- **Procedimiento Nº: PS/00384/2020**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: D. ***A.A.A.***, en nombre y representación de D. ***B.B.B.*** (en adelante, el reclamante) con fecha 30/07/2019 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra la DIRECCIÓN GENERAL DE LA GUARDIA CIVIL con NIF ***S2816003D*** (en adelante, el reclamado). Los motivos en que basa la reclamación son, en síntesis: la cesión sin consentimiento y la difusión de información personal del afectado contenida en el acuerdo de inicio de suspensión de su licencia de armas, al ser adjuntado dicho documento en un correo electrónico enviado el 17/09/2018 desde la cuenta genérica, *al-cmd-almeria-ia@guardiacivil.org*, titularidad de la Unidad de Intervención de Armas de la Guardia Civil de Almería, a la cuenta genérica *al-pto-canjayar@guardiacivil.es*, titularidad de la Unidad del Puesto de Canjayar, con el fin de que fuese notificado al interesado.

Tras la resolución de inadmisión a trámite, con fecha 06/09/2019, el reclamante interpone recurso de reposición alegando que el correo electrónico fue enviado en el ámbito del trabajo a destinatarios genéricos con datos personales sensibles. Que las cuentas de correo electrónico remitente y destinatario no son personales sino cuentas de departamentos determinados de la Guardia Civil pudiendo ser consultadas por personas indeterminadas y numerosas que formen parte de los mismos.
Con fecha 16/10/2019 se dicta resolución estimatoria.

SEGUNDO: A la vista de los hechos denunciados en la reclamación y de los documentos aportados por el reclamante, 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 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD).

Con fecha 04/12/2019, el reclamado remite a esta Agencia la siguiente información:

1. Que lo que se denomina en la denuncia una cuenta genérica de correo electrónico no es tal. Que la GUARDIA CIVIL dispone de una red de comunicación privada aislada del exterior y a la que solo se puede acceder desde medios oficiales dentro de la cual existe un sistema de mensajería denominado GroupWise en el que cada Unidad o Puesto de Trabajo puede tener asignada una dirección de uso exclusivo por el personal de esa Unidad para comunicaciones internas y al que se accede después de

identificarse con una tarjeta inteligente y una contraseña individual.

2. Que este sistema es utilizado de manera regular para las comunicaciones entre las distintas Unidades, al quedar garantizado que cualquier comunicación o documentación que se remite a través del mismo queda aislada del exterior y mantiene su nivel de confidencialidad.

3. Muestra su disconformidad en relación con la cesión indiscriminada de datos personales. Señala que la instrucción de un procedimiento administrativo requiere que entre los distintos órganos o departamentos involucrados en el mismo se comparta información en aras de poder llevar a efecto la función asignada a la Administración (el control de la documentación que autoriza la tenencia de armas cortas para garantizar el adecuado uso de las mismas y por derivación la seguridad de terceros) y el derecho del administrado a conocer los hechos en que se fundamenta tal actuación y recibir cumplida información al respecto.

4. Que el propio denunciante era uno de los que accedían a dicho sistema de mensajería en la fecha de remisión de la misma junto al Sargento comandante de puesto y otros cuatro guardias civiles. Que el hecho de tener acceso al sistema de mensajería no implica que tal acto se llevase a cabo.

5. Que si después de transcurrido más de un año de dicha comunicación el denunciante no señala que la misma haya tenido trascendencia y con ello un perjuicio para él, es de suponer que quien accedió a la misma fue él o los encargados de notificarle la iniciación del procedimiento.

6. Que en cuanto a la Intervención de Armas remitente el acceso a dicho sistema de mensajería estaba al alcance del personal destinado en dicha unidad, en total once personas, lo que al igual que en el caso anterior no quiere decir que accediesen a dicho documento.

TERCERO: Con fecha 08/11/2020, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al reclamado, por la presunta infracción de los artículos 5.1.f) y 32.1 del RGPD, sancionadas conforme a lo dispuesto en el artículo 58.2.b) del RGPD.

