SEUR indica que "En cuanto al volumen final de afectos por país, teniendo en cuenta que el volumen total de personas afectadas es de 22.000.000 personas, es el siguiente: en España 12927139 personas, en Alemania 1353079 personas, en Bulgaria 8462 personas, en Dinamarca 58782 personas, en Eslovenia 17183 personas, en Reino Unido 72955 personas, en Irlanda 80075 personas, en Lituania 29620 personas, en Países Bajos 524691 personas, en República Checa 46848 personas, en Austria 176106 personas, en Chipre 600 personas, en Francia 5437918 personas, en Estonia 12439 personas, en Grecia 14365 personas, en Italia 1058115 personas, en Luxemburgo 44935 personas, en Polonia 198908 personas, en Rumanía 13199 personas, en Bélgica 446385 personas, en Croacia 9120 personas, en Eslovaquia 25692 personas, en Finlandia 19160 personas, en Hungría 36106 personas, en Letonia 12906 personas, en Malta 570 personas, en Portugal 307326 personas y en Suecia 65158 personas."

4) Respecto de las medidas de seguridad implantadas:

Medidas de seguridad implantadas con anterioridad a la brecha en los tratamientos de datos donde se ha producido.

Aportan a su escrito de 25 de octubre de 2024 como Anexo XII un "Extracto Análisis de riesgos (AR) realizados sobre la actividad de tratamiento que ha sufrido la brecha de seguridad" y como Anexo XIII, la "*Copia de la Evaluación de Impacto para la Protección de Datos personales (EIPD) de la actividad de tratamiento afectada por la brecha*" fechada el 20 de septiembre de 2023.

De acuerdo con las manifestaciones de SEUR en el apartado 7 de su escrito de 25 de octubre de 2024, tenían implantadas las siguientes herramientas:

- (…)

En el Anexo I a su escrito de 25 de octubre de 2024, "*Copia del informe elaborado y documentación acreditativa en relación con la brecha notificada"*, se contemplan las siguientes medidas técnicas y organizativas adoptadas para evitar incidentes como el sucedido:

(…)

QUINTO: Con fecha 23 de noviembre de 2025, la Presidencia de la AEPD adoptó un proyecto de resolución de archivo de actuaciones. Siguiendo el proceso establecido en el artículo 60 del RGPD, al día siguiente se transmitió a través del sistema IMI el citado proyecto y se les hizo saber a las autoridades interesadas que tenían cuatro semanas desde ese momento para formular objeciones pertinentes y motivadas. El plazo de tramitación de las actuaciones quedó suspendido automáticamente durante estas cuatro semanas, de acuerdo con lo dispuesto en el artículo 64 de la LOPDGDD.

Dentro del plazo a tal efecto, las autoridades de control interesadas no presentaron objeciones pertinentes y motivadas al respecto, por lo que se considera que todas las autoridades están de acuerdo con dicho proyecto y están vinculadas por éste, de conformidad con lo dispuesto en el apartado 6 del artículo 60 del RGPD.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) confiere a cada autoridad de control y según lo dispuesto en los artículos 47 y 48.1 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 Presidencia 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
Sistema de Información del Mercado Interior (IMI)

El Sistema de Información del Mercado Interior se encuentra regulado por el Reglamento (UE) nº 1024/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012 (Reglamento IMI), y su objetivo es favorecer la cooperación administrativa transfronteriza, la asistencia mutua entre los Estados miembros y el intercambio de información.

III
Establecimiento principal, tratamiento transfronterizo y autoridad de control principal

El artículo 4.16 del RGPD define «establecimiento principal»:

“a) en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal;
b) en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas

con arreglo al presente Reglamento"

Por su parte el artículo 4.23 del RGPD considera «tratamiento transfronterizo»:

"a) el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o
b) el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro"

El RGPD dispone, en su artículo 56.1, para los casos de tratamientos transfronterizos, previstos en su artículo 4.23), en relación con la competencia de la autoridad de control principal, que, sin perjuicio de lo dispuesto en el artículo 55, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento será competente para actuar como autoridad de control principal para el tratamiento transfronterizo realizado por parte de dicho responsable o encargado con arreglo al procedimiento establecido en el artículo 60.

