- **Expediente Nº: E/06661/2021**

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: D. ***A.A.A.*** (en adelante, el RECLAMANTE) con fecha 8 de abril de 2021 interpuso reclamación ante la AEPD. La reclamación se dirige contra **TRILLO & VALIENTE NOTARIOS S.C.P** con CIF J88302575 (en adelante, la NOTARÍA).

Los motivos en que basa la reclamación son los siguientes:

Con fecha de 24 de enero de 2018 el reclamante se puso en contacto con la NOTARÍA al objeto de realizar un trámite, a través de correo electrónico, facilitando una serie de datos de carácter personal ("Nombre, Apellidos, Fotocopia de DNI, justificante de ingreso de provisión de fondos […]mi número de teléfono móvil").

Con fecha de 5 de enero de 2021 a las 8:35 horas recibió un correo electrónico con origen en una dirección que le resulta desconocida (******EMAIL.1***) con el asunto "Adjunto certificado con el nombre nuevo. ***Contraseña: ***CONTRASEÑA.1***" y un archivo adjunto que manifiesta no haber descargado. El cuerpo de este correo contiene el contenido literal de dos correos enviados el 24 de enero de 2018 por la NOTARÍA que incluyen sus datos personales ("Nombre, Apellidos, DNI, número de móvil, email y copia en imagen de mi DNI"). El reclamante identifica el origen de este correo electrónico con una notaría de ******PROVINCIA.1*** (***B.B.B.***).

- Con posterioridad, el mismo día 5 de enero de 2021 a las 11:31 horas recibió un correo electrónico con origen en una dirección que le resulta desconocida (******EMAIL.2***) con el asunto "Re: Solicitud de copia autorizada de testamento" y el adjunto "report.-zip"."Zip file attached to email: report.zip Password: ******PASSWORD.1***" y un archivo adjunto que manifiesta no haber descargado. Según señala, el cuerpo de este correo contiene el mismo contenido literal que el referido en el párrafo anterior procedente de dos correos intercambiados con la NOTARÍA.

- El RECLAMANTE manifiesta haber comunicado telefónicamente a la NOTARÍA y a la notaría de ******PROVINCIA.1*** lo ocurrido, indicándole que "han sido infectados por un virus y que su informático está revisándolo" ante lo cual les solicita que se pongan en contacto con él para conocer "hasta donde han llegado los daños y determinar cuanta información mía les han podido robar".

Si bien, es cierto que ninguna de ellas se ha puesto en contacto con el RECLAMANTE.

Además, el RECLAMANTE, de un tiempo a esta parte, ha recibido mensajes de empresas de capital riesgo, inversiones y criptomonedas, que le inducen a pensar que sus datos personales han podido ser accedidos de forma no autorizada y podrían haberse divulgado por internet.

Junto a la reclamación se aporta:

- Copia de los correos electrónicos intercambiados entre el reclamante (******EMAIL.3*** y la NOTARÍA (“***C.C.C.” ***EMAIL.4***) los días 24 y 25 de enero de 2018 bajo el asunto “Solicitud de copia autorizada de testamento”. En el cuerpo de estos correos figuran los siguientes datos personales del RECLAMANTE: nombre, apellidos, número de DNI, y número de teléfono móvil. Además, se refieren adjuntos que consignarían la imagen digitalizada de su DNI y el justificante de provisión de fondos para la realización del trámite.
- Copia del correo electrónico recibido por el reclamante (******EMAIL.3*** el día 5 de enero de 2021 a las 8:35 horas, procedente de “***C.C.C.***” (******EMAIL.1***) con el asunto “RV: certificado” y el adjunto “certificado.zip”. El cuerpo del mensaje incluye el texto “[…] Adjunto certificado con el nombre nuevo. Contraseña: ******CONTRASEÑA.1*** […] ***C.C.C.***” y, a continuación, la cadena de mensajes precedentes.
  Estos últimos se corresponden con correos intercambiados el día 24 de enero de 2018 entre reclamante y la NOTARÍA.
- Copia del correo electrónico recibido por el reclamante (******EMAIL.3***el día 5 de enero de 2021 a las 11:31 horas, procedente de “***C.C.C.***” (******EMAIL.2***) con el asunto “Re: Solicitud de copia autorizada de testamento” y el adjunto “report.zip”. El cuerpo del mensaje incluye el texto “Re: Solicitud de copia autorizada de testamento Zip file attached to email: report.zip Password: ******PASSWORD.1 C.C.C.***” y, a continuación, la cadena de mensajes precedentes.
  Estos últimos se corresponden con correos intercambiados el día 24 de enero de 2018 entre RECLAMANTE y la NOTARÍA, copia del mensaje enviado por la NOTARÍA, de fecha 29 de diciembre de 2020.