CUARTO: Notificado el acuerdo de inicio, el reclamado el 30/11/2020 presento escrito de alegaciones señalando que se reiteraba en las alegaciones formuladas el 30/05/2020 y que la denuncia del reclamante se refiere a una mera posibilidad de que alguien hubiese accedido a sus datos personales sin que pueda afirmarlo, por lo que las supuestas infracciones no han llegado a materializarse.

QUINTO: Con fecha 14/12/2020 se inició un período de práctica de pruebas, acordándose las siguientes:

- Dar por reproducidos a efectos probatorios la reclamación interpuesta por el reclamante y su documentación, los documentos obtenidos y generados por los Servicios de Inspección que forman parte del expediente E/10062/2019.
- Dar por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio presentadas por el reclamado

- Solicitar al reclamante copia de la documentación que obre en su poder relativa al procedimiento sancionador que por cualquier motivo no hubieran sido aportadas en el momento de la reclamación ó, si lo estima oportuno, cualquier otra manifestación en relación con los hechos denunciados.

SEXTO: Con fecha 27/05/2021 se formuló propuesta de resolución en el sentido siguiente:

1. Que por la Directora de la Agencia Española de Protección de Datos se dirija apercibimiento contra el reclamado, por la infracción de los artículos 5.1.f) y 32 del RGPD, tipificadas, respectivamente, en los artículos 83.5.a) y 83.4.a) del mismo Reglamento.

2. Que se requiera al reclamado para que, en el plazo que se determine, adopte las medidas necesarias para adecuar las operaciones de tratamiento que realiza a la normativa de protección de datos personales, con el alcance expresado en los Fundamentos de Derechos de la propuesta de resolución.

SÉPTIMO: Notificada a la entidad reclamada la citada propuesta de resolución, con fecha 07/06/2021, se recibió en esta Agencia escrito de alegaciones en el que manifiesta de nuevo que no ha quedado acreditado que un tercero haya tenido conocimiento de los datos personales, ni el perjuicio causado al reclamante.

Por otra parte, en relación con el traslado de información de un órgano gestor a otro, se han puesto en marcha acciones para evitar repeticiones futuras, como la Circular elaborada por el Delegado de Protección de Datos (DPD), señalada con el número DPD 1-2020, de 01/12/2020, que ha sido difundida a todas las Unidades y se encuentra disponible en la Intranet del DPD.

Aporta copia de esta Circular, en la que se expone lo siguiente:

"En cuanto a la primera cuestión, garantizar la confidencialidad, siempre que se adjunte a una comunicación electrónica documentación que incluya datos personales, máxime cuando los mismos contengan datos de salud (documentación médica, psicológica o sanitaria de cualquier tipo); relativos a sanciones penales o administrativas (sentencias, notificación de sanciones, procedimientos disciplinarios); o referentes a acciones derivadas de lo anterior (retirada de armamento, citaciones para comparecer, etc.), deberán remitirse en carpetas cifradas con contraseña que será facilitada previa identificación del solicitante como perteneciente a la Unidad u Órgano destinatario como el que debe resolver la cuestión, no debiendo ser facilitada a unidades u órganos intermediadores que no necesitan conocer el contenido concreto de la documentación para su tramitación, limitándose al máximo el número de personas que acceden al mismo y debiendo ser capaces caso de que sea necesario para responder a una denuncia identificar a quienes han accedido al mismo.

En aquellos casos en los que se trate de documentación que debe ser entregada al propio interesado, se procurará que dicha entrega se realice garantizando la máxima reserva posible y que esta sea realizada por su mando directo, evitando que sea efectuada por personal que realiza tareas burocráticas, salvo que dicha entrega se materialice en un sobre cerrado; en estos casos, se deberá hacer constar en el recibo que el receptor recibe la documentación con tales garantías de confidencialidad.

Cuando, se trate de documentos que deban ser firmados por el interesado y devueltos a la

unidad u órgano remitente, se observará lo señalado en el párrafo anterior para la entrega y firma; y se adoptarán las medidas anteriormente referidas para su retorno mediante comunicaciones electrónicas.

En aquellos casos en los que se utilicen otros medios de comunicación, postal, etc., se adoptarán medidas análogas adaptadas al medio siempre con el objetivo de garantizar la confidencialidad de los datos personales.