En el caso examinado, la reclamada tiene su establecimiento principal en España, por lo que la Agencia Española de Protección de Datos es la competente para actuar como autoridad de control principal.

IV
Autoridad de control interesada

De conformidad con lo dispuesto en el artículo 4.22) del RGPD, es "autoridad de control interesada", *"la autoridad de control a la que afecta el tratamiento de datos personales debido a que:*

a) el responsable o encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control;
b) los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o
c) se ha presentado una reclamación ante esa autoridad de control"

V
Seguridad del tratamiento

El artículo 32 del RGPD estipula lo siguiente:

"*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, en el momento de producirse la brecha de seguridad, no consta que SEUR no dispusiese de medidas de seguridad razonables en función de los posibles riesgos estimados. De acuerdo con los informes presentados por SEUR, la brecha de seguridad se produjo por un ataque que combinaba varias herramientas mediante una amenaza avanzada persistente, con un malware hecho a medida, por lo que no era una vulnerabilidad publicada en las bases de datos de vulnerabilidades y no existían soluciones para dicho ataque. Circunstancias que, en caso de existir, podrían haber supuesto indicios de infracción por parte del responsable del tratamiento. Así, de acuerdo con las manifestaciones de SEUR en el apartado 7 de su escrito de 25 de octubre de 2024, tenían implantadas las siguientes herramientas:

- (…)

Asimismo, SEUR tomó las siguientes medidas en respuesta al incidente según el escrito mencionado:

"(…)"

Todo ello sin perjuicio de que en su escrito de 25 de octubre de 2024 también indican que ***"(…)."***

En consecuencia, no existen evidencias de que no se hayan tomado las medidas adecuadas al nivel de riesgo del tratamiento antes de que se produjera el ataque.

VI

Comunicación de una violación de la seguridad de los datos personales al interesado

La comunicación de una violación de la seguridad de los datos personales al interesado está regulada en el artículo 34 del RGPD, según el cual:

"*1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.*
2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).
3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:
a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;
b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;
c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.
4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3."

SEUR efectuó una publicación de la violación de la seguridad de los datos personales de los interesados mediante una noticia en la sección de "Información de interés" de su sitio web (***(...)***) en español y en su versión en inglés. De acuerdo con las investigaciones realizadas por esta Agencia, dicha publicación se efectuó en su sitio web con fecha de 12 de junio de 2024. El contenido de esta publicación es el siguiente:

> "*Geopost anuncia haber identificado un incidente de ciberseguridad consistente en un acceso reciente no autorizado a una base de datos operada por su filial en España.*
> *Tras tener conocimiento del incidente, la compañía informó proactivamente al Instituto Nacional de Ciberseguridad (INCIBE) y a la Agencia Española de Protección de Datos (AEDP) e inició rápidamente una investigación junto con los expertos en ciberseguridad.*
> *Esta investigación permite confirmar que los datos comprometidos se limitan a los necesarios para la prestación del servicio de transporte, es decir, nombre, apellidos, dirección postal, dirección de correo electrónico y, en determinados casos, número de teléfono.*
> *Geopost también confirma haber tomado, con su filial española, todas las medidas necesarias para gestionar el incidente y mitigar su impacto,*

garantizando que nuestra respuesta ha sido inmediata y nuestro sistema de seguridad reforzado. Más específicamente, estas medidas incluyen una variedad de acciones de seguridad como renovaciones de contraseñas, formateo de dispositivos afectados, mejoras en la seguridad de la red, monitoreo en tiempo real y mejoras en la automatización de la respuesta a eventos sospechosos para proteger nuestros sistemas e información.

Este hecho, que no es una situación de ransomware, puede dar lugar al uso de los datos robados para intentos de spam o phishing. Por lo tanto, invitamos a nuestros clientes remitentes o receptores a aumentar su nivel de precaución con respecto a correos electrónicos o llamadas telefónicas sospechosas de contactos desconocidos.

