- **Expediente N.º: EXP202414356**

RESOLUCIÓN DE TERMINACIÓN DEL PROCEDIMIENTO POR RECONOCIMIENTO DE RESPONSABILIDAD Y PAGO VOLUNTARIO

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

ANTECEDENTES

PRIMERO: Con fecha 12 de abril de 2025, la Presidencia de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a ***A.A.A.*** (en adelante, ***A.A.A.***), mediante el acuerdo que se transcribe:

<<

Expediente N.º: EXP202414356

ACUERDO DE INICIO DE PROCEDIMIENTO SANCIONADOR

De las actuaciones practicadas por la Agencia Española de Protección de Datos y en base a los siguientes

HECHOS

PRIMERO: La Agencia Española de Protección de Datos (AEPD) ha tenido conocimiento de ciertos hechos que podrían constituir posibles infracciones imputables a ***A.A.A.*** con NIF ******NIF.1*** (en adelante, ***A.A.A.,*** la farmacia o parte denunciada), en tanto que titular de la oficina de farmacia ******NIF.2,*** a raíz de una denuncia presentada por la Direcció General D'Ordenació i Regulació Sanitària de la Comunidad Autónoma de Cataluña, tras la realización de inspecciones a oficinas de farmacia en el ejercicio de sus competencias.

La denuncia tuvo entrada en la AEPD el 7 de septiembre de 2023, remitida por la Autoritat Catalana de Protecció de Dades en cumplimiento del artículo 14 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

En la misma, la Direcció General D'Ordenació i Regulació Sanitària alerta sobre posibles vulneraciones de la normativa de protección de datos respecto al tratamiento de datos personales de residentes en centros geriátricos por parte de determinadas oficinas de farmacia como, entre otros: presuntos accesos y cesiones ilícitos a datos personales de salud o el intercambio de datos personales a través de medios electrónicos no seguros

SEGUNDO: Como consecuencia de los hechos conocidos, el 19/10/2023 la Directora de la Agencia Española de Protección de Datos, instó a la Subdirección General de Inspección de Datos (SGID) a iniciar las actuaciones previas de investigación a las que se refiere el artículo 67 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección

de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD). Todo ello a fin de recopilar los elementos de juicio necesarios para conocer en profundidad los hechos descritos y los tratamientos llevados a cabo para, en su caso, determinar las consecuencias que de ellos pueden derivarse para los derechos y libertades de las personas.

TERCERO: 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 las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VIII, de la LOPDGDD.

Como consecuencia de las actuaciones realizadas, se ha tenido conocimiento de los siguientes extremos:

1. **Respecto a la información facilitada por el Servicio de Inspección de Farmacia.**

En su escrito de respuesta, de fecha de registro 22/01/2024, el Servicio de Inspección de Farmacia aporta la siguiente información respecto de la farmacia ***A.A.A.***:

"Según la información a disposición de este Servicio de Inspección de Farmacia de la facturación de medicamentos a cargo del Servei Català de la Salut (CatSalut), los absorbentes de incontinencia urinaria (pañales), dispensados a los residentes de la ******RESIDENCIA.1*** *no son facturados a la Farmacia* ***B.B.B. (***NIF.3)*** *sino a otra a oficina de farmacia,* ******NIF.2****, situada en la calle* ******DIRECCIÓN.1,*** *el titular de la cual es* ***A.A.A.*** *(a partir de ahora Farmacia* ***A.A.A.****).*
Por este motivo, el 23 de noviembre de 2023, se realizó una inspección a la Farmacia ***A.A.A. (***NIF.2****):*

- *Durante la inspección, el titular de la oficina de farmacia confirmó que los pañales para los residentes de la* ******RESIDENCIA.1*** *eran dispensados desde su oficina de farmacia.*
- *Que hacía unos 2 años el señor* ***C.C.C.*** *(presentado a través del gerente de* ******EMPRESA.1****), le propuso realizar la dispensación de pañales a una residencia a la cual "su farmacia" realizaba la dispensación de medicamentos en SPD.*
- *El señor* ***A.A.A.*** *informó que inicialmente trabajaba con la Farmacia* ***D.D.D.*** *(*******NIF.4****), de la calle* ******DIRECCIÓN.2*** *y ahora con la Farmacia* ***B.B.B. (***NIF.3),*** *y que al principio dispensaba los pañales para los residentes de la* ******RESIDENCIA.2*** *y desde mediados de 2023 lo hacía a los residentes de la* ******RESIDENCIA.1,*** *por indicación de la Farmacia* ***B.B.B. (***NIF.3****).*
- *El titular de la oficina de Farmacia* ***A.A.A. (***NIF.2)****, confirmó que no tenía ningún contacto con las residencias ni los residentes y que la Farmacia* ***B.B.B. (***NIF.3****), le había facilitado unos códigos de acceso al programa informático de ***PROGRAMA.1 con el que obtenía los CIP de los residentes para poder acceder a su receta electrónica y dispensar los pañales, que le relacionaban en los Excel enviados por correo electrónico desde* ******EMAIL.1****. Posteriormente, él enviaba un correo electrónico con la relación de aportación monetaria de los residentes, que le pagaban desde la Farmacia* ***B.B.B. (***NIF.3****)."*