Deben evitarse prácticas inadecuadas como el imprimir y guardar copia de la documentación remitida o entregada, que comprometen y dificultan mantener la confidencialidad de dicha información a lo largo del tiempo".

De las actuaciones practicadas en el presente procedimiento, han quedado acreditados los siguientes:

HECHOS PROBADOS

PRIMERO: Con fecha 17/09/2018, desde la dirección de correo electrónico *al-cmd-almeria-ia@guardiacivil.org*, asignada a la Unidad de Intervención de Armas de la Guardia Civil de Almería, se remitió un correo electrónico a dirección *al-pto-canjayar@guardiacivil.es*, perteneciente a la Unidad del Puesto de Canjayar, con el asunto *"Rdo. Acuerdo inicio suspensión licencia de armas tipo…* (tipo licencia, nombre, apellidos y DNI del reclamante) *para notificación a interesado"*.

El texto del mensaje es el siguiente:

"Se remite notificación para su entrega al interesado, debiendo remitir copia datada y firmada de su recepción a esta I.A., para su remisión a la Jefatura de Zona, tal como se indica en el c.e. adjunto".

Este correo adjuntaba el documento al que se refiere su asunto, que corresponde al acuerdo de inicio de procedimiento de suspensión de licencia de armas incoado al reclamante por la Dirección General de la Guardia Civil. En este documento constan los datos identificativos del reclamante, su situación administrativa y destino, así como todas las circunstancias de hecho que determinaron la iniciación de dicho procedimiento (actuaciones policiales y judiciales seguidas contra el reclamante por violencia de género).

SEGUNDO: La reclamada ha informado a esta Agencia que dispone de un sistema de mensajería que asigna a cada unidad o puesto una dirección de uso exclusivo por el personal de la unidad de que se trate. En el caso de la dirección de correo electrónico correspondiente a la Unidad del Puesto de Canjayar, se indica que la misma podía ser accedida por el Sargento comandante del puesto, el reclamante y cuatro guardias civiles más.

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

El artículo 58 del RGPD, Poderes, señala:

"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;
(…)".

En primer lugar, el artículo 5 del RGPD establece los principios que han de regir el tratamiento de los datos personales y menciona entre ellos el de *"integridad y confidencialidad"*:

"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").
(…)".

El artículo 5, Deber de confidencialidad, de la LOPDGDD, señala que:

"1. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.

2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.

3. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento".

III

La documentación obrante en el expediente acredita que el reclamado vulneró el artículo 5 del RGPD, principios relativos al tratamiento, en relación con el artículo 5 de la LOPGDD, deber de confidencialidad, materializado en la difusión de datos de carácter personal relativos al reclamante contenida en el acuerdo de inicio de suspensión de su licencia de armas, adjuntado a un correo electrónico que fue

remitido a la cuenta genérica al-pto-canjayar@guardiacivil.es, que es titularidad de la Unidad del Puesto de Canjayar (Almería), la cual estaba al alcance y podía ser accedida por el personal destinado en dicha unidad, un total de cinco personas, además del reclamante.

Este deber de confidencialidad, con anterioridad deber de secreto, tiene como finalidad evitar que se realicen filtraciones de los datos no consentidas por los titulares de los mismos.

Por tanto, ese deber de confidencialidad es una obligación que incumbe no sólo al responsable y encargado del tratamiento sino a todo aquel que intervenga en cualquier fase del tratamiento y complementaria del deber de secreto profesional.

La reclamada ha alegado que no se produce una cesión indiscriminada de datos personales y que la instrucción de un procedimiento administrativo requiere que distintas unidades administrativas o departamentos compartan información. Sin embargo, lo que ocurre en este caso no se ajusta a dicho esquema, por cuanto la información relativa al denunciante no se remite a una unidad que intervenga formalmente en el procedimiento seguido contra el mismo.