Los interesados pueden contactar con el Delegado de Protección de Datos de Geopost España SL a través de la dirección de correo electrónico ***(...)*** *para resolver sus dudas, ampliar la información disponible o recibir consejos útiles*."

La AEPD, el 30 de mayo de 2024, solicitó a SEUR que se comunicara el incidente de seguridad a los afectados en el resto de los países. En su escrito de 14 de junio de 2024, SEUR indica que va a realizar la publicación en los sitios web de GEOPOST en el resto de los países de la Unión Europea donde hay afectados por la brecha, y aporta evidencias de su publicación en los sitios web de las filiales de GEOPOST en Francia, Italia, Austria, Polonia, Eslovenia, Eslovaquia, República Checa, Lituania y Croacia.

SEUR declaró que "*el motivo acerca del cual no se ha comunicado la brecha a los afectados vía correo electrónico o teléfono es porque no se disponía de los datos de contacto de todos los afectados y, dado el volumen de los mismos se consideró que era un esfuerzo desproporcionado para SEUR realizar dicha comunicación de forma individualizada."* Considerando que se estima que aproximadamente 22.000.000 de registros han sido comprometidos, y atendiendo a lo previsto en el artículo 34.3.c del RGPD, se entiende que la obligación de comunicar la violación de la seguridad de los datos personales a los interesados queda válidamente cumplida mediante la publicación de un comunicado en la página web de SEUR.

VIII
Caducidad de las actuaciones previas de investigación

El artículo 67 de la LOPDGDD determina lo siguiente, respecto a las actuaciones previas de investigación:

"1. Antes de la adopción del acuerdo de inicio de procedimiento, y una vez admitida a trámite la reclamación si la hubiese, la Agencia Española de Protección de Datos podrá llevar a cabo actuaciones previas de investigación a fin de lograr una mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento.

La Agencia Española de Protección de Datos actuará en todo caso cuando sea precisa la investigación de tratamientos que implique un tráfico masivo de datos personales.

2. Las actuaciones previas de investigación se someterán a lo dispuesto en la Sección 2.ª del Capítulo I del Título VII de esta ley orgánica y no podrán tener una duración superior a dieciocho meses a contar desde la fecha del acuerdo de admisión a trámite o de la fecha del acuerdo por el que se decida su iniciación cuando la Agencia Española de Protección de Datos actúe por propia iniciativa o como consecuencia de la comunicación que le hubiera sido remitida por la autoridad de control de otro Estado miembro de la Unión Europea, conforme al artículo 64.3 de esta ley orgánica."

Por su parte, el Reglamento de desarrollo de la LOPD (RLOPD), aprobado por Real Decreto 1720/2007, de 21 de diciembre, en vigor en todo aquello que no contradiga, se oponga o resulte incompatible con lo dispuesto en el RGPD y en la LOPDGDD, en su artículo 122.4 dispone que *"El vencimiento del plazo sin que haya sido dictado y notificado acuerdo de inicio de procedimiento sancionador producirá la caducidad de las actuaciones previas*".

A tenor de lo dispuesto en los artículos transcritos, las actuaciones previas han de entenderse caducadas si, transcurridos más de dieciocho meses contados desde la fecha de su iniciación, no se ha procedido a dictar y notificar el acuerdo de inicio de procedimiento sancionador.

En el presente supuesto el cómputo de los dieciocho meses de duración máxima de las actuaciones previas se inició el día 30 de mayo de 2024, por lo que deben declararse caducadas.

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

PRIMERO: DECLARAR la CADUCIDAD de las presentes actuaciones previas de investigación.

SEGUNDO: NOTIFICAR la presente Resolución a GEOPOST ESPAÑA, S.L. y a la parte reclamante.

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 Presidencia 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.

907-271125

Lorenzo Cotino Hueso
Presidente de la Agencia Española de Protección de Datos