



RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR POR INFRACCIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS PERSONALES

Resolución	RPS-2025/029
Procedimiento Sancionador	PS-2024/005
Expediente	RCO-2022/142
Entidad incoada	Dirección General de Asistencia Sanitaria y Resultados en Salud - Centro de Emergencias Sanitarias 061 (Servicio Andaluz de Salud)
Motivo de la reclamación	Acceso indebido a datos personales de la reclamante y sus familiares durante un curso de formación al personal de la empresa
Artículos afectados	Artículo 32 RGPD Artículo 5.1.f) RGPD

Abreviaturas:

RGPD. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

LOPDGDD. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

LOPDP. Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

LTPA. Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía

ESTATUTOS CTPDA. Estatutos del Consejo de Transparencia y Protección de Datos de Andalucía, aprobados por Decreto 434/2015, de 29 de septiembre.

LPAC. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas

LRJSP. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

ENS. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

ANTECEDENTES

Primero. El 17 de noviembre de 2022, [XXXXX] (en adelante, la persona reclamante), interpuso reclamación ante el Consejo de Transparencia y Protección de Datos de Andalucía (en adelante, el Consejo) contra contra la, en aquel momento Empresa Pública de Emergencias Sanitaria 061, cuyas funciones actualmente realiza el Centro Emergencias Sanitaria 061 adscrito a la Dirección General de Asistencia Sanitaria y Resultados en Salud del Servicio Andaluz de Salud (en adelante, el órgano reclamado), por una presunta infracción de la normativa de protección de datos personales.

En la citada reclamación se exponía lo siguiente:

"[...] El pasado mes de Junio *una persona* en formación de teleoperadora para el 061 de nnnn, publicó en Facebook de forma pública un primer estado en el que decía " En mi trabajo tengo acceso a determinadas *[informaciones]*...". Al día siguiente publicó, también de forma pública, las terminaciones de los DNI de 3 miembros de mi unidad familiar.[...]

A primeros de octubre recibí una primera respuesta del 061 con la que no quedé conforme ya que decía que ella no tenía acceso a mis datos clínicos, que en el curso sólo se accedía





a datos administrativos. Les volví a poner una reclamación donde decía que esa carta no daba respuesta a mi escrito [...].

El pasado 28 de octubre recibí respuesta de mi segunda reclamación y me dicen que "...la posibilidad de que la persona a la que se refiere en su escrito sea la que ha accedido a los datos de sus familiares y posteriormente los haya divulgado en redes sociales existe; no obstante nosotros, no estamos en condiciones de asegurar que hubiese sido esa persona concreta la que accediese y fotografiase esos datos, ya que, como explicamos en la entrevista que mantuvimos, la entrada en los módulos de formación se hace a través de claves genéricas que imposibilitan una trazabilidad única del acceso a los datos por parte de una persona concreta".

He consultado con un abogado y con lo que ahora mismo tengo sólo puedo denunciar al 061 y a [*nombre empresa concesionaria emergencias*] por no tener medios suficientes para confirmarme que ella ha accedido a mis datos personales.

Mi intención es denunciar sólo a ella por haber usado, según mi sospecha, el curso para:

1º- aprovechar el curso de formación para obtener información nuestra.

2º- aprovechar que ha obtenido esta información y publicar las terminaciones de 3 miembros de mi unidad familiar [...]

Le mando capturas de pantalla, de los estados a los que me refiero a mi publicación cebo del día 9 de octubre a las [*hh:mm*] a su publicación el día [*dd/mm*]. [...]"

Se adjuntaba a la reclamación copias de pantallas de facebook con los comentarios que indica en la reclamación.

Segundo. En virtud de los artículos 37 y 65 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), con fecha 5 de Diciembre de 2022 se dio traslado de la reclamación al Delegado de Protección de Datos del órgano reclamado, efectuándose el 20 de diciembre de 2022, un segundo traslado al presentar la reclamante la misma reclamación ante la AEPD, para que, en el plazo máximo de un mes, comunicara la respuesta dada a la reclamación y, en su caso, las actuaciones realizadas en relación con la misma.

