- **Expediente N.º: EXP202212345**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: EL AYUNTAMIENTO DE MADRID, en fecha 24 de octubre de 20222, mediante informe de la Policía Municipal, remitió un informe a la Agencia Española de Protección de Datos. El informe se dirige contra ASOCIACIÓN DE SCOUTS INDEPENDIENTE DE MADRID con NIF G84849546 (en adelante, SCOUTS). Los motivos en que basa el informe son los siguientes:

Se aporta informe policial de fecha 14 de octubre de 2022, en el que se pone de manifiesto que, en fecha 13 de octubre de 2022 se hallaron residuos abandonados en la vía pública, en la zona de (…), encontrándose, entre otros, documentos emitidos por la ASOCIACIÓN DE SCOUTS INDEPENDIENTE DE MADRID, incluyéndose datos de menores de edad e Informes Médicos.

Junto al informe policial se aporta un reportaje fotográfico sobre la ubicación exacta del encuentro de la documentación relativa a los datos personales, así como fotografías de algunos de los documentos encontrados, donde se pueden encontrar datos personales, que en el informe policial se resumen así:

1.- Fotografía “Ficha médica” son 29 unidades con datos personales de personas diferentes en cada ficha. Con el informe, se aporta una fotografía de dicha ficha médica en la que se observan el nombre y apellidos, fecha de nacimiento, DNI, domicilio, teléfono de contacto, y datos médicos como pueden ser vacunación al día, alergias, entre otros.

2. y 3.- Fotografía “Protocolo de actuación frente al covid en las actividades de ocio y tiempo libre” son 29 unidades con datos de personas diferentes en cada documento. Con el informe se aportan dos fotografías de dicho protocolo en el que se aprecia nombre y apellidos, y DNI.

4.- Fotografía “Autorización para hacer el raid solos” son 3 unidades con datos de personas diferentes en cada autorización. En la fotografía que se adjunta al informe, se observa el nombre, apellidos y DNI tanto de un menor como del tutor/padre/madre del mismo.

5.- Fotografía “Autorización para campamento 2021” son 30 unidades con datos de personas diferentes en cada autorización. En la fotografía aportada junto al informe se aprecia el nombre, apellidos, DNI y domicilio del padre/madre/ tutor legal, así como de un menor.

6.- Fotografía “Fichas personal” son 25 unidades con datos de personas diferentes en cada ficha. En la fotografía aportada junto al informe se observa el nombre, apellidos, fecha de nacimiento, DNI, domicilio, números de teléfono y correo electrónico de contacto de un menor, así como los mismos datos del padre y la madre o tutor legal. Se incluye una fotografía del menor.

7.- Fotografía “Consentimiento explícito para la toma de datos” es 1 unidad consentimiento con datos personales. En la fotografía aportada junto al informe se observa nombre, apellidos y DNI.

8.- Fotografía “Consentimiento explícito para el tratamiento de imágenes” es 1 unidad consentimiento con datos personales. En la fotografía aportada se observa nombre, apellidos y DNI.

9.- Fotografía “Fotocopia de Documento Nacional de Identidad” es 1 unidad fotocopia Dni, por las dos caras de un menor de edad.

10.- Fotografía “Fotocopia a color de Tarjeta Sanitaria” es 1 unidad fotocopia Tarjeta Sanitaria.

11.- Fotografía “Informe de traslado de Urgencias 061” es 1 unidad original informe sanitario. En la fotografía aportada se observa el informe de transporte sanitario urgente, que incluye nombre, apellidos y domicilio de un menor de edad.

12.- Fotografía “Documento de identificación de socio” es 1 unidad original. En la fotografía aportada se observa que dicho carnet recoge nombre, apellidos y domicilio, entre otros datos.

SEGUNDO: Con fecha 29 de junio de 2023, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, por la presunta infracción del Artículo 5.1.f) del RGPD y Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD y Artículo 83.5 del RGPD.

