- **Procedimiento Nº: PS/00187/2020**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: Con fecha 14 de enero de 2020, la Subdirección General de Nacionalidad y Estado Civil (en adelante, SGNEC) adscrita a la Dirección General de los Registros y del Notariado (actualmente Dirección General de Seguridad Jurídica y Fe Pública, en adelante, DGSJFP) dependiente en la actualidad orgánica y funcionalmente de la Secretaría General para la Innovación y Calidad del Servicio Público de Justicia (en adelante, SGICSPJ) del Ministerio de Justicia, notifica a esta Agencia Española de Protección de Datos (en adelante, AEPD) una brecha de seguridad de los datos personales (en adelante, brecha de seguridad) tras tener conocimiento a través de un correo electrónico por parte de un ciudadano de una notificación de concesión de la nacionalidad española correspondiente a otra persona (tratamiento relativo a la aplicación ******APLICACIÓN.1***).

La SGNEC contactó telefónicamente con la directora de la División de Tecnologías de Información y Comunicaciones del Ministerio de Justicia (actualmente División de Tecnologías y Servicios públicos Digitales, en adelante, DTSPD) para conocer la naturaleza y alcance del problema y el número de potenciales notificaciones afectadas. Finalmente, confirmada la brecha de seguridad, la SGNEC manifiesta que se decidió la paralización de las notificaciones automatizadas hasta conocer la causa y alcance del incidente y su resolución.

SEGUNDO: Con fecha de 4 de febrero de 2020, la directora de la AEPD acuerda iniciar actuaciones de investigación, por lo que 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 notificación, teniendo conocimiento de los siguientes extremos:

ANTECEDENTES

Fecha de los hechos: ******FECHA.1***

Fecha de detección de la brecha de seguridad: ******FECHA.2***

Fecha de la notificación de la quiebra de seguridad: 14/01/2020

ENTIDADES INVESTIGADAS

Dirección General de Seguridad Jurídica y Fe Pública del Ministerio de Justicia con NIF S2813610I y DIR3 E00131304, y con domicilio en Plaza de Jacinto Benavente 3, 28012 Madrid (adscrita orgánica y funcionalmente a la SGICSPJ con NIF S2813610I y DIR3 E05077001 en calidad de responsable del tratamiento).

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1. Respecto a los hechos:

- En torno a las 14:30 horas del ******FECHA.2***, la SGNEC manifiesta haber recibido comunicación telefónica con relación a la recepción de un correo electrónico por parte de un ciudadano de una notificación de concesión de la nacionalidad española por residencia correspondiente a otro solicitante. En ese momento, la SGNEC contactó telefónicamente con la DTSPD para conocer la naturaleza del problema y el número de notificaciones potencialmente afectadas por la brecha de seguridad, y se decidió la paralización de las notificaciones automatizadas hasta conocer y solucionar la causa del incidente. No se aporta copia del correo electrónico del ciudadano.

- La SGNEC informa de que el día 13 de enero de 2020 recibió de la DTSPD informe base de la notificación de la quiebra de seguridad que fue comunicada a la AEPD el día 14 de enero de 2020. Del citado informe, la SGNEC manifiesta que el incidente alcanza a 34 casos y posteriormente incorporaron otros 2 más, hasta 36, de las 23.394 resoluciones de nacionalidad resueltas hasta ese momento. No consta la intervención del Delegado de Protección de Datos conforme señala el art 39 del RGPD.

- La SGNEC declara haber adjuntado dicho informe a la AEPD en su notificación de quiebra de seguridad, y puntualiza lo siguiente:

  "el problema tuvo su origen en una modificación en el proceso de generación de resoluciones de concesión de nacionalidad por residencia que se había realizado en la aplicación ******APLICACIÓN.1****, de tramitación de expedientes de nacionalidad por residencia, el día* ******FECHA.1****".*

- La SGNEC informa de que el fallo detectado se originó al adjuntar el certificado de nacimiento del solicitante de nacionalidad al documento de resolución de concesión de nacionalidad. El elevado número de resoluciones generadas de

manera concurrente es consecuencia de un plan de refuerzo que puntualmente implica un escenario de alta concurrencia de solicitudes. Asimismo, la SGNEC añade que dicho plan de refuerzo ha implicado la participación de un número muy superior de personal tramitador al previsto inicialmente en el diseño de la aplicación.