Con fecha 19 de enero de 2023, se recibe respuesta del órgano reclamado donde dice lo siguiente:

"El día [*dd/mm/aa*] entre [*hh:mm*] y las [*hh:mm*] desde el entorno de formación en [*XXX*] se realizaron varias búsquedas sobre usuarios con apellidos [*apellidos de la persona reclamante*]. Estas consultas se hicieron todas con el usuario de formación [*nnn*]. El acceso se realizó a los registros de la Base de Datos de Usuarios que incluye datos de contacto (domicilio postal, teléfono y correo electrónico) y administrativos. No se accedió a datos de carácter clínico o de salud. Consta que, con fecha [*dd/mm/aa*], [*XXXXXX*], en horario de [*hh:mm*] a [*hh:mm*] participó en las sesiones de formación para el proceso selectivo de gestor Telefónico, impartido por la empresa [*nombre empresa concesionaria emergencias*], adjudicataria del servicio de teleoperación. Su participación se realizó con el código de usuario de formación indicado [...]"

También se manifiesta en dicho escrito, lo siguiente:

"Que el día [*dd/mm/aa*] se cambió la conexión del entorno de formación del sistema de atención de llamadas Centros en Red (CCR) con la Base de Datos de Usuario (BDU). A partir de ese momento la conexión es con el entorno de preproducción de BDU. Preproducción es el entorno de pruebas de validación relacionadas con el desarrollo de los aplicativos. Que el día [*dd/mm/aa*] se desconectó la conexión entre el entorno de formación de Centros en Red y el entorno de preproducción de BDU. Se encuentra en desarrollo un aplicativo es-



pecífico para formación en Centros en Red que devuelva, ante una consulta, datos disociados y aleatorios.”

En consecuencia, a partir del día 26 de octubre de 2022 las personas que reciben la formación para el Sistema de despacho de llamadas en los Centros de Coordinación no acceden, en ningún caso, a ningún dato, ni administrativos ni clínicos, de pacientes reales.”.

Tercero. Una vez que la reclamación inició su tramitación con arreglo al procedimiento establecido en el Título VIII de la LOPDGDD, y en virtud de los artículos 65.5 y 67.1 de la misma, con fecha 20 de enero de 2023 el Director del Consejo ordenó admitir a trámite la reclamación presentada contra el órgano reclamado y también el inicio de actuaciones previas de investigación a los efectos de lograr una mejor determinación de los hechos y circunstancias que justificaran la tramitación de un posible procedimiento sancionador.

Cuarto. En el marco de dichas actuaciones y con el objeto de completar la información relacionada con los hechos denunciados, el 20 de enero de 2023, desde el Consejo se requirió al DPD, para que, en el plazo de 15 días, remitiera información y documentación.

En respuesta al requerimiento anterior, con fecha 3 de febrero de 2023, el órgano reclamado remite contestación reiterándose en lo expresado anteriormente, y manifestando que en ningún caso las personas en formación han accedido a datos clínicos y de salud, únicamente han accedido a datos de contacto y administrativos de usuarios del Servicio Andaluz de Salud, estimando, el órgano reclamado, razonable que dichos alumnos accedieran a datos reales de pacientes, por los motivos que aduce en su escrito.

Por último, señala el organismo reclamado que “ [...] que desde el día 26 de octubre de 2022 las personas que reciben la formación para el Sistema de despacho de llamadas en los Centros de Coordinación no acceden, en ningún caso, a ningún dato de pacientes reales.”.

Quinto. Acuerdo de inicio de procedimiento sancionador. (arts. 68 LOPDGDD; Art. 64 LPAC).

1. El 11/04/2024 el director del Consejo dictó Acuerdo de Inicio de procedimiento sancionador contra el Centro de Emergencias Sanitarias 061 (Servicio Andaluz de Salud) con CIF Q9150013B, por la presunta infracción del artículo 32 RGPD, tipificadas en el artículo 83.4.a) RGPD, en relación con la ausencia de medidas técnicas y organizativas apropiadas para garantizar la confidencialidad de los datos personales y evitar así la divulgación de éstos a terceros; y la vulneración del artículo 5.1.f) del RGPD, sobre confidencialidad, tipificada en el artículo 83.5.a) RGPD.

2. Notificado el acuerdo de inicio al órgano reclamado el 16/04/2024, éste no presentó alegaciones.

Sexto. Propuesta de resolución. (art. 89 LPAC).

1. Finalizada la instrucción del procedimiento, se procedió a realizar la correspondiente propuesta de resolución, estableciendo el plazo de diez días para la formulación de alegaciones, de conformidad con el artículo 89.2 LPACAP y en relación con el artículo 73.1 de la misma norma.

2. Notificada la propuesta de resolución al órgano reclamado el 2 de enero de 2025, éste no presentó alegaciones.

HECHOS PROBADOS



De los documentos obrantes en el expediente y de las actuaciones practicadas, pueden considerarse como hechos probados:

Único. Se ha constatado el acceso a datos personales de carácter identificativo [incluyendo nombre y apellidos, domicilio postal, número de teléfono y dirección de correo electrónico], así como a datos administrativos de carácter sanitario de usuarios del Servicio Andaluz de Salud, por parte de personas sin vínculo contractual alguno con la Empresa Pública ni con la empresa adjudicataria del servicio, las cuales se encontraban en un proceso de formación previa con vistas a su posible incorporación como teleoperadores.

FUNDAMENTOS JURÍDICOS

Primero. Sobre la competencia.

1. De conformidad con lo previsto en el artículo 57.1 y 64.2 LOPDGDD y el artículo 43.1 LTPA en relación con el artículo 3.1 LTPA corresponde a este Consejo como autoridad autonómica de protección de datos personales y dentro de su ámbito competencial, el ejercicio de la potestad sancionadora y de los poderes previstos en el artículo 58 RGPD.

2. La competencia para la adopción de esta resolución reside en el Director, conforme al art. 48.1.i) LTPA y el art. 10.3.i) Estatutos.

3. Debe destacarse a su vez que, en virtud del artículo 16.5 del Decreto 434/2015, de 29 de septiembre, por el que se aprueban los Estatutos del Consejo de Transparencia y Protección de Datos de Andalucía, “[e]l personal funcionario del Consejo, cuando realice funciones de investigación en materias propias de la competencia del Consejo, tendrá el carácter de agente de la autoridad”, con las consecuencias que de aquí se derivan para los sujetos obligados en relación con la puesta a disposición de la información que les sea requerida en el curso de tales funciones investigadoras.

4. Este procedimiento se inicia como consecuencia de una presunta vulneración de la normativa de protección de datos por parte de una entidad bajo el control del Consejo en lo que respecta al cumplimiento de dicha normativa. Por ello, en el presente caso, solo serán analizadas y valoradas aquellas cuestiones planteadas por el reclamante, en relación con la materia de protección de datos personales, que queden incluidas dentro de la esfera de responsabilidad de la mencionada entidad.

Segundo. Sobre el tratamiento de datos personales.

1. El artículo 1.1 RGPD establece que “[e]l presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos”. Según el artículo 4.1 RGPD se entiende por «dato personal», “[t]oda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona”.

2. El artículo 2.1 RGPD dispone respecto al ámbito de aplicación del mismo que “[e]l presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero”, definiéndose el concepto de «tratamiento» en el artículo 4.2 RGPD como “cual-



quier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción”.

De acuerdo con las anteriores definiciones, los datos relativos al nombre y apellidos, domicilio postal, teléfono, correo electrónico y los datos administrativos sanitarios de una persona, han de considerarse datos personales a los que se ha realizado un tratamiento. Por consiguiente, tanto los datos personales tratados como el tratamiento que se realice de los mismos ha de someterse a lo establecido en la normativa sobre protección de datos personales.