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 la NOTARIA, 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.

La notificación del traslado de la reclamación se llevó a cabo, a través del e del Servicio de Notificaciones Electrónicas y Dirección Electrónica Habilitada, constando su aceptación en fecha 29 de abril de 2021.

TERCERO: Con fecha 31 de mayo de ese mismo año, la NOTARÍA contesta al traslado en los siguientes términos:

Manifiesta que no existen indicios de que la captura de los datos referidos por el RECLAMANTE haya tenido lugar en sus equipos informáticos y no en los del RECLAMANTE.

Niega haberle manifestado al RECLAMANTE que hubiera sido infectado por un virus informático.

Si bien, “lo que se pudo informar a dicho cliente y a otros varios clientes habituales del despacho es que nosotros mismos y una infinidad de usuarios de Outlook, a nivel mundial, estábamos siendo atacados (no infectados) por ese tipo de correos que, simulando proceder de contactos habituales y reproduciendo -total o parcialmente antiguos correos cruzados (si bien con diferente calibre y tipo de letra y espacio de interlineado), eran sin embargo cuentas absolutamente desconocidas para nosotros, teniendo, como él mismo, la precaución de no abrirlos.”

Añade que “ese ataque masivo no fue comunicado a la AEPD dado que, de haberlo hecho nosotros (respecto de los correos de ese tipo recibidos) y el resto de los afectados, sin duda se habría colapsado la Agencia. Simplemente tomamos las medidas y precauciones que a continuación se relatarán.”

Facilita información relativa al ataque sufrido indicando, no obstante, que ello no implica “en absoluto el reconocimiento de su vinculación con lo ocurrido al reclamante, y mucho menos cualquier reconocimiento, aún tácito o presunto, de haber existido brecha de seguridad y captura de datos en las bases a nuestro cargo.”

Además, la NOTARÍA aporta información y documentación sobre el ataque sufrido.

CUARTO: Con fecha 4 de junio de 2021, y de conformidad con lo dispuesto en el art. 65 de la LOPDGDD se produjo la admisión a trámite de la reclamación interpuesta por la parte RECLAMANTE.

QUINTO: 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, teniendo conocimiento de los siguientes extremos:

Con fecha de 5 de enero de 2021 a las 8:35 horas el RECLAMANTE recibió un correo electrónico con origen en una dirección que le resulta desconocida (******EMAIL.1***) con el asunto “Adjunto certificado con el nombre nuevo. Contraseña: ******CONTRASEÑA.1***” y un archivo adjunto que manifiesta no haber descargado.
-Con posterioridad, el mismo día 5 de enero de 2021 a las 11:31 horas recibió un correo electrónico con origen en en una dirección que le resulta desconocida (******EMAIL.2***) con el asunto "Zip file attached to email: report.zip Password: ******PASSWORD.1***" y un archivo adjunto que manifiesta no haber descargado.

Lo que comunica telefónicamente a la NOTARÍA y a la notaría de ******PROVINCIA.1***. Según indica, éstos le habrían indicado que “han sido infectados por un virus y que su informático está revisándolo” ante lo cual les solicita que se pongan en contacto con él para conocer “hasta donde han llegado los daños y determinar cuanta información mía les han podido robar”.

La NOTARÍA niega este extremo; si bien afirma que “lo que se pudo informar a dicho-cliente y a otros varios clientes habituales del despacho es que nosotros mismos y una infinidad de usuarios de Outlook, a nivel mundial, estábamos siendo atacados (no infectados) por ese tipo de correos que, simulando proceder de contactos habituales y reproduciendo -total o parcialmente antiguos correos cruzados (si bien con diferente calibre y tipo de letra y espacio de interlineado), eran sin embargo cuentas absolutamente desconocidas para nosotros, teniendo, como él mismo, la precaución de no abrirlos.”

“En la semana del 19 al 23 de octubre del año 2020 (habiéndose reproducido el ataque en ocasiones durante los meses siguientes), se empezaron a recibir una gran cantidad de correos electrónicos aparentemente con remitentes conocidos (contactos habituales) en los buzones de correo electrónico de algunos empleados de la Notaría, pero se aprecia que las cuentas de los remitentes de estos correos electrónicos no se corresponden con la del “supuesto” remitente y tienen extensiones y terminaciones extrañas y desconocidas, además de reproducirse en los correos, con distinto tipo y tamaño de letra e interlineado, todo o parte de aquellos correos cruzados en su día con el cliente. De esta circunstancia se recibe información de los sistemas de seguridad de la entidad que provee de servicio de dominios de internet y correos electrónicos (Arsys), durante los días 19 y 21 de octubre de 2020.”