El acuerdo de inicio fue enviado, conforme a las normas establecidas en la LPACAP, mediante notificación postal, siendo devuelto a origen por desconocido en fecha 10 de julio de 2023, como consta en el certificado que obra en el expediente, procediendo a su publicación en el Boletín Oficial del Estado, en fecha 3 de agosto de 2023, de acuerdo con lo establecido en el artículo 44 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

TERCERO: Notificado el citado acuerdo de inicio conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP) y transcurrido el plazo otorgado para la formulación de alegaciones, se ha constatado que no se ha recibido alegación alguna por la parte reclamada.

El artículo 64.2.f) de la LPACAP -disposición de la que se informó a la parte reclamada en el acuerdo de apertura del procedimiento- establece que si no se efectúan alegaciones en el plazo previsto sobre el contenido del acuerdo de iniciación, cuando

éste contenga un pronunciamiento preciso acerca de la responsabilidad imputada, podrá ser considerado propuesta de resolución. En el presente caso, el acuerdo de inicio del expediente sancionador determinaba los hechos en los que se concretaba la imputación, la infracción del RGPD atribuida a la reclamada y la sanción que podría imponerse. Por ello, tomando en consideración que la parte reclamada no ha formulado alegaciones al acuerdo de inicio del expediente y en atención a lo establecido en el artículo 64.2.f) de la LPACAP, el citado acuerdo de inicio es considerado en el presente caso propuesta de resolución.

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran hechos probados los siguientes,

HECHOS PROBADOS

PRIMERO: Consta que en fecha 24 de octubre de 2022 tiene entrada un informe de la Policía Municipal de Madrid en el que se pone de manifiesto que el 13 de octubre de 2022 se hallaron documentos emitidos por los SCOUTS con datos de menores de edad e informes médicos.

SEGUNDO: Consta que, junto al informe policial se adjuntaba un reportaje fotográfico del lugar en el que se había encontrado la documentación, así como fotografías de algunos de los documentos encontrados.

FUNDAMENTOS DE DERECHO

I
Competencia y normativa aplicable

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: "Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."

II
Cuestiones previas

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 y 4.2 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que SCOUTS

realiza la recogida y conservación de, entre otros, los siguientes datos personales de personas físicas: nombre y apellido, fecha de nacimiento, DNI, datos de salud, entre otros tratamientos.

SCOUTS realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y medios de tal actividad, en virtud del artículo 4.7 del RGPD.

El artículo 4 apartado 12 del 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*".

En el presente caso, consta una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad, al haberse dejado sin ningún tipo de seguridad en la vía pública documentación con información personal sobre menores de edad.

Dentro de los principios del tratamiento previstos en el artículo 5 del RGPD, la integridad y confidencialidad de los datos personales se garantiza en el apartado 1.f) del artículo 5 del RGPD. Por su parte, la seguridad de los datos personales viene regulada en el artículo 32 RGPD, que reglamenta la seguridad del tratamiento.

III
Principio de integridad y confidencialidad

El artículo 5.1.f) "*Principios relativos al tratamiento*" del RGPD establece:

"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, de la documentación obrante en el expediente, consta que los datos personales de los afectados fueron indebidamente expuestos a terceros en la vía pública, lo que denota una absoluta falta de aplicación de medidas técnicas y organizativas destinadas a garantizar el principio de confidencialidad.

De conformidad con las evidencias de las que se dispone en esta fase de resolución de procedimiento sancionador, se considera que los hechos conocidos son constitutivos de una infracción, imputable a SCOUTS, por vulneración del artículo 5.1.f) del RGPD.

IV
Tipificación de la infracción del artículo 5.1.f) del RGPD

La citada infracción del artículo 5.1.f) del RGPD supone la comisión de las infracciones tipificadas en el artículo 83.5 del RGPD que bajo la rúbrica *"Condiciones generales para la imposición de multas administrativas"* dispone:

"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; (…)"*

A efectos del plazo de prescripción, el artículo 72 "*Infracciones consideradas muy graves*" de la LOPDGDD indica:

"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
Sanción por la infracción del artículo 5.1.f) del RGPD

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone en el presente momento de resolución de procedimiento sancionador, se considera que el balance de las circunstancias contempladas en el artículo 83.2 del RGPD y 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 5.1.f) del RGPD, permite fijar una multa de 1.000 € (mil euros).

VI
Seguridad en el tratamiento

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".

En el presente caso, se ha tenido conocimiento del abandono de documentación en la vía pública, en la que figuran datos personales de menores, incluyendo datos de salud, lo que supone una vulneración de la normativa de protección de datos.

Los hechos puestos en cuestión en el informe presentado se concretan en la existencia de un incidente de seguridad de los SCOUTS al permitir que documentación con datos de carácter personal, (entre los que se incluyen datos de salud de menores) fueran abandonados, de tal manera que la seguridad de los datos no se vio garantizada, poniéndose en riesgo la confidencialidad de los mismos.

De la documentación obrante en el expediente se ofrecen indicios evidentes de que SCOUTS ha vulnerado el artículo 32.1 del RGPD, al producirse una brecha de seguridad en la medida en que no había implantado medidas de seguridad apropiadas que garanticen la confidencialidad de datos de carácter personal contenidos en documentos que fueron abandonados por SCOUTS.

En el presente supuesto, la responsabilidad de SCOUTS viene determinada porque es responsable de tomar decisiones destinadas a implementar de manera efectiva las medidas de seguridad apropiadas para garantizar un nivel de seguridad adecuado al riesgo, lo que no ha hecho. Responsabilidad que resulta exigible, aunque no se hubiera producido una brecha de datos personales.

Por tanto, de conformidad con las evidencias de las que se dispone en este momento de resolución de procedimiento sancionador, se considera que los hechos conocidos son constitutivos de una infracción, imputable a SCOUTS, por vulneración del artículo 32 del RGPD, al no haber tenido la capacidad de garantizar los datos personales, incluyendo los de menores de edad, entre ellos, los datos de salud.

IV
Tipificación y calificación de la infracción

Los hechos conocidos son constitutivos de una infracción, imputable a SCOUTS**,** tipificada en el artículo 83.4.a), que estipula lo siguiente:

"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;*

A efectos del plazo de prescripción de las infracciones, el artículo 73. (infracciones consideradas graves) de la LOPDGDD, indica:

"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."*

IV
Sanción por la infracción del artículo 32 del RGPD

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone en el presente momento de resolución de procedimiento sancionador, se considera que el balance de las circunstancias contempladas en el artículo 83.2 del RGPD y 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 32 del RGPD, permite fijar una sanción de multa administrativa de 1.000 € (mil euros).

Por lo tanto, a tenor de lo anteriormente expuesto, por la Directora de la Agencia Española de Protección de Datos,
SE ACUERDA:

PRIMERO IMPONER a **ASOCIACIÓN DE SCOUTS INDEPENDIENTE DE MADRID**, con NIF **G84849546**,

-por la presunta infracción del Artículo 5.1.f) del RGPD tipificada en el Artículo 83.5 del RGPD, con multa administrativa de 1.000 € (mil euros)

-por la presunta infracción del artículo 32, del RGPD tipificada en el artículo 83.4 del RGPD, con multa administrativa de 1.000 € (mil euros).

SEGUNDO: NOTIFICAR la presente resolución a ***ASOCIACIÓN DE SCOUTS INDEPENDIENTE DE MADRID***.

TERCERO: Esta resolución será ejecutiva una vez finalice el plazo para interponer el recurso potestativo de reposición (un mes a contar desde el día siguiente a la notificación de esta resolución) sin que el interesado haya hecho uso de esta facultad. Se advierte al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el art. 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP), en el plazo de pago voluntario establecido en el art. 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso, indicando el NIF del sancionado y el número de procedimiento que figura en el encabezamiento de este documento, en la cuenta restringida nº ***IBAN: ES00-0000-0000-0000-0000-0000***, abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A.. En caso contrario, se procederá a su recaudación en período ejecutivo.

Recibida la notificación y una vez ejecutiva, si la fecha de ejecutividad se encuentra entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si se encuentra entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

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.

938-16012024

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