- **Procedimiento Nº: PS/00118/2020**

938-300320

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: Las actuaciones de inspección se inician por la recepción en esta Agencia Española de Protección de Datos (en lo sucesivo AEPD) de un escrito de notificación de brecha de seguridad de los datos personales remitido por la entidad IKATZ, S.A. en calidad de responsable del tratamiento, en el que informa de que, con fecha 10 de julio de 2019, recibieron un correo electrónico de la entidad encargada del tratamiento, a su vez remitido a ésta por el INCIBE, informando de una posible intrusión en los sistemas de información de la investigada.

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:

ANTECEDENTES
Fecha de notificación de la brecha de seguridad: 28 de agosto de 2019

ENTIDADES INVESTIGADAS
Durante las presentes actuaciones se han realizado investigaciones a las siguientes entidades:

IKATZ, S.A. (en lo sucesivo IKATZ o entidad investigada), con NIF A01043652 y con domicilio en C/ Arkatxa 1, Pabellón 4 (Pol. Industrial Uritiasolo), 01006 Vitorial-Gasteiz,Araba-Álava). (gira con el nombre comercial de Fotoprix)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1. Con fechas 26 de septiembre y 13 de diciembre de 2019 se remiten sendos requerimientos de información a la entidad investigada y de las respuestas recibidas, en fechas 14 de octubre de 2019 y 14 de enero de 2020, se desprende lo siguiente:

Respecto del responsable del tratamiento. Contratos con empresas encargadas del tratamiento.

- La entidad investigada, en calidad de responsable del tratamiento, tiene como objeto social la comercialización de material de fotografía y telefonía. Gira comercialmente con la marca comercial FOTOPRIX.

- Tiene contratada a la entidad SPCNET, en calidad de encargada del tratamiento, el alojamiento de la información en sus servidores.

Respecto de la cronología de los hechos. Medidas de minimización de la incidencia.

- Con fecha 9 de julio de 2019, a las 23h:28m, la empresa SPCNET -donde se aloja la información de la entidad investigada- recibe un correo electrónico remitido por el INCIBE informando de una posible intrusión en los servidores que alojan la información.

- Con fecha 10 de julio de 2019, a las 9h:25m, SPCNET reenvía a la entidad investigada el correo citado recibido del INCIBE. La empresa investigada confirma la intrusión a las 10h:30m al comprobar que se habían modificado archivos desactualizados instalados en una de las máquinas.

  En ese momento se procede a la descarga de los archivos para su estudio y se borran con objeto de eliminar la puerta de entrada al sistema de información.

- Con fecha 11 de julio de 2019, la investigada comprueba que ha habido nuevas modificaciones por lo que proceden a restaurar los sistemas a fecha anterior a la fecha estimada de la intrusión. No obstante, se comprueba que se continúan modificando los archivos por lo que proceden a restaurar los sistemas con una copia del último *backup* disponible de mediados de junio que contenía los archivos a fecha marzo/abril, por lo que el 12 de julio bloquean el acceso a la máquina desde todas las IPs no autorizadas (solo permiten el acceso a IPs contenidas en las listas *Whitelist -listas blanca-*).

La entidad investigada ha aportado copia del mail remitido del INCIBE en que se informa que desde el CERT del INCIBE se ha tenido conocimiento de un posible incidente de seguridad que apunta a dos direcciones IP e indicando dos direcciones web que han sido modificadas.

Respecto de las causas que hicieron posible la incidencia

- La entidad investigada manifiesta que seguramente ha habido dos incidentes de seguridad, el último de los cuales fue detectado por el INCIBE y fue eliminado con la primera restauración del sistema en julio de 2019. Respecto de la brecha anterior manifiestan que es distinta y desconocen el método de acceso.

- Respecto al último incidente, detectado por el INCIBE en julio de 2019, la entidad investigada manifiesta que fue debido a una vulnerabilidad del WORDPRESS (herramienta para creación y gestión de contenidos incorporando las funcionalidades típicas de los *blogs y* creación de páginas webs comerciales) que permitió la instalación de un *plugin* (programa informático) lo que permitió el acceso al sistema de ficheros y a la modificación del código.

- La entidad investigada manifiesta que la máquina afectada por los incidentes de seguridad estaba técnicamente obsoleta.

Respecto a la categoría de los datos afectados. Notificación e indexación

- Los datos personales afectados corresponden a: nombre y apellidos, dirección, mail, DNI, teléfono, móvil, fecha de nacimiento, número de hijos y género.

- El número de clientes afectados fue un máximo de 75.000, de los cuales 15.000 tenían el DNI.

- La entidad investigada manifiesta que no tienen constancia de la utilización por terceros de los posibles datos obtenidos a través de la brecha de seguridad.

- La entidad investigada manifiesta que han considerado que no era necesaria la comunicación a los posibles afectados después de valorar los parámetros de volumen (entre 1.000 y 100.000), la tipología de los datos (datos no sensibles) e impacto (externo) considerando un riesgo (nivel 18) que indica que no es necesario el envío de comunicación a los clientes afectados.