“Al respecto, el día 20 de Octubre de 2020, por medio de un correo electrónico al servicio de soporte de Arsys, se les solicita desde la Notaría que revisen este extremo, informando el proveedor de esta recepción de SPAM e indicando recomendaciones de actuación […]

A la vez, desde la Notaría, se produce una comunicación con el Administrador del Sistema Informático Externo contratado (la entidad Distribuciones Notariales, S.L.) la cual realiza un chequeo completo del sistema informático […]

El día 22 de Octubre de 2020, se remite desde Gerencia un correo electrónico interno a toda la Notaría, advirtiendo de la existencia de este tipo de correos, para que se extreme la atención a la hora de abrir correos electrónicos. Con un pantallazo de la forma de actuar y como las cuentas del remitente que aparecen en el correo no se corresponden con las del contacto de referencia.”

En el informe de intervención técnica de fecha 19 de mayo de 2021 realizado por Distribuciones Notariales S.L. para la NOTARIA refiere los siguientes aspectos en relación con la incidencia:

(…).

“Entre los días 27 y 28 de octubre de 2020, se procedió al cambio de todas las claves de los buzones de correo electrónico del sistema informático de la Notaría. Al haberse efectuado todas las actuaciones y valoraciones oportunas […] y no constar más incidentes, se considera la circunstancia por concluida.”

De acuerdo con el informe emitido por el administrador del sistema informático "se considera que la causa que ha podido generar el incidente se deriva de la actuación del malware "******MALWARE.1******".
Dicho malware se propaga por correo electrónico al descargarse archivos adjuntos" … "no consta que nadie del despacho hubiera abierto dichos archivos adjuntos".

Se identifican dos equipos afectados por el incidente y expresa que para solucionar el incidente "se llevó a cabo un análisis de seguridad y neutralización del virus infectado haciéndose uso de las herramientas específicas y software antivirus -EmoCheck y ******MALWARE.1******-Stopper-".

Además, en cuanto a las medidas tomadas para resolver el incidente, se citan las siguientes:

"Igualmente, mantener las contraseñas de cadenas alfanuméricas de doce dígitos, con caracteres alfabéticos en mayúsculas y minúsculas.

Asimismo, reforzar:

- Las revisiones informáticas generales en el ámbito del mantenimiento periódico
contratado.
- Las actuaciones de aviso y advertencia desde Gerencia a los empleados de la Notaria ante circunstancias similares que puedan estar produciéndose, habiéndose dado indicaciones precisas relativas a extremar las precauciones ante correos sospechosos, no debiéndose proceder a la apertura de sus archivos adjuntos en modo alguno.
- Las revisiones relativas a protección de datos de carácter personal, especialmente en lo tocante a la responsabilidad proactiva ("accountability") y al análisis y control de las medias técnicas y organizativas implantadas."

En relación con el número de afectados y categorías de datos personales implicados, "…según las valoraciones efectuadas por el propio Administrador del Sistema Informático externo contratado en la Notaría, que no es posible concretar el número de contactos filtrados. No obstante, el número de contactos en la BD local de usuario no excede de las 1000 direcciones".

No obstante, se afirma que "se han visto afectadas las "libretas de direcciones" de correo electrónico: en concreto, los nombres de contacto de dichas "Libretas"" y que la posible consecuencia para estos es el "envío masivo de correos electrónicos utilizando técnicas de phishing (suplantación de identidad) adquiriendo la libreta de direcciones personal del usuario infectado y reenviando correos adjuntando el virus EMOTEC al recipiente del destinatario".

Respecto a las medidas de seguridad implantadas con carácter previo al incidente, la NOTARIA adjunta la siguiente documentación:

(…).

En relación con la notificación a la AEPD, la NOTARÍA manifiesta que “no fue comunicado a la AEPD dado que, de haberlo hecho nosotros (respecto de los correos de ese tipo recibidos) y el resto de los afectados, sin duda se habría colapsado la Agencia. Simplemente tomamos las medidas y precauciones que a continuación se relatarán.”