Asimismo, el reclamado ha manifestado que las actuaciones no acreditan que un tercero haya accedido a información confidencial relativa al reclamante. Sin embargo, no tiene en cuenta las circunstancias de hecho que han dado lugar al presente procedimiento. En este caso, consta que la notificación del acuerdo de inicio apertura de un procedimiento de suspensión de licencia de armas, seguido contra el reclamante, fue remitida a una cuenta de correo electrónico genérica, titularidad de la Unidad del Puesto de Canjayar, con la finalidad de que fuese entregada al interesado, es decir, al reclamante. Este envío, en sí mismo considerado, ya supone una infracción a la normativa de protección de datos personales, en la medida en que posibilita el acceso a la información relativa al reclamante por parte de terceros. Además, la formalización o cumplimentación de este trámite, con la entrega del acuerdo al reclamante, conlleva que un tercero o varios accedieron a la información. A este respecto, conviene reproducir nuevamente las instrucciones contenidas en el mencionado correo electrónico sobre la entrega de la documentación:

"Se remite notificación para su entrega al interesado, debiendo remitir copia datada y firmada de su recepción a esta I.A., para su remisión a la Jefatura de Zona, tal como se indica en el c.e. adjunto".

IV

El artículo 83.5 a) del RGPD, considera que la infracción de *"los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9"* es sancionable, de acuerdo con el apartado 5 del mencionado artículo 83 del citado RGPD, *"con multas administrativas de 20.000.000€ 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"*.

Por otro lado, la LOPDGDD, a efectos de prescripción, en su artículo 72 indica:

“Infracciones consideradas muy graves:

“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.
(…)”.

V

En segundo lugar, el artículo 32 del RGPD *“Seguridad del tratamiento”*, establece que:

“1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros”.

La vulneración del artículo 32 del RGPD se encuentra tipificada en el artículo 83.4.a) del citado RGPD en los siguientes términos:

“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.
(…)”.

Por su parte, la LOPDGDD en su artículo 71, Infracciones, señala que:

"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".

Y en su artículo 73, a efectos de prescripción, califica de *"Infracciones consideradas graves"*:

"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:
(…)
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.
(…)".

VI

El RGPD define las violaciones de seguridad de los datos personales como *"todas aquellas violaciones de la seguridad que ocasionen la destrucción, perdida o alteración accidental o ilícita de datos personales trasmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos"*.

De la documentación obrante en el expediente se acredita que el reclamado ha vulnerado el artículo 32.1 del RGPD, al producirse un incidente de seguridad consistente en dar traslado de los datos del reclamante mediante un correo corporativo que era accesible a todos los integrantes de la unidad destinataria.

Hay que señalar que el RGPD en el citado precepto no establece un listado de las medidas de seguridad que sean de aplicación de acuerdo con los datos que son objeto de tratamiento, sino que establece que el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas que sean adecuadas al riesgo que conlleve el tratamiento, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, alcance, contexto y finalidades del tratamiento, los riesgos de probabilidad y gravedad para los derechos y libertades de las personas interesadas.

Asimismo, las medidas de seguridad deben resultar adecuadas y proporcionadas al riesgo detectado, señalando que la determinación de las medidas técnicas y organizativas deberá realizarse teniendo en cuenta: la seudonimización y el cifrado, la capacidad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia, la capacidad para restaurar la disponibilidad y acceso a datos tras un incidente, proceso de verificación (que no auditoría), evaluación y valoración de la eficacia de las medidas.

En todo caso, al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, 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 y que pudieran ocasionar daños y perjuicios físicos, materiales o inmateriales.

En este mismo sentido el considerando 83 del RGPD señala que:

"(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como 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, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales".

En el presente caso, tal y como consta en los hechos y en el marco del expediente de investigación E/10062/2019, fue trasladada al reclamado la reclamación presentada para su análisis, solicitando la aportación de información relacionada con la incidencia reclamada en la que muestra su disconformidad con la cesión indiscriminada de datos, si bien manifiesta que el acceso al sistema de mensajería interna estaba al alcance del personal destinado en dicha unidad.