Respecto de las medidas de seguridad implantadas con anterioridad al incidente

- La entidad investigada ha aportado copia de los *logs* de sus sistemas de información.

Respecto de las medias implantadas con posterioridad a la incidencia

- La entidad investigada manifiesta que se han revisado y actualizado los sistemas, se procede a la revisión periódica y han aportado listado de las actualizaciones realizadas.

TERCERO: Con fecha 9 de junio de 2020, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a IKATZ, por la presunta infracción de los artículos 32, 33 y 34 del RGPD, tipificada en el artículo 83.4 del RGPD y como infracción grave en el artículo 73.f), g) r) y s) de la LOPDGDD.

CUARTO: Con fecha 16/06/2020 se notificó el acuerdo de inicio a IKATZ, que no presentó alegaciones.

HECHOS PROBADOS

PRIMERO: Con fecha 10 de julio de 2019, IKATZ, recibió un correo electrónico de la entidad encargada del tratamiento (SPCNET), a su vez remitido a ésta por el INCIBE, informando de una posible intrusión en los sistemas de información de la investigada.

SEGUNDO: Con fecha 10/07/2019, IKATZ confirma que su sistema de información de clientes ha sido objeto de acceso indebido a las 10h:30m al comprobar que se habían modificado archivos desactualizados instalados en una de las máquinas

TERCERO: Hasta el 28 de agosto de 2019 IKATZ no notificó a la AEPD la brecha de seguridad.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada autoridad de control, y según lo establecido en los artículos 47 y 48 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para iniciar y para resolver este procedimiento.

II

Establece el artículo 4.12 del RGPD que se considera "*violación de la seguridad de los datos personales: 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*."

Establece el artículo 33 del RGPD lo siguiente:

"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."

De las actuaciones practicadas se desprende que la entidad investigada informó a esta Agencia el 28 de agosto de 2019, casi dos meses después de tener conocimiento de la brecha de los datos personales en su sistema de información.

III

Establece el artículo 32 del RGPD, *seguridad del tratamiento*, 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 (El subrayado es de la AEPD).

El considerando 75 del RGPD enumera una serie de factores o supuestos asociados a riesgos para los derechos y libertades de los interesados:

"Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados."

En el presente caso, la entidad investigada no ha aportado el análisis de riesgos de los tratamientos de los que es responsable lo que impide evaluar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, careciendo de la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento, lo que ha provocado el acceso por tercero no autorizado a los datos alojados en su sistema de información.

IV

Establece el artículo 28 de la LOPDGDD lo siguiente:

1. Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y

acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV del citado reglamento.

2. Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:

a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.

c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas. (…) (El subrayado es de la Agencia Española de Protección de Datos.).

En el presente caso, consta que la entidad encargada del tratamiento (SPCNET) informó en tiempo y forma a la entidad responsable (la investigada) del mismo sobre la incidencia detectada en julio de 2019 por el INCIBE.

V

De las actuaciones practicadas se ha verificado que las medidas de seguridad que contaba la entidad investigada en relación con los datos que sometía a tratamiento, no eran las adecuadas al momento de producirse la brecha de seguridad.

La consecuencia de esta falta de medidas de seguridad adecuadas fue la exposición a terceros ajenos de los datos personales de los clientes. Es decir, los afectados se han visto desprovistos del control sobre sus datos personales.

Hay que añadir que, sobre la posibilidad de combinación de informaciones referidas a un titular de datos personales, se puede traer a colación el Dictamen 4/2007 del Grupo de Trabajo del Articulo 29, "*Sobre el concepto de datos personales*" que analiza las posibilidades de identificar a alguien a través de combinaciones con otras informaciones, partiendo únicamente de los datos de un cliente y combinándola con otra.

En concreto indica lo siguiente: (…) *cuando hablamos de «indirectamente» identificadas o identificables, nos estamos refiriendo en general al fenómeno de las «combinaciones únicas», sean estas pequeñas o grandes. En los casos en que, a primera vista, los identificadores disponibles no permiten singularizar a una persona determinada, ésta aún puede ser «identificable», porque esa información combinada*

con otros datos (tanto si responsable de su tratamiento tiene conocimiento de ellos como si no) permitirá distinguir a esa persona de otras. Aquí es donde la Directiva se refiere a «uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social». Algunas de esas características son tan únicas que permiten identificar a una persona sin esfuerzo (el «actual presidente del Gobierno de España»), pero una combinación de detalles pertenecientes a distintas categorías (edad, origen regional, etc.) también puede ser lo bastante concluyente en algunas circunstancias, en especial si se tiene acceso a información adicional de determinado tipo. Este fenómeno ha sido estudiado ampliamente por los estadísticos, siempre dispuesto a evitar cualquier quebrantamiento de la confidencialidad (…). *Así pues, se unen las diferentes piezas que componen la personalidad del individuo con el fin de atribuirle determinadas decisiones.* (…)

Como se ha indicado anteriormente, en este caso la búsqueda en internet, por ejemplo, del nombre, apellidos o dirección de correo electrónico de alguno de los afectados puede ofrecer resultados que combinándolos con los ahora accedidos por terceros ajenos, nos permitan el acceso a otras aplicaciones de los afectados o la creación de perfiles de personalidad, que no tienen por qué haber sido consentida por su titular.

Esta posibilidad supone un riesgo añadido que se ha de valorar y que aumenta la exigencia del grado de protección en relación con la seguridad y salvaguarda de la integridad y confidencialidad de estos datos.

Este riesgo debe ser tenido en cuenta por el responsable del tratamiento que en función del mismo, debe establecer las medidas técnicas y organizativas necesarias que impedida la pérdida de control de los datos por parte del responsable del tratamiento y, por tanto, por parte de los titulares de los datos que se los proporcionaron.

VI

Establece el artículo 34 del RGPD, comunicación de una violación de la seguridad de los datos personales al interesado, lo siguiente:

“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).

1. 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, la entidad investigada no ha aportado el análisis de riesgos asociado a los tratamientos de datos de los que es responsable, si bien señala que no responde a un nivel alto (indica nivel 18) por lo que no es preceptiva la comunicación a los interesados. No obstante, la entidad investigada deberá responsabilizarse de la ausencia de tal comunicación y, en su caso, de la preceptiva evaluación de impacto según señala el art 35 del RGPD, tras la nueva evaluación del riesgo requerida en la parte resolutiva de esta Resolución.

VII

Establece el artículo 71 de la LOPDGDD, bajo la rúbrica "*Infracciones*" lo siguiente: *Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica.*

Establece el artículo 73 de la LOPDGDD, bajo la rúbrica "Infracciones consideradas graves" lo siguiente: *En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:*

f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.

g) El quebrantamiento, como consecuencia de la falta de la debida diligencia, de las medidas técnicas y organizativas que se hubiesen implantado conforme a lo exigido por el artículo 32.1 del Reglamento (UE) 2016/679.

r) El incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.

En el presente caso concurren las circunstancias infractoras previstas en el artículo 73 apartados f), g) y r) de la LOPDGDD arriba transcritos.

VIII

Establece la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en el Capítulo III relativo a los "*Principios de la Potestad sancionadora*", en el artículo 28 la bajo la rúbrica "*Responsabilidad*", lo siguiente:

"1. Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa"

La falta de diligencia a la hora de implementar de origen las medidas de seguridad adecuadas constituyen el elemento de la culpabilidad que requiere la imposición de sanción.

IX

El artículo 58.2 del RGPD, señala lo siguiente*:*

2. Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

(…)

b) sancionar a todo responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;

El artículo 83 del RGPD, señala lo siguiente:
(…)

"4. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) Las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43"

El artículo 76 de la LOPDGDD bajo la rúbrica "*Sanciones y medidas correctivas* ", señala lo siguiente:

1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

(…)

3. Será posible, complementaria o alternativamente, la adopción, cuando proceda, de las restantes medidas correctivas a las que se refiere el artículo 83.2 del Reglamento (UE) 2016/679.

X

En el presente caso, en atención a la complejidad de los sistemas de información afectados, así como las acciones tomadas tendentes a minimizar las consecuencias negativas de la citada brecha de seguridad de los datos personales de sus clientes, se considera conforme a derecho no imponer sanción consistente en multa administrativa y sustituirla por la sanción de apercibimiento de conformidad con el artículo 76.3 de la LOPDGDD en relación con el articulo 58.2 b) del RGPD.

Por lo tanto, de acuerdo con la legislación aplicable la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER a IKATZ, S.A., con NIF A01043652, por infracción de los artículos 32 y 33 del RGPD, tipificada en el Artículo 83.4 del RGPD y artículo 73.f), g) y r) de la LOPDGDD, una sanción de apercibimiento.

SEGUNDO: Requerir a IKATZ, S.A. para que en el plazo de tres meses aporte a esta AEPD la siguiente documentación:

- Aportar procedimiento reglado de actuación y notificación a la AEPD ante una incidencia de seguridad que permita conocer en tiempo y forma si ha afectado a datos personales y que identifique las ubicaciones y recursos afectados (brecha de seguridad).

- Aportar auditoría realizada tras la brecha de seguridad que certifique el correcto funcionamiento y configuración del sistema de información al objeto de evitar la exposición indebida a terceros ajenos de recursos con datos personales, así como un nuevo análisis de riesgos.

TERCERO: NOTIFICAR la presente resolución a IKATZ, S.A., con NIF A01043652 y con domicilio en C/ Arkatxa 1, Pabellón 4 (Pol. Industrial Uritiasolo), 01006 Vitorial-Gasteiz,Araba (Álava).

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 conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, 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.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

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