Con respecto a la comunicación a los afectados la NOTARÍA señala que “no fue comunicado a los afectados ya que no se consideró que el mismo pudiera entrañar un “alto riesgo” para los derechos y libertades de los titulares de los datos. […]
Y ello ya que los riesgos que pueda comportar dicho incidente no supusieron entre otros, daños físicos, daños reputacionales, etc., pudiendo, además, mitigarse o evitarse por parte de la persona afectada posibles daños posteriores, con una mera y simple actuación de comprobación de la dirección remitente del e-mail “fraudulento” recibido.”

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, 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 la NOTARIA realiza, entre otros tratamientos, la recogida, la consulta y la utilización de los siguientes datos personales de personas físicas, tales como: nombre, apellidos, dirección de correo electrónico, dirección postal de la vivienda unifamiliar..., etc.

La NOTARIA 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 citado 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, consecuencia del envío de un correo electrónico procedente de un tercero con los datos

personales de la parte RECLAMANTE, que constaban en las bases de datos de la NOTARÍA.

Hay que señalar que la recepción de una reclamación sobre una brecha de seguridad no implica la imposición de una sanción de forma directa, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

La seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD, que regulan tanto 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 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, de la documentación aportada por la NOTARÍA en el curso de estas actuaciones de investigación no se desprende que, con anterioridad a la brecha de seguridad, careciera de medidas de seguridad razonables en función de los posibles riesgos estimados.

La NOTARÍA reconoce que la causa que ha podido generar el incidente se deriva de la actuación del malware "******MALWARE.1***".
Dicho malware se propaga por correo electrónico al descargarse archivos adjuntos." Añade, no obstante que, "no consta que nadie del despacho hubiera abierto dichos archivos adjuntos".
La NOTARÍA identifica dos equipos afectados por el incidente y expresa que para solucionar el incidente "se llevó a cabo un análisis de seguridad y neutralización del virus infectado haciéndose uso de las herramientas específicas y software antivirus-Emo-Check y ******MALWARE.1***-Stopper-".

Asimismo, no existen evidencias de que no hubiera actuado de forma diligente una vez conocida la brecha de seguridad, ni que las medidas adoptadas con posterioridad al incidente aquí analizado no fueran adecuadas.

Así, después de producirse la brecha de seguridad, la NOTARÍA manifiesta que ha reforzado las medidas de seguridad implantadas:
- Revisiones informáticas generales en el ámbito del mantenimiento periódico contratado.
- Actuaciones de aviso y advertencia desde Gerencia a los empleados de la Notaria ante circunstancias similares que puedan estar produciéndose, habiéndose dado indicaciones precisas relativas a extremar las precauciones ante correos sospechosos, no debiéndose proceder a la apertura de sus archivos adjuntos en modo alguno.
- Revisiones relativas a protección de datos de carácter personal, especialmente en lo tocante a la responsabilidad proactiva ("accountability") y al análisis y control de las medias técnicas y organizativas implantadas."

Cabe destacar la buena disposición de la NOTARÍA en el sentido de que, en cuanto ha tenido conocimiento del incidente, ha puesto en marcha las medidas oportunas para evitar que se pueda repetir en el futuro.

En consecuencia, la NOTARÍA adoptó todas las medidas que estaban a su disposición para impedir y minimizar el impacto de la brecha de seguridad ocurrida.

IV
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 dispone:

"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 supuesto, se ha comprobado que era improbable que la quiebra de seguridad constituyera un riesgo para los derechos y libertades de las personas físicas, por lo que la NOTARÍA estaba exenta de notificar la brecha de seguridad a esta Agencia, según lo establecido en el artículo 33 del RGPD.

V

Artículo 34 del RGPD

El artículo 34 "*Comunicación de una violación de la seguridad de los datos personales al interesado"* del RGPD establece*:*

"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 afectados por la violación de la seguridad de los datos personales, en particular 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."

En el presente caso, no resultaba probable que la brecha de seguridad entrañara un alto riesgo para los derechos y libertades de las personas físicas.

No obstante y a pesar de ello, la NOTARÍA tomó medidas ulteriores que garantizaban que ya no existía la probabilidad de que se concretara un alto riesgo para los derechos y libertades de los interesados, por lo que no estaba obligada a realizar la comunicación a los interesados de que se había producido una brecha de seguridad, en los términos del artículo 34 del RGPD.

VI
Conclusión

Por lo tanto, en base a lo indicado en los párrafos anteriores, no se han encontrado evidencias que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos.

Así pues, 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 D. ***A.A.A.*** y **TRILLO & VALIENTE NOTARIOS S.C.P** con CIF 00681030T.

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.

1245-050422

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