Asimismo, la Inspección de Farmacia remite el acta de la inspección realizada el 23 de noviembre de 2023, cuyo contenido se reproduce a continuación:

(…)

1.1 Anexos del Acta de inspección.

Esta acta incluye las siguientes evidencias:

- Anexo I: correo electrónico de fecha 16/11/2023 que contiene un intercambio de correos entre la dirección de correo ******EMAIL.1*** y ******EMAIL.2*** en el que se adjunta un documento Excel llamado ***"***EXCEL.1"*** que contiene el nombre y apellido de los residentes de la residencia ******RESIDENCIA.3*** que tienen pañales disponibles esa semana.

- Anexo II: correo electrónico de fecha 17/11/2023 enviado desde la cuenta de correo ******EMAIL.2*** a la dirección de correo ******EMAIL.1*** y con copia a ******EMAIL.4*** con el texto: "*Adjunto ventas y aportación del17 de noviembre*". El correo lleva adjunto un documento Excel llamado ***"***EXCEL.2"*** que contiene, entre otra información, el nombre y apellido de residentes de ******RESIDENCIA.3.***

1. Información aportada en las respuestas a los requerimientos de información de la AEPD.

Con fecha 6/11/2024 se realiza un requerimiento de información a la parte denunciada solicitándole, entre otros puntos, el listado de las residencias a las que presta o ha prestado servicio, descripción de los tratamientos realizados y su base de legitimación, la copia del RAT, del Análisis de Riesgos y de la Evaluación del Impacto (en adelante, EIPD), así como, información sobre el intercambio de los datos personales con terceras entidades.

La parte denunciada responde a este requerimiento de información, con fecha de registro de entrada 20/11/2024, proporcionando únicamente un documento que incluye en su interior la siguiente información:

- Registro Actividades.
- Análisis de riesgos.
- Relación sucinta de actuaciones que debe realizar los titulares de la oficina de farmacia para cumplir con RGPD.

2.1. Residencias a las que presta o ha prestado servicio.

La parte denunciada ofrece en su escrito de respuesta al requerimiento el listado de residencias a las que presta servicio junto con la fecha de comienzo y fin. Refiere dar servicio de dispensación de absorbentes de incontinencia urinaria a los residentes de dichos centros.

- ******RESIDENCIA.4*** desde 2019 hasta actualidad. 6 residentes

- ***RESIDENCIA.5** desde junio 2024 hasta actualidad. 19 residentes
- ***RESIDENCIA.2** desde 20/1/21 hasta 25/4/23. Un promedio de 20 residentes
- ***RESIDENCIA.6** desde 10/5/23 hasta 23/11/23. Un promedio de 20 residentes

La parte denunciada indica que los tratamientos realizados sobre los datos de carácter personal de los residentes son: recogida, consulta y comunicación.

Asimismo, manifiesta que el titular de la oficina de Farmacia actúa como responsable del tratamiento y que la base de legitimación es la Ley de garantías y uso racional de los medicamentos y productos sanitarios.

2.1. Contratos con las residencias.

Requerida la copia de los contratos suscritos con cada una de las residencias que incluya, en su caso, el correspondiente encargo de tratamiento, la parte denunciada refiere que:
"*No aplica porque el titular de la Oficina de Farmacia actúa como responsable de los datos.*"

2.2. Procedimientos seguidos para cumplir con el deber de información a los residentes.

Con relación a los procedimientos seguidos para cumplir con el deber de información a los residentes, la parte denunciada señala en su escrito de respuesta al requerimiento que:
"*No teníamos ningún contacto con los residentes. Toda la información la recibíamos a través de la farmacia intermediaria."*

2.3. Documentación requerida por RGPD.

La parte denunciada facilita la siguiente información integrada dentro de su escrito de respuesta al requerimiento:

- Registro Actividades.
- Análisis de riesgos.
- Relación sucinta de actuaciones que deben realizar los titulares de la oficina de farmacia para cumplir con el RGPD.