- La SGNEC señala que los datos personales afectados en la brecha de seguridad corresponderían al NIE (Número de Identificación de Extranjero), nombre, apellidos, lugar y fecha de nacimiento, domicilio en el momento de presentar la solicitud, la propia concesión de nacionalidad y copia del certificado de nacimiento (en el que figuran nuevamente datos de fecha y lugar de nacimiento y nombre y apellidos de los progenitores).

- La SGNEC informa de que ha registrado otros dos incidentes de seguridad de los datos personales, en fechas 28/06/2019 y 31/10/2019, también con notificaciones incorrectas por error de destinatarios al comunicar concesiones de nacionalidad, con 11 y 70 personas afectadas respectivamente y ya solucionado. La SGNEC expone que el incidente acontecido el 28/06/2019 derivó del proceso de envío de notificaciones telemáticas por una incidencia en la base de datos de la aplicación, mientras que el del 31/10/2019 consistía en una gestión incorrecta de excepciones en el caso de saturación de distintos sistemas con los que la aplicación interactúa, entre ellos el portafirmas del Ministerio de Justicia.

- La Inspección de Datos hace constar que, con fecha 5/09/2018, la AEPD dictó resolución de procedimiento sancionador, de referencia AP/00049/2018, en el que se sancionó por los mismos hechos a los ahora investigados a la Dirección General de los Registros y del Notariado dependiente de la Subsecretaria de Justicia (ahora DGSJFP, dependiente de la SGICSPJ). En concreto, en el citado expediente sancionador quedó acreditado que *“La División de Tecnologías de la Información y Comunicaciones del Ministerio de Justicia informó que el servicio no contemplaba la concurrencia y se equivocó al componer el certificado de nacimiento. El tomo y pagina que figuran en el certificado son correctos y corresponden a los datos de su inscripción de nacimiento, pero el contenido con la imagen digitalizada son los de otra solicitud, la de matrimonio”.* (el subrayado es de la AEPD).

2. Respecto a las medidas previas al acontecimiento de la quiebra de seguridad:

- La SGNEC se encuentra actualmente identificada en el RAT (registro de actividades de tratamiento) del Ministerio de Justicia como responsable del tratamiento de los datos en la gestión de solicitudes de nacionalidad española. La SGNEC aporta documento de trabajo interno de actualización del RAT en que se especifica a la DTSPD como corresponsable del tratamiento ahora analizado a partir de enero de 2020.

- La SGNEC manifiesta haber realizado una EIPD (evaluación de impacto relativa a la protección de datos) en junio de 2019, que contiene un análisis de riesgos asociado los tratamientos de datos que gestiona.

- La SGNEC dispone de un informe de acciones derivadas de la EIPD en la gestión de solicitudes de nacionalidad española, que tiene por objeto minimizar los riesgos potenciales analizados mediante la implantación de diversas acciones correctoras hasta disminuirlos a riesgos residuales que han resultado ser de nivel alto.

- La DTSPD, en calidad de corresponsable del tratamiento (según el RAT aportado y vigente desde enero de 2020), dispone de un procedimiento sobre la calidad de los proyectos de *software* del Ministerio de Justicia a lo largo de todo su ciclo de vida, que sirve de base en su construcción y desarrollo en el que se definen las fases que rigen el análisis y diseño de la solución, así como las pruebas que deben realizarse en los diferentes entornos (desarrollo, integración, calidad y preproducción), hasta su implantación definitiva en el entorno de producción, y la monitorización activa tras su puesta en producción.

3. Respecto a las medidas posteriores al acontecimiento de la brecha de seguridad:

3.1. De carácter correctivo (reactivas para subsanar la brecha de seguridad):

- La SGNEC expone que, una vez conocido el incidente, el ******FECHA.2*** a las 14:30 horas, se procedió a bloquear el proceso de firma y de notificación automatizada de las concesiones de nacionalidad española en la aplicación involucrada (******APLICACIÓN.1***).