La responsabilidad del reclamado viene determinada por la quiebra de seguridad puesta de manifiesto por el reclamante. El reclamado es responsable de tomar decisiones destinadas a implementar de manera efectiva las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para asegurar la confidencialidad de los datos y, entre ellas, las dirigidas a restaurar la disponibilidad y el acceso a los datos de forma rápida en caso de incidente físico o técnico. Sin embargo, de la documentación aportada con anterioridad a la tramitación del procedimiento, se desconoce si se había adoptado medida alguna a fin de poner fin a incidencias como la que motivó la reclamación.

De conformidad con lo que antecede, resulta que el reclamado es responsable de la infracción del RGPD por la vulneración del artículo 32, infracción tipificada en el artículo 83.4.a) del mismo Reglamento.

VII

No obstante, también 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:

a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.
b) Los órganos jurisdiccionales.
c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.
d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.

e) Las autoridades administrativas independientes.
f) El Banco de España.
g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.
h) Las fundaciones del sector público.
i) Las Universidades Públicas.
j) Los consorcios.
k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

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".

Hay que señalar que la LOPDGDD contempla en su artículo 77 la posibilidad de apercibir al responsable de la infracción y requerirle para que adecúe los tratamientos de datos personales que no se ajusten a sus previsiones, cuando los responsables o encargados del tratamiento enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta Ley Orgánica.

Por este motivo, se elaboró propuesta de resolución para que se acuerde requerir a la

entidad responsable la adopción de las medidas necesarias para llevar a cabo aquella adaptación a la normativa de protección de datos personales, impidiendo que las actuaciones administrativas que realice puedan ser accedidas por personas que no intervienen directamente en su formalización. En concreto, tratándose de notificaciones administrativas, se advertía que tales notificaciones se entreguen directamente al interesado, sin la intermediación de otras unidades ajenas a las que tengan encomendada la actuación de que se trate; o bien, de intentarse esa notificación con la colaboración de alguna otra unidad, evitando siempre que ésta pueda acceder al contenido del acto que se notifica.

Conocida esta respuesta por el reclamado, con ocasión del trámite de audiencia concedido aportó copia de una "Circular" emitida por el DPD, relativa al envío de documentación mediante comunicaciones electrónicas. Analizada esta Circular se constatan algunas mejoras en sus previsiones, como el cifrado de carpetas a las que se accederá mediante la contraseña que se facilite al interesado. Sin embargo, existen otras instrucciones que no cumplen las exigencias mencionadas anteriormente, como son la entrega de documentación a través del "mando directo" del interesado o el envío de documentos "en abierto" para que sean firmados por el interesado y devueltos a la unidad remitente. La misma Circular hace advertencia sobre "prácticas inadecuadas como el imprimir o guardar copia" de la documentación remitida, lo que equivale a reconocer que la posibilidad de que un tercero pueda acceder a la documentación se mantiene.

Por lo tanto, se estima procedente requerir al reclamado para que las notificaciones que deba practicar garanticen la confidencialidad de los datos personales que contienen.

A este respecto, se advierte que no atender los requerimientos de este organismo puede ser considerado como una infracción administrativa grave al *"no cooperar con la Autoridad de control"* ante los requerimientos efectuados, pudiendo ser valorada tal conducta a la hora de la apertura de un procedimiento administrativo sancionador.

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: DIRIGIR UN APERCIBIMIENTO a la entidad ***DIRECCIÓN GENERAL DE LA GUARDIA CIVIL***, con NIF ***S2816003D***, por una infracción de los artículos 5.1.f) y 32 del RGPD, tipificadas en los artículos 83.5.a) y 83.4.a) del RGPD, respectivamente.

SEGUNDO: REQUERIR a la entidad ***DIRECCIÓN GENERAL DE LA GUARDIA CIVIL***, para que, en el plazo de un mes, contado desde la notificación de la presente resolución, adecúe a la normativa de protección de datos personales las operaciones de tratamiento de datos personales que realiza, con el alcance expresado en el Fundamento de Derecho VII. En el plazo indicado, la ***DIRECCIÓN GENERAL DE LA GUARDIA CIVIL*** deberá justificar ante esta Agencia Española de Protección de Datos la atención del presente requerimiento.

TERCERO: NOTIFICAR la presente resolución a ***DIRECCIÓN GENERAL DE LA GUARDIA CIVIL***.

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

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.

938-131120

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