2.1. Registro de actividades (RAT).

La parte denunciada facilita como Registro de las Actividades, un único tratamiento. Se extrae, entre otras, la siguiente información:

- Receta Médica del Sistema Nacional de Salud (Electrónica y/o soporte papel) o con cargo a las mutuas de accidentes de trabajo
- Datos de categorías especiales en soporte mixto de Titularidad pública
- Nombre o razón social del Titular del fichero: Servei Català de Salut, MUFACE, ISFAS y MUGEJU, y las diferentes Mutuas de Accidentes de Trabajo
- Responsable: ***A.A.A***.

- Finalidad y usos previstos: Dispensación de medicamentos recetados por el SNS con receta electrónica.
- Datos categorías especiales: Salud
- Aplicaciones informáticas: Sistema de RE (Receta Electrónica)

Añade la información general de este tratamiento mostrada a continuación:

"Los responsables del tratamiento son CATSALUT, MUFACE, ISFAS Y MUGEJU, y las diferentes Mutuas de Accidentes de Trabajo.
Se trata de ficheros de titularidad pública, por lo que la obligación de informar sobre el contenido y finalidad del fichero se entiende cumplida con la publicación en los boletines oficiales del acuerdo de creación del fichero, antes de la aplicación del Reglamento europeo de PPDD.
Responsable de tratamiento: También lo puede ser el farmacéutico titular propietario de la oficina de farmacia y, en su caso, el farmacéutico regente.
Se deben adoptar las medidas de seguridad de carácter técnico y organizativo de nivel alto.
El farmacéutico titular de la oficina de farmacia no decide sobre la finalidad del fichero. Únicamente puede, conforme dispone la Ley de Garantías y Uso Racional de los Medicamentos y Productos Sanitarios 29/2006 de 26 de julio, y RD 1718/2010 de Receta Médica y el RD 1675/2012 de Receta Médica de Estupefacientes, retener y almacenar y tratar los datos correspondientes al medicamento o producto dispensado, el precio y la referencia de la oficina de farmacia, para proceder a su facturación. En el caso que el titular de la oficina de farmacia pretenda hacer un uso más allá de lo que prevé la normativa vigente, deberá recabar el consentimiento del afectado, siguiendo las pautas que se recogen para los ficheros de Clientes, Atención Farmacéutica, SPD, Ortopedia, según la finalidad para la que se obtengan los datos.
En algunos casos el titular de la farmacia necesita obtener la prestación de servicios por terceros para dispensar la medicación o el producto prescrito en la receta. Éste es el caso de las fórmulas magistrales y vacunas.
El farmacéutico titular, dispone de encargados del Tratamiento cuando encarga a otro titular de oficina de farmacia la realización de las fórmulas magistrales, encarga al laboratorio vacunas individualizadas.
El Colegio de Farmacéuticos es encargado de tratamiento cuando elabora la factura y gestiona el cobro de los medicamentos y otros productos dispensados con receta del Sistema Nacional de Salud o de las mutuas de accidentes de trabajo. Al margen de los proveedores informáticos de los sistemas empleados que siempre tienen la consideración de encargados de tratamiento.
El fichero que contiene los datos personales de la prestación farmacéutica del "Servei Català de la Salut" es un fichero de titularidad pública, cuyo registro a la APDCAT se produjo mediante la Orden de 288/1999 de 26 de octubre."

2.1. Informes técnicos del DPD.

Solicitados informes técnicos o recomendaciones elaborados por el Delegado de Protección de Datos, la parte denunciada incluye la información, *"Relación sucinta de actuaciones que deben realizar los titulares de la oficina de farmacia para cumplir con RGPD"* e indica el acceso al documento electrónico en ******URL.1,*** necesitándose usuario y contraseña para poder acceder a dicha página web.

La información de dicha página web, entre otros puntos, específica:

"De conformidad al contenido del Protocolo de Protección de datos personales el titular debe:

[…]

4. Obtener el consentimiento explícito de los clientes/usuarios para el tratamiento de sus datos personales. Tener firmada por parte de los clientes-pacientes la Cláusula B.1 del Anexo B.