- El martes día 14 de enero de 2020 se notifica la brecha de seguridad a la AEPD.

- La SGNEC manifiesta que el miércoles 15 de enero de 2020 a las 15:50 horas se procede a la retirada de *Carpeta Ciudadana* de las notificaciones electrónicas de las concesiones de nacionalidad española emitidas con contenido erróneo al referirse a otro solicitante de nacionalidad.

- La SGNEC aporta evidencias de que el jueves día 16 de enero de 2020 se firmaron electrónicamente 72 oficios comunicando la brecha de seguridad tanto a los destinatarios de las resoluciones como a las personas que las habían recibido erróneamente, se cumplimentaron los acuses de recibo, ensobrado y albaranes para su envío postal a los interesados.

- La SGNEC manifiesta que el 21 de enero de 2020 se registró la salida desde el Registro General del Ministerio de Justicia la relación de notificaciones administrativas junto con los sobres, los acuses de recibo y los albaranes para tramitación de las comunicaciones a los interesados.

- La SGNEC informa de que el proceso de firma vuelve a habilitarse el día 23 de enero de 2020 a las 15:40 horas, no así el proceso de notificación automática de las concesiones de nacionalidad española que continuaba bloqueado a fecha 26 de febrero de 2020.

- La SGNEC expone que a partir del viernes día 24 de enero del 2020 a las 9:00 horas se empiezan a realizar notificaciones de concesión de nacionalidad de manera manual previa comprobación de que el documento a notificar es correcto.

3.2. De carácter preventivo (proactivas para evitar que se repita la quiebra de seguridad):

- La DTSPD manifiesta haber diseñado en la aplicación ******APLICACIÓN.1*** una medida más robusta que compruebe el contenido de los documentos de concesión de nacionalidad española con carácter previo a la notificación, de tal forma que no se pueda notificar documento alguno no correspondiente en contenidos con el expediente tratado. La SGNEC informa que se ha establecido un protocolo de control de calidad previo (no lo detalla) para asegurar que el documento a notificar sea correcto, realizándose la notificación de manera manual y supervisada.

- La DTSPD expone que se encuentra en fase de pruebas la nueva versión de la aplicación que incorpora en el proceso de notificación la lectura y comprobación del contenido del documento a comunicar con carácter previo a la notificación. La SGNEC traslada que la nueva versión de la aplicación está (a fecha 26 de febrero de 2020) siendo sometida a controles de calidad (pruebas funcionales, pruebas de rendimiento y pruebas de concurrencia).

- La DTSPD informa de haber detectado el origen de la brecha de seguridad en un manejo inadecuado de ficheros temporales al realizar el anexado de la partida de nacimiento a la resolución de concesión de nacionalidad. Adicionalmente, la SGNEC destaca que se está trabajando en la implementación de un proceso automático que recorra los formularios de la aplicación y que permita realizar un control de calidad adicional al propio realizado en las opciones de la aplicación, de tal forma que se garantice que las resoluciones de concesión de la nacionalidad española son notificadas correctamente.

- A fecha del presente acuerdo de inicio la Inspección de Datos de la AEPD no ha sido informada del progreso y las garantías establecidas/implantadas en la nueva aplicación/versión de notificaciones de concesión de la nacionalidad, así como de las pruebas en la nueva versión de noviembre de 2019 realizadas, análisis de riesgos, evaluación de impacto sobre los derechos y libertades de los interesados y si el incidente ha sido resuelto.

TERCERO: Con fecha 9 de julio de 2020, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al reclamado, por la presunta infracción del Artículo 32 del RGPD, Artículo 5.1.f) del RGPD, Artículo 25 del RGPD, tipificada en el Artículo 83.5 del RGPD.