Las operación de tratamiento que se observa en relación con los datos personales es facilitar el acceso de las personas que se forman para su eventual incorporación a la plantilla de teleoperadores del 061 a la Base de Datos de Usuarios (BDU) con datos reales del entorno de producción.

En el registro de Actividades de Tratamiento se recoge la actividad de tratamiento “Sistema de despacho de llamadas”.

3. Por último el Art. 4.7 RGPD considera responsable del tratamiento a aquella “...autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento...” Esta identificación del responsable de tratamiento debe entenderse completada por la concreción del tercero realizada en el art. 4.10 RGPD, e incluir por tanto a las “personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable...”.

El responsable de los tratamientos, actualmente es la Dirección General de Asistencia Sanitaria y Resultados en Salud (Centro de Emergencias Sanitarias 061) del Servicio Andaluz de Salud, con CIF Q9150013B (Art. 4.7 RGPD).

Tercero. Sobre la calificación jurídica de los hechos.

1. Preceptos infringidos.

El artículo 5.1.f RGPD indica “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 32 RGPD se refiere a la “seguridad del tratamiento”, y en su apartado primero establece que:

“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".

En este mismo sentido, el considerando 83 RGPD señala que: *"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".*

De conformidad con la Disposición Adicional Primera de la LOPDGDD:

"2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado"

En el Anexo II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad se prevé la siguiente medida, siendo de aplicación a todos los sistemas que están categorizados como de seguridad BÁSICA, MEDIA o ALTA.

"- [op.acc.4.3] Necesidad de conocer y responsabilidad de compartir: los privilegios se asignarán de forma que las entidades, usuarios o procesos sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones o funciones."

Recordemos que el Esquema Nacional de Seguridad es de obligado cumplimiento para todas las administraciones públicas desde el 5 de noviembre de 2017.

2. Consideraciones jurídicas sobre la existencia de infracción.

De la documentación incorporada al expediente y tras la práctica de las actuaciones previas de investigación, ha quedado acreditado y así ha sido reconocido expresamente por la propia Empresa Pública que se ha producido un acceso a datos personales identificativos (nombre y apellidos, domicilio postal, número de teléfono, correo electrónico) y a datos administrativos de carácter sanitario de usuarios del Servicio Andaluz de Salud, por parte de personas no vinculadas contractualmente ni con la Empresa Pública ni con la empresa adjudicataria del servicio. Dichas personas se encontraban participando en un proceso de formación previa con vistas a su eventual incorporación a la plantilla de teleoperadores del servicio.

La razón que permitió dicho acceso se encuentra en la configuración del sistema informático empleado durante la formación, que se encontraba conectado con la base de datos en entorno de producción del servicio 061. Esta contenía datos reales de carácter personal de los usuarios, en lugar de estar conectado a un entorno de formación o reproducción con datos ficticios o anonimizados, como sería exigible en tales circunstancias.

Este Consejo no aprecia fundamento alguno que justifique que personas en formación, sin vínculo laboral vigente, deban tener acceso a datos reales de usuarios del sistema sanitario. El



conocimiento de dicha información no resulta necesario para el desarrollo de su actividad formativa, cuya finalidad es, exclusivamente, prepararlos para una eventual incorporación al servicio. En este sentido, el órgano responsable del tratamiento no ha aportado justificación alguna que respalde la necesidad de dicho acceso.

La situación descrita pone de manifiesto la ausencia de medidas técnicas y organizativas adecuadas dirigidas a garantizar un nivel de seguridad adecuado al riesgo, en los términos exigidos por el artículo 32 del RGPD. Esta deficiencia supuso una exposición indebida de los datos personales de los usuarios del servicio 061, materializándose en este caso concreto en la divulgación no autorizada de los datos personales de la persona reclamante y de personas vinculadas a la misma.

Como se ha señalado, la falta de aplicación de medidas de seguridad adecuadas posibilitó que personas en formación accedieran sin restricciones a la base de datos de usuarios del servicio 061. Tal acceso pudo mantenerse durante un periodo de tiempo no determinado y afectó potencialmente a un volumen significativo de personas, dada la magnitud del servicio (según datos del avance de memoria anual de 2022, se atendieron 3.160.604 llamadas). En uno de los casos, una persona en formación utilizó indebidamente los datos accedidos para fines personales, incluyendo su publicación en redes sociales, lo cual generó perjuicios efectivos a los derechos y libertades de las personas afectadas y provocó la pérdida de control sobre su información personal.

La situación descrita constituye una vulneración del principio de confidencialidad en el tratamiento de los datos personales, tal y como establece el artículo 5.1.f) del RGPD, el cual impone la obligación de garantizar la protección frente al acceso no autorizado o ilícito por parte de terceros no habilitados.

No obstante, procede dejar constancia de que, a partir del 26 de octubre de 2022 [fecha anterior a la presentación de la reclamación], se modificó el procedimiento de formación de los operadores. Desde dicha fecha, las personas en formación no tienen acceso en ningún caso a datos reales de pacientes, siendo derivadas exclusivamente a un entorno de reproducción que contiene datos ficticios. Asimismo, se encuentra en desarrollo un entorno de formación específico, que garantiza la completa desvinculación de los entornos reales del sistema y la protección de los datos personales.

En consecuencia se constata que los ilícitos administrativos que se imputan al órgano reclamado son, por un lado, la falta de medidas de seguridad técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuada prevista en el artículo 32 del RGPD, tipificada en el artículo 83.4.a) RGPD, en relación con la ausencia de medidas técnicas y organizativas apropiadas para garantizar la confidencialidad de los datos personales y evitar así la divulgación de éstos a terceros; y por otro lado, la vulneración del principio de confidencialidad previsto en el artículo 5.1.f) del RGPD de la LOPDGDD, tipificada en el artículo 83.5.a) RGPD.

3. Tipificación.

El incumplimiento de las disposiciones relativas a "los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9" del RGPD tipificada en el artículo 83.5.a) RGPD; calificada a efectos de prescripción en la LOPDGDD como infracción muy grave por vulneración sustancial del artículo 5.1.f) RGPD "Principio de confidencialidad" y, en particular, en el artículo 72.1 i) LOPDGDD:

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



El incumplimiento de las disposiciones relativas a "las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43" del RGPD tipificada en el artículo 83.4.a) RGPD; calificada a efectos de prescripción en la LOPDGDD como infracción grave por vulneración sustancial/formal del artículo 32 RGPD "Seguridad del tratamiento" y, en particular, según el artículo 73.1 f) LOPDGDD:

"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".

Todo ello, sin perjuicio de que, como consecuencia de la presente reclamación, el órgano reclamado ha procedido a adoptar diversas medidas con el fin de dar cumplimiento a la normativa de protección de datos personales.

Cuarto. Sobre la identificación de la entidad responsable (art. 89.3 LPAC).

De conformidad con lo previsto en el artículo 70.1 LOPDGDD, se identifica como entidad responsable de la infracción, a Centro de Emergencias Sanitarias 061 .

Quinto. Declaración de la infracción y medidas a adoptar (art. 77.2 LPAC y 58.2 RGPD).

1. El artículo 77 LOPDGDD establece el régimen sancionador aplicable a determinadas categorías de responsables o encargados del tratamiento; incluyendo, entre otros a:

"a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.

[...]

c) [...] 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 [...]"

En el mencionado artículo, en su apartado 2, se señala que:

"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 declarando la infracción y estableciendo, en su caso, las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido, con excepción de la prevista en el artículo 58.2.i del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.[...]"

Así, de acuerdo con el artículo 77.2 LOPDGDD, procede declarar la infracción o infracciones antes descritas.

2. Por otra parte, en relación con las medidas que proceda adoptar, el artículo 58.2 RGPD dispone que:

"Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación: [...]"



d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado;[...]".

Respecto a las posibles medidas que proceda adoptar no se considera preciso ordenar al órgano incoado la puesta en marcha de medidas adicionales a las ya adoptadas.

Sexto. Notificaciones y comunicaciones.

En relación con la notificación de la resolución del procedimiento sancionador, el artículo 77.2 LOPDGDD dispone que "*[l]a 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*".

Además, el artículo 77.4 LOPDGDD señala que "*[s]e 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*", y el 77.56 LOPDGDD, que "*[s]e 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*".

En virtud de todo lo expuesto, el director del Consejo de Transparencia y Protección de Datos de Andalucía dicta la siguiente,

RESOLUCIÓN

Primero. Declarar que la Dirección General de Asistencia Sanitaria y Resultados en Salud (Centro de Emergencias Sanitarias 061), con CIF NNNNN, ha cometido las siguientes infracciones:

-Infracción tipificada el artículo 83.4 RGPD y calificada a efectos de prescripción como grave en el artículo 73.e) LOPDGDD por vulneración sustancial del artículo 32 RGPD referido a la seguridad del tratamiento en relación con la ausencia de medidas técnicas y organizativas apropiadas para garantizar la confidencialidad de los datos personales.

-Infracción tipificada en el art. 83.5. RGPD y calificada a efectos de prescripción como muy grave en el artículo 72.a) LOPDGDD por vulneración sustancial del artículo 5.1.f) RGPD referido al principio de confidencialidad en relación con la divulgación indebida de datos a terceros.

Segundo. No se considera preciso ordenar al órgano incoado la puesta en marcha de medidas adicionales a las ya adoptadas.

Tercero. Que se notifique la presente resolución al órgano infractor y a la Dirección Gerencia del Servicio Andaluz de Salud como órgano superior jerárquico.

Cuarto. Que se comunique la presente resolución al Defensor del Pueblo Andaluz, de conformidad con lo establecido en el artículo 77.5 LOPDGDD

En consonancia con lo establecido en el artículo 50 LOPDGDD, la presente Resolución se hará pública, disociando los datos que corresponda, una vez haya sido notificada a los interesados.

El incumplimiento de esta resolución podría comportar la comisión de la infracción considerada en el artículo 72.1.m) LOPDGDD, sancionable de acuerdo con el artículo 58.2 RGPD.

Contra esta Resolución, que pone fin a la vía administrativa, cabe interponer recurso potestativo de re-



posición ante este Consejo, en el plazo de un mes, o interponer directamente recurso contencioso-administrativo ante el Juzgado de lo Contencioso Administrativo de Sevilla que por turno corresponda, en el plazo de dos meses, en ambos casos a contar desde el día siguiente al de su notificación, de conformidad con lo dispuesto en los artículos 30.4, 123 y 124 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y en los artículos 8.3 y 46.1 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.

No obstante, al tratarse de un acto en materia de sanciones, el demandante podrá elegir alternativa-mente interponer el citado recurso contencioso-administrativo ante el juzgado o el tribunal en cuya circunscripción tenga aquél su domicilio, siempre entendiendo esta elección limitada a la circunscripción del Tribunal Superior de Justicia de Andalucía, de conformidad con lo dispuesto en los apartados segundo y tercero del artículo 14.1 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.

Conforme a lo previsto en el art. 90.3.a) LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta ante este Consejo su intención de interponer recurso contencioso-administrativo y traslada al mismo, una vez interpuesto, la documentación que acredite su presentación. Si el Consejo no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo correspondiente o en dicho recurso no se solicitara la suspensión cautelar de la resolución, se daría por finalizada la mencionada suspensión.

EL DIRECTOR DEL CONSEJO DE TRANSPARENCIA Y PROTECCIÓN DE DATOS DE ANDALUCÍA

La resolución original consta firmada electrónicamente