5. Tener firmados con los Encargados del tratamiento descritos en el Anexo C, el modelo de contrato C.1 con la empresa de informática, la gestoría que realiza las nóminas, la empresa de seguridad si procede, etc. y el modelo C.2 con el farmacéutico titular de la oficina de farmacia que realiza las fórmulas magistrales por encargo.

[…]

21. El envío telemático de las fórmulas magistrales y de las vacunas debe hacerse de forma segura: o por fax disociando los datos, o por correo ordinario al formulador o al distribuidor en el caso de las vacunas o por correo-e encriptado."

3. **Terceras entidades**.

La parte denunciada manifiesta en su escrito de respuesta al requerimiento, información de terceras entidades, relacionadas con su farmacia, que realizan tratamientos de datos personales de los residentes:

"nuestro único contacto era a través de la farmacia.
*Farmacia **E.E.E.** desde el 25-01-21 hasta 28-10-22*
*Farmacia **B.B.B.** desde 14-11-22 hasta el 23-11-23*

*Los pañales eran proporcionados por nuestro distribuidor oficial *****EMPRESA.1** o *****EMPRESA.2** que es quien nos presentó a C.C.C. para dispensar los pañales de la ***RESIDENCIA.2.*

*La obtención de la receta electrónica se realizaba a través del programa informático *****PROGRAMA.1**."*

Solicitada la descripción de los tratamientos realizados por esas terceras entidades sobre los datos de carácter personal de los residentes, la parte denunciada indica:

"A través de un Excel la farmacia nos hacía llegar la información sobre qué pacientes teníamos que dispensar los pañales"

Consultada por la base legal que legitima dichos tratamientos en particular, la parte denunciada no contesta a esta pregunta específica.

Con relación a los contratos de encargados del tratamiento, la parte denunciada manifiesta:

*"En el caso de las residencias *****RESIDENCIA.5 y ***RESIDENCIA.4** disponemos de todas las autorizaciones según el modelo que exige el colegio de Farmacéuticos de Barcelona, debidamente cumplimentados por el paciente o en defecto por la persona responsable."*

4. **Intercambio de información de datos personales de los residentes.**

Consultada por el procedimiento de intercambio de información de datos personales entre la oficina de farmacia y las residencias, la parte denunciada contesta:

*"5.1 no había ningún contacto con las residencias *****RESIDENCIA.2 o ***RESIDENCIA.6**. En el caso de las otras residencias nosotros tenemos toda la información debidamente autorizada por el paciente para acceder a sus datos y poder enviar los pañales. Mediante un mail encriptado nos indican que pacientes necesitan pañales. Estos nos lo envían *****EMPRESA.1** a la farmacia y de aquí los enviamos la residencia."*

Consultada por el procedimiento de intercambio de información de datos personales entre la oficina de farmacia y otras terceras entidades, la parte denunciada contesta:

*"5.2 en el caso de las residencias *****RESIDENCIA.2 y ***RESIDENCIA.6**, el intercambio de información se obtenía a través de un Excel que la farmacia nos enviaba. A través del programa *****PROGRAMA.1** y un código de usuario que no enviaron, podíamos ver el código de la receta electrónica y así poder dispensar los pañales que no habían indicado que teníamos que dispensar."*

5. **Utilización de software, hojas Excel o similar para la recogida de datos de los residentes**.

Consultada por la utilización de software, hojas Excel o similar para la recogida de datos de los residentes, la parte denunciada manifiesta en su escrito de respuesta al requerimiento:

*"La información sobre los pañales que teníamos que vender a las residencias *****RESIDENCIA.2** y posteriormente a *****RESIDENCIA.6** nos llegaba a través de un Excel que nos indicaba a quien debíamos vender los pañales.*
*La información de la receta electrónica se obtenía a través del programa *****PROGRAMA.1,** a la cual accedíamos mediante un código de usuario que nos proporcionaron."*

6. **Programa de ***PROGRAMA.1**.

Solicitada confirmación del uso del programa de ***PROGRAMA.1 para acceder a los datos de los residentes e información sobre la tipología de datos que se obtienen desde dicho programa, la parte denunciada indica:

*"8.1 se usaba el programa de ***PROGRAMA.1 para la obtención de los datos de la receta electrónica.*
8.2 solo podíamos acceder al número de su receta electrónica por el nivel de usuario que teníamos."