CUARTO: Con fecha 7 de octubre de 2020 se formuló propuesta de resolución, proponiendo en los siguientes términos:

<<Que por la Directora de la Agencia Española de Protección de Datos se sancione a la Secretaría General para la Innovación y Calidad del Servicio Público de Justicia**,** con NIF S2813610I, por:

1. Infracción del artículo 5.1.f) del RGPD tipificada en el artículo 83.5.a) del RGPD con sanción de apercibimiento.
2. Infracción de los artículos 25, 32 y 33 del RGPD en relación con el artículo 5.1.f) del RGPD, tipificada en el artículo 83.4.a) del RGPD con sanción de apercibimiento.
3. Infracción del artículo 34 del RGPD en relación con el artículo 5.1.f) del RGPD, tipificada en el artículo 83.4.a) del RGPD, con sanción de apercibimiento.
4. Y requerir a la SGICSPJ a que aporte a esta AEPD resumen del resultado final del plan de actuación, ya iniciado en febrero de 2020, por el que se aplican medidas más robustas de seguridad en los tratamientos de datos en el aplicativo ******APLICACIÓN.1*** del que es responsable en materia de protección de datos a través de la SGNEC>>.

QUINTO: En fecha 23/10/2020 la investigada presenta alegaciones a la propuesta de resolución en los siguientes términos:

En primer lugar, la investigada considera que no hubo brecha de integridad, toda vez que conforme define el Esquema Nacional de Seguridad (ENS), la integridad es aquella *"propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada",* por lo que no es de aplicación al presente caso.

Al respecto, se debe señalar que el nuevo principio de integridad, antes denominado seguridad, recogido en el artículo 5.1. f) del RGPD, trae causa de lo dispuesto en el artículo 1 del citado reglamento (objeto del RGPD) respecto al tratamiento de los datos personales en sentido amplio y con proyección temporal con independencia de los datos concretos que sean objeto de tratamiento, y no solo respecto a datos concretos y estáticos en el tiempo para un tratamiento determinado. En consecuencia, la alegación debe rechazarse.

En segundo lugar, respecto a la dimensión de confidencialidad de los datos tratados, la investigada señala que se limitó a 36 personas directas y otras 36 de forma indirecta, por lo que se produjo a un número de personas finitas y determinadas, y no a un número de personas indeterminadas, conforme señala el artículo 25.2 del RGPD.

En este sentido, se significa que la indeterminación a la que hace mención el artículo 25.2 del RGPD se refiere al principio de diseño por defecto en virtud del cual las medidas técnicas y organizativas aplicadas garantizarán en particular que, por defecto, los datos personales no sean accesibles a un número indeterminado de personas

físicas, y no al número de personas afectadas por la brecha. En consecuencia, la alegación debe ser rechazada.

En tercer lugar, aporta un conjunto de medidas adoptadas de índole reactivo y proactivo, de las que se desprende una conducta diligente al objeto de minimizar el impacto de la brecha y evitar que en el futuro se repita situaciones similares. En este sentido aporta documental sobre nuevas actuaciones de calidad en el código, pruebas funcionales que contemplan en especial la concurrencia de solicitudes y composición de documentos a notificar, revisión del ciclo de vida, formación del equipo de desarrollo y plan de seguimiento periódico del plan de calidad del código.

En cuarto lugar, la investigada aporta documental sobre la licitación de un expediente de contratación para la adecuación de los tratamientos efectuados en la unidad al ENS, iniciándose su ejecución en septiembre de 2020, reforzándose las políticas de seguridad tanto por el personal adscrito a la DTSPD como a sus principales proveedores de servicios que actúen como encargados del tratamiento. A tal efecto se aporta pliego de prescripciones técnicas que rigen dicho contrato.

En quinto lugar, la investigada aporta notificación a la AEPD de las brechas de seguridad de fechas 28/06/2019 y 31/10/2019.

Por último, la investigada informa sobre el nuevo escenario de corresponsabilidad en los tratamientos conforme señala el artículo 26 del RGPD por parte de la DTSPD.

De las actuaciones practicadas en el presente procedimiento y de la documentación obrante en el expediente, han quedado acreditados los siguientes:

HECHOS PROBADOS

PRIMERO: Con fecha 14 de enero de 2020, la Subdirección General de Nacionalidad y Estado Civil (en adelante, SGNEC) adscrita a la Dirección General de los Registros y del Notariado (actualmente Dirección General de Seguridad Jurídica y Fe Pública, en adelante, DGSJFP) dependiente en la actualidad orgánica y funcionalmente de la Secretaría General para la Innovación y Calidad del Servicio Público de Justicia (en adelante, SGICSPJ) del Ministerio de Justicia, notifica a esta Agencia Española de Protección de Datos (en adelante, AEPD) una brecha de seguridad de los datos personales de fecha 22/11/2019 tras tener conocimiento a través de un correo electrónico por parte de un ciudadano de una notificación de concesión de la nacionalidad española correspondiente a otra persona (tratamiento relativo a la aplicación ******APLICACIÓN.1***).

SEGUNDO: La brecha de seguridad notificada alcanza a 34 afectados y posteriormente incorporaron otros 2 más, hasta 36, todos ellos relativos a resoluciones de nacionalidad indebidamente notificadas a terceros ajenos. La brecha de seguridad fue comunicada a los interesados el 16/01/2020.

TERCERO: La brecha de seguridad tuvo su origen técnico en una modificación en el proceso de generación de resoluciones de concesión de nacionalidad por residencia que se había realizado en la aplicación ******APLICACIÓN.1***, de tramitación de expedientes de nacionalidad por residencia, el día ******FECHA.1***.

CUARTO: El fallo detectado se originó al adjuntar el certificado de nacimiento del solicitante de nacionalidad al documento de resolución de concesión de nacionalidad como consecuencia del elevado número de resoluciones generadas de manera concurrente.

QUINTO: Los datos personales afectados en la brecha de seguridad corresponderían al NIE (Número de Identificación de Extranjero), nombre, apellidos, lugar y fecha de nacimiento, domicilio en el momento de presentar la solicitud, la propia concesión de nacionalidad y copia del certificado de nacimiento (en el que figuran nuevamente datos de fecha y lugar de nacimiento y nombre y apellidos de los progenitores).

SEXTO: Consta que la SGNEC, dependiente orgánicamente de la SGICSPJ, ha registrado otros dos incidentes de seguridad de los datos personales, en fechas 28/06/2019 y 31/10/2019, también con notificaciones incorrectas por error de destinatarios al comunicar concesiones de nacionalidad, con 11 y 70 personas afectadas respectivamente y ya solucionado. Dichas brechas de seguridad fueron debidamente notificadas a la AEPD pero no consta que fueran comunicadas a los afectados.

SÉPTIMO: Consta, con fecha 5/09/2018, la AEPD dictó resolución de procedimiento sancionador de referencia AP/00049/2018, en el que se sancionó por los mismos hechos a los ahora investigados a la Dirección General de los Registros y del Notariado dependiente de la Subsecretaria de Justicia (ahora DGSJFP, dependiente de la SGICSPJ). En concreto, en el citado expediente sancionador quedó acreditado y así consta en los hechos probados, que *"La División de Tecnologías de la Información y Comunicaciones del Ministerio de Justicia informó que el servicio no contemplaba la concurrencia y se equivocó al componer el certificado de nacimiento".*

OCTAVO: Respecto de los tratamientos llevados a cabo por la SGNEC, consta haber realizado una EIPD (evaluación de impacto relativa a la protección de datos) en junio de 2019, que contiene un análisis de riesgos (AR) asociado los tratamientos de datos que gestiona. Sin embargo, no consta actualización del AR y EIDP en las modificaciones de los tratamientos llevados a cabo el 22/11/2019 que dieron lugar la brecha de seguridad de esa fecha. Sin embargo, en alegaciones la propuesta de resolución se aporta la adecuada actualización al RGPD, LOPDGDD y ENS de los tratamientos llevados a cabo por la investigada así como la implantación de las medidas correctoras tanto activas como proactivas para evitar la repetición en el futuro de hechos similares.

FUNDAMENTOS DE DERECHO

I

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

II

Definiciones:
Artículo 4.12 del RGPD, "*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*.
Artículo 4.7 del RGPD, *"responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros".*

III

En el presente caso, conforme lo dispuesto el citado art 4.7 del RGPD y en el RD 453/2020, de 10 de marzo, por el que se desarrolla la estructura orgánica básica del Ministerio de Justica, artículo 3.1, corresponde a la SGICSPJ la dirección, impulso y gestión de las atribuciones ministeriales relativas al estado civil y nacionalidad, a través de la DGSJFP (art 7.1.b) del citado RD) que tramita y resuelve los expedientes de nacionalidad.

En consecuencia, en la actualidad es la SGICSPJ la responsable de los tratamientos de datos personales en todas las actuaciones llevadas a cabo por las diferentes unidades orgánicas a ella adscritas relativas al estado civil y nacionalidad, toda vez que, tal y como señala el art 4.7 del citado RGPD, es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determina los fines y medios del tratamiento, en coherencia con lo dispuesto en el art 3 del citado RD 453/2020 por el que corresponde a la SGICSPJ la *"dirección, impulso y gestión de las atribuciones ministeriales relativas a estado civil y nacionalidad … ".*

Cabe señalar, que si bien la Secretaría General para la Innovación y Calidad del Servicio Público de Justicia no era la responsable del tratamiento de datos ahora analizado en el momento de producirse la/s brecha/s de seguridad (de fechas 28/06/2019, 31/10/2019 y 22/11/2019), es cierto que con la actual estructura básica del Ministerio de Justicia le compete llevar a cabo las preceptivas regularizaciones en los tratamientos de datos de los que es responsable y promover con la diligencia debida su adecuación al RGPD.

IV

El artículo 5.1.f) del RGPD, Principios relativos al tratamiento, señala lo siguiente:
"1. Los datos personales serán:
(…)
f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)".

En el presente caso, la brecha de seguridad debe ser calificada de integridad y de confidencialidad como consecuencia, en primer lugar, de la falta de seguridad adecuada y medidas técnicas u organizativas apropiadas (integridad), y en segundo lugar por los accesos no autorizados a datos personales por terceros ajenos

(confidencialidad), ambos principios regulados en el mismo artículo 5.1.f) del RGPD arriba transcrito.

V

Establece el Artículo 25 del RGPD, lo siguiente:

"Protección de datos desde el diseño y por defecto

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo".

En este sentido, y respecto a la alegación referida a que la brecha de seguridad que dio lugar al procedimiento sancionador AP/00049/2018 (resuelto el 5/09/2018) se corresponde a *"tratamientos de datos completamente diferentes",* se debe señalar que el origen de las brechas analizadas tiene causa común en la falta de previsión desde el diseño del factor de concurrencia en los procesos de ambos aplicativos (******APLICACIÓN.2*** y ******APLICACIÓN.1***).

Establece el artículo 32 del RGPD, 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".

Establece el artículo 34.1 del RGPD, 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."

Respecto al artículo 32, consta que el responsable del tratamiento no aplicó las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo; riesgo que ni siquiera fue evaluado en la actualización de la nueva versión del aplicativo ******APLICACIÓN.1***.

Respecto al artículo 34, cabe señalar que de las actuaciones practicadas se desprende que la SGICSPJ, a través de la SGNEC, notificó a esta AEPD la brecha de seguridad de datos personales de fecha ******FECHA.1*** y lo comunicó a los interesados el 16/01/2020. Sin embargo, la investigada afirma también que hubo dos brechas de seguridad similares y previas a la ahora investigada. Consta en las alegaciones a la propuesta de resolución que las brechas de fechas 26/06/2019 y 31/10/2019 fueron notificadas a esta AEPD (art 33 RGPD) pero no consta que hayan sido comunicadas a los interesados (art 34 RGPD), si bien en la primera se afirma en la notificación que se comunicará a los interesados pero no consta realizada y, en la segunda se afirma que se comunicó a los interesados telefónicamente pero tampoco consta realizada.

VI

El artículo 24 del RGPD, responsabilidad del responsable del tratamiento, señala lo siguiente:

"1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.
2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos" (…).

VII

De los hechos descritos consta que la SGICSPJ, como responsable de los tratamientos ahora analizados y a través de sus órganos jerárquicamente dependientes, no aplicó las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, toda vez que consta acreditado que terceros ajenos tuvieron acceso a información reservada al interesado (solicitante de nacionalidad española) como consecuencia del mal funcionamiento en la puesta en producción de la nueva versión de la aplicación ******APLICACIÓN.1*** que gestiona la DGSJFP a través de la SGNEC, ambas dependientes jerárquicamente a la SGICSPJ.

Los riesgos en el tratamiento contemplados en la nueva versión de la aplicación ***APLICACIÓN.1** debió ser tenido en cuenta y evaluado por el responsable del tratamiento (SGICSPJ) a través del preceptivo análisis de riesgos y en su caso evaluación de impacto y, en función del mismo, haber establecido las medidas técnicas y organizativas que hubieran impedido la pérdida de control de los datos personales de los solicitantes de nacionalidad española como consecuencia de la reiterada y ya conocida falta de previsión de procesos concurrentes en el tratamiento de datos de los diferentes aplicativos (***APLIACIÓN.1** y ***APLIACIÓN.2**).

Se debe insistir, en que el nivel de riesgo y el impacto ya eran conocidos con antelación toda vez que consta en esta AEPD un expediente sancionador por hechos similares (AP/00049/2018 y fecha de resolución el 5/09/2018) y, además, la SGNEC señala que se registraron hechos similares en fechas previas a la brecha de seguridad de fecha 22/11/2019, en concreto en fechas 28/06/2019 y 31/10/2019.

Consta también en el citado procedimiento sancionador previo que la actual DTSPD informó a la SGNEC que *"el servicio no contemplaba la concurrencia y se equivocó al componer el certificado de nacimiento …"* y, no obstante, un año más tarde se repitió en otras tres ocasiones fielmente el incidente por la misma causa.

La consecuencia de esta usencia en el control de los tratamientos de datos desde el diseño y por defecto (art 25 RGPD) y de la implantación de medidas de seguridad apropiadas (art 32 RGPD) al riesgo de la nueva versión de la aplicación ***APLICACIÓN.1** causante de la brecha de fecha ***FECHA.1**, fue la pérdida de integridad y confidencialidad de los datos personales, vulnerando los dos principios recogidos en el art 5.1.f) del RGPD.

VIII

El artículo 83.4 del RGPD dispone 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;"

En el presente caso consta vulnerados los artículos 25, 32 y 34 del RGPD, tipificados en el artículo 83.4 del RGPD arriba transcrito.

El artículo 83.5 del RGPD dispone lo siguiente:

"5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) *los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;"*

En el presente caso consta nuevamente vulnerado el artículo 5.1.f) del RGPD, esta vez referido al principio de confidencialidad, por lo que es de aplicación la tipificación que señala el artículo 83.5 del RGPD arriba transcrito.

Por su parte, el artículo 71 de la LOPDGDD, bajo la rúbrica "*Infracciones*" determina 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 72 de la LOPDGDD, bajo la rúbrica de infracciones consideradas muy graves, lo siguiente: *"1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:*

a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679".

Establece el artículo 73 de la LOPDGDD, bajo la rúbrica *"Infracciones consideradas graves",* lo siguiente: "*1. 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:*

(…)

d) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el diseño, así como la no integración de las garantías necesarias en el tratamiento, en los términos exigidos por el artículo 25 del Reglamento (UE) 2016/679.

(…)

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

(…)

t) El tratamiento de datos personales sin haber llevado a cabo la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales en los supuestos en que la misma sea exigible. (…)". Este apartado, en relación con los cambios realizados en ******FECHA.1*** en la aplicación ******APLICACIÓN.1***.

Establece el artículo 74 de la LOPDGDD, bajo la rúbrica *"Infracciones consideradas leves",* lo siguiente: *"Se consideran leves y prescribirán al año las restantes infracciones de carácter meramente formal de los artículos mencionados en los apartados 4 y 5 del artículo 83 del Reglamento (UE) 2016/679 y, en particular, las siguientes:*

(…)

ñ) El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos que entrañe un alto riesgo para los derechos y libertades de los afectados, conforme a lo exigido por el artículo 34 del Reglamento (UE) 2016/679, salvo que resulte de aplicación lo previsto en el artículo 73 s) de esta ley orgánica".

De todo lo anterior, se concluye lo siguiente:

Respecto a la tipificación de infracciones del artículo 83.5.a) del RGPD

- Vulneración del principio de confidencialidad (art 5.1.f) RGPD), es considerada infracción muy grave a efectos de prescripción (tres años) conforme señala el artículo 72.1.a) de la LOPGDD, sancionable con apercibimiento según dispone el artículo 77.2 de la LOPDGDD.

Respecto a la tipificación de infracciones del artículo 83.4.a) del RGPD

- Falta de diligencia a la hora de implementar la protección de datos desde el diseño (art 25 RGPD en relación con el artículo 5.1.f) del RGPD), la ausencia, quebrantamiento falta de diligencia debida en la aplicación de medidas de seguridad adecuadas en función del riesgo (art 32 RGPD en relación con el artículo 5.1.f) del RGPD), son consideradas infracciones graves a efectos de prescripción (dos años) conforme señala el artículo 73.d), f), g) y t), de la LOPGDD y sancionables con apercibimiento según dispone el artículo 77.2 de la LOPDGDD.

- La falta de comunicación a los interesados de la brecha de seguridad de fecha 28/06/2020 y de fecha 31/10/2019 (artículo 34 del RGPD en relación con el artículo 5.1.f) del RGPD) considerada infracción leve a efectos de prescripción (un año) conforme señala el artículo 74.ñ) de la LOPGDD y sancionable con apercibimiento según dispone el artículo 77.2 de la LOPDGDD.

En consecuencia, la vulneración de ambos principios (integridad y confidencialidad) constituyen el elemento de la culpabilidad que requiere la imposición de sanción.

Se debe insistir en que la ausencia de consideración del riesgo ya conocido y sancionado anteriormente por esta AEPD en el citado procedimiento sancionador (AP/00049/2018) y tras ambas brechas de seguridad previas a la actual de fechas 28/06/2019 y 31/10/2019, ha derivado nuevamente en el acceso indebido por terceros ajenos a datos personales del interesado y afectando de forma reiterada a los

principios de integridad y de confidencialidad, agrava el reproche culpabilístico y sancionador de la conducta llevada a cabo por la SGICSPJ.

IX

Establece el artículo 58.2 del RGPD 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;

Establece el artículo 76 de la LOPDGDD bajo la rúbrica "*Sanciones y medidas correctivas* ", 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

No obstante, la LOPDGDD en su artículo 77, *Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*, establece lo siguiente:

"1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

(…)

c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.

(…)

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.
La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.
Cuando la competencia corresponda a una autoridad autonómica de protección de datos se estará, en cuanto a la publicidad de estas resoluciones, a lo que disponga su normativa específica".

De las evidencias de las que se dispone conforme a los hechos probados en el presente procedimiento sancionador, consta acreditado por parte del responsable (la SGICSPJ) infracción a lo dispuesto en los artículos 5.1.f) y 25, 32 y 34 en relación con el 5.1.f) del RGPD en los términos antes descritos.

En el supuesto objeto de este procedimiento, se considera que se han tomado las medidas adecuadas para evitar que se vuelva a producir el incidente de seguridad referido, por lo que no se requiere al responsable de la adopción de nuevas medidas.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada, la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER a la **SECRETARÍA GENERAL PARA LA INNOVACIÓN Y CALIDAD DEL SERVICIO PÚBLICO DE JUSTICIA**, **con NIF S2813610I**, por:

1. Infracción del artículo 5.1.f) del RGPD tipificada en el artículo 83.5.a) del RGPD con sanción de apercibimiento.

2. Infracción de los artículos 25 y 32 del RGPD en relación con el artículo 5.1.f) del RGPD, tipificada en el artículo 83.4.a) del RGPD con sanción de apercibimiento.

3. Infracción del artículo 34 del RGPD en relación con el artículo 5.1.f) del RGPD, tipificada en el artículo 83.4.a) del RGPD, con sanción de apercibimiento.

SEGUNDO: NOTIFICAR la presente resolución a la **SECRETARÍA GENERAL PARA LA INNOVACIÓN Y CALIDAD DEL SERVICIO PÚBLICO DE JUSTICIA, con NIF S2813610I**.

TERCERO: COMUNICAR la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 77.5 de la LOPDGDD.

TERCERO: 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