Requerida confirmación de posesión de un usuario propio en el programa de ***PROGRAMA.1, la parte denunciada manifiesta:

> *"8.3 al principio de contactar con la farmacia **E.E.E.** se nos envió mediante un mail el nombre de usuario y la contraseña pertinente."*

CUARTO: La oficina de farmacia ******NIF.2***, es titularidad de ***A.A.A.*** con NIF ******NIF.1***.

FUNDAMENTOS DE DERECHO

I
Competencia

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 Presidencia de la Agencia Española de Protección de Datos.

II
Procedimiento

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".*

De acuerdo con el artículo 64 de la LOPDGDD, y teniendo en cuenta las características de las presuntas infracciones cometidas, se inicia un procedimiento sancionador.

El procedimiento tendrá una duración máxima de doce meses a contar desde la fecha del acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones, de conformidad con lo establecido en el artículo 64 de la LOPDGDD.

Si en el plazo estipulado no efectuara alegaciones a este acuerdo de inicio, el mismo podrá ser considerado propuesta de resolución, según lo establecido en el artículo 64.2.f) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP).

III
Cuestiones previas

1. Normativa sectorial aplicable

1.1. Oficinas de farmacia

Las oficinas de farmacia son, de acuerdo con el artículo 86.6 del Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios, establecimientos sanitarios privados, de interés público.

Su regulación se encuentra, entre otras normas de aplicación, en la Ley 14/1986, de 25 de abril, General de Sanidad; la Ley 16/1997, de 25 de abril, de Regulación de Servicios de las Oficinas de Farmacia; el Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios; así como en la legislación autonómica aplicable como, en el caso de Cataluña, la Ley 31/1991, de 13 de diciembre, de Ordenación Farmacéutica de Cataluña.

Tanto la Ley 14/1986, de 25 de abril como la Ley 16/1997, de 25 de abril, señalan:

> "*el farmacéutico titular-propietario de las mismas, asistido, en su caso, de ayudantes o auxiliares, deberá prestar los siguientes servicios básicos a la población:*
>
> > *1. La adquisición, custodia, conservación y dispensación de los medicamentos y productos sanitarios.*
> > *2. La vigilancia, control y custodia de las recetas médicas dispensadas (…)".*

Por su parte, el artículo 3 del Real Decreto Legislativo 1/2015, de 24 de julio, es más tajante al afirmar que la custodia, conservación y dispensación de medicamentos de uso humano corresponde exclusivamente a:

> *"a) A las oficinas de farmacia abiertas al público, legalmente autorizadas.*
>
> *b) A los servicios de farmacia de los hospitales, de los centros de salud y de las estructuras de atención primaria del Sistema Nacional de Salud para su aplicación dentro de dichas instituciones o para los medicamentos que exijan una particular vigilancia, supervisión y control del equipo multidisciplinar de atención a la salud, de conformidad con la calificación otorgada por la Agencia Española de Medicamentos y Productos Sanitarios para tales medicamentos (…)".*

Las oficinas de farmacia están obligadas, de acuerdo con el artículo 86.3 del Real Decreto Legislativo 1/2015, de 24 de julio, a la *"dispensación de medicamentos que se les demanden tanto por los particulares como por el Sistema Nacional de Salud en las condiciones reglamentarias establecidas".* No obstante, debe respetarse el principio de libre elección de farmacia. Así esta norma consagra como infracción grave en su artículo 111 b):

> *"26.ª Coartar la libertad del usuario en la elección de la oficina de farmacia mediante cualquier acto u omisión".*

También se tipifica como infracción grave en el mismo artículo:

> *"22.ª Defraudar, las oficinas de farmacia, al Sistema Nacional de Salud o al beneficiario del mismo con motivo de la facturación y cobro de recetas oficiales".*

Se subraya, asimismo, que, de acuerdo con el mencionado Real Decreto Legislativo, constituye una infracción muy grave según el artículo 111 c):

> *"23.ª Realizar, por parte de las oficinas de farmacia, actividades de distribución de medicamentos a otras oficinas de farmacia, entidades de distribución autorizadas, u otras entidades, centros o personas físicas sin autorización para la actividad de distribución o bien la realización de envíos de medicamentos fuera del territorio nacional"*

Por su parte, la Ley 16/1997, de 25 de abril, consagra la figura del farmacéutico como elemento esencial e imprescindible para el funcionamiento de una oficina de farmacia al determinar en su artículo 5:

> *"1. La presencia y actuación profesional de un farmacéutico es condición y requisito inexcusable para la dispensación al público de medicamentos. La colaboración de ayudantes o auxiliares no excusa la actuación de farmacéutico en la oficina de farmacia, mientras permanezca abierta al público, ni excluye su responsabilidad profesional.*
>
> *2. Las Comunidades Autónomas podrán regular el número mínimo de farmacéuticos adjuntos, que, además del titular, deban prestar servicios en las oficinas de farmacia al objeto de garantizar la adecuada asistencia profesional a los usuarios. Esta regulación deberá tener en cuenta, entre otros factores, el volumen y tipo de actividad de las oficinas de farmacia y el régimen de horario de los servicios.*
>
> *3. Sin perjuicio de la actuación del adjunto, el farmacéutico titular será responsable de garantizar el servicio a los usuarios".*

Asimismo, el artículo 103 de la Ley 14/1986, de 25 de abril, General de Sanidad señala:

> *"1. La custodia, conservación y dispensación de medicamentos corresponderá:*
>
> *a) A las oficinas de farmacia legalmente autorizadas.*
>
> *b) A los servicios de farmacia de los hospitales, de los Centros de Salud y de las estructuras de Atención Primaria del Sistema Nacional de Salud para su aplicación dentro de dichas instituciones o para los que exijan una particular vigilancia, supervisión y control del equipo multidisciplinario de atención a la salud.*
>
> *2. Las oficinas de farmacia abiertas al público se consideran establecimientos sanitarios a los efectos previstos en el título IV de esta Ley.*
>
> *3. Las oficinas de farmacia estarán sujetas a la planificación sanitaria en los términos que establezca la legislación especial de medicamentos y farmacias.*
>
> *4. Sólo los farmacéuticos podrán ser propietarios y titulares de las oficinas de farmacia abiertas al público".*

En consecuencia, el titular de la farmacia es quien responde de las actuaciones realizadas por la oficina de farmacia y a quien cabe exigir responsabilidades.

1.2 Dispensación de medicamentos

Además de la normativa anteriormente mencionada, resulta de interés en materia de dispensación farmacéutica el Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación cuyo capítulo IV está dedicado a "la receta médica electrónica oficial del SNS", contemplando los criterios generales de su desarrollo, así como la coordinación en el SNS. En su artículo 9, se señala:

"1. La dispensación será realizada por las oficinas de farmacia conectadas al sistema de receta médica electrónica, mediante el procedimiento normalizado establecido por las autoridades sanitarias competentes, que determinarán sus condiciones específicas, siendo necesario el certificado electrónico del titular de la oficina de farmacia, o, en su caso, del farmacéutico regente, adjunto o sustituto, expedido por la entidad competente.
2. Tras la identificación inequívoca del paciente, y en su caso de la persona en quien delegue, el farmacéutico sólo podrá acceder desde los equipos instalados en la oficina de farmacia, con los requisitos y condiciones que se establecen en el apartado siguiente, a los datos necesarios para una correcta dispensación informada y seguimiento del tratamiento y dispensará exclusivamente, de entre las prescripciones pendientes de dispensar, las que el paciente solicite.
3. Sólo se permitirá el acceso de los farmacéuticos al sistema electrónico mediante la tarjeta sanitaria del paciente debidamente reconocida por el sistema de receta electrónica, debiendo ser devuelta de forma inmediata a su titular y sin que pueda ser retenida en la oficina de farmacia. El acceso del farmacéutico siempre quedará registrado en el mencionado sistema.
4. En el momento de la dispensación, los sistemas de receta electrónica deberán incorporar y remitir a las Administraciones sanitarias correspondientes, los datos de identificación del producto dispensado, codificados conforme al Nomenclátor oficial de productos farmacéuticos del Sistema Nacional de Salud, número de envases dispensados y su identificación unitaria cuando sea posible, identificación de la oficina de farmacia dispensadora, utilizando para ello el NIF/CIF de su titular, así como el número de identificación de la oficina de farmacia otorgado por la Administración sanitaria competente, y la fecha de dispensación, en el formato que el nodo nacional de intercambio tenga establecido al efecto. Esta información será la única que quedará a efectos de facturación en la organización farmacéutica colegial, en tanto intervenga como responsable de la misma, y estará a disposición de las Administraciones sanitarias competentes de conformidad con su normativa de aplicación".

Asimismo, en su artículo 11 determina:

"*El sistema de receta médica electrónica garantizará la seguridad en el acceso y transmisión de la información, así como la protección de la confidencialidad de los datos, de conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Se implantarán las medidas de seguridad de nivel alto, previstas en la referida normativa de*

> *protección de datos de carácter personal. Para garantizar dichos niveles de seguridad, esta información sólo será accesible desde la oficina de farmacia a efectos de dispensación, residirá de forma permanente en los sistemas de receta electrónica gestionados por las Administraciones sanitarias y no podrá ser almacenada en los repositorios o servidores ajenos a éstas, establecidos para efectuar la facturación, una vez esta se haya producido."*

A nivel autonómico, en Cataluña destaca el Real Decreto 159/2007, de 24 de julio, *Recepta electrònica i la tramitació telemàtica de la prestació farmacèutica a càrrec del Servei Català de la Salut.*

Por último, señalar la Orden SLT/72/2008, de 12 de febrero, por la que se desarrolla el Decreto 159/2007, de 24 de julio, por el que se regula la receta electrónica y la tramitación telemática de la prestación farmacéutica a cargo del Servicio Catalán de la Salud. En su artículo 7 determina:

> *"Con el fin de acceder a la dispensación de recetas electrónicas, se tiene que identificar la persona paciente como titular del derecho a la prestación farmacéutica a la oficina de farmacia mediante la presentación de la tarjeta sanitaria individual, y se tiene que entregar al farmacéutico o farmacéutica la hoja de medicación activa donde se recoja el tratamiento para el que se solicita la dispensación del producto incluido en la prestación farmacéutica."*

2. Sobre la presunción de veracidad de las actas de la Inspección de farmacia

El artículo 108 del Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios, señala que compete a las administraciones sanitarias en el ámbito de sus competencias la realización de las inspecciones necesarias para asegurar el cumplimiento de lo previsto en esta ley.

Este artículo supone prácticamente una reproducción de lo previsto por el artículo 30 de la Ley 14/1986, de 25 de abril, General de Sanidad que determina que *"todos los centros y establecimientos sanitarios, así como las actividades de promoción y publicidad, estarán sometidos a la inspección y control por las Administraciones Sanitarias competentes".*

Ambas normas prevén, en sus artículos 108.3 y 31 respectivamente, a tales efectos, una serie de potestades para el personal al servicio de las Administraciones Públicas en el ejercicio de la potestad inspectora entre las que se incluyen la posibilidad de entrar libremente y sin notificación en los centros sujetos a las mismas, como son las oficinas de farmacia; así como proceder a las pruebas, investigaciones o exámenes necesarios para comprobar el cumplimiento normativo; tomar muestras, en orden a la comprobación del cumplimiento de las mismas, así como realizar cuantas actuaciones sean precisas en orden al cumplimiento de las funciones de inspección que desarrollen.

En el ámbito autonómico, la Ley 26/2010, de 3 de agosto, de régimen jurídico y de procedimiento de las administraciones públicas de Catalunya consagra en su artículo 89.2 la consideración de autoridad del personal de su Administración encargado de las funciones públicas de inspección y control.

A este respecto conviene señalar que el artículo 77.5 de la LPACAP establece la presunción de veracidad de los documentos firmados por empleados públicos que tengan la consideración de autoridad, salvo prueba en contrario. En concreto, señala: *"los documentos formalizados por los funcionarios a los que se reconoce la condición de autoridad y en los que, observándose los requisitos legales correspondientes recojan los hechos constatados por aquéllos, harán prueba de éstos salvo que se acredite lo contrario".*

En el mismo sentido, la anteriormente citada Ley 26/2010, de 3 de agosto, de Catalunya en su artículo 90. 1 determina que los hechos constatados por el personal de la Administración encargado de las funciones públicas de inspección y control, y que se formalizan en un documento público observando los requisitos legalmente establecidos, tienen valor probatorio, sin perjuicio de las pruebas que puedan aportar las personas interesadas en defensa de sus derechos e intereses.

En consecuencia, las actas han de estar firmadas ineludiblemente por el inspector, sin perjuicio de que la falta de firma por parte del inspeccionado no invalide el acta ni su valor probatorio.

3. Responsabilidad del tratamiento en el ámbito de protección de datos personales

El artículo 4.1) del RGPD, define «dato personal» como: "toda 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".

El artículo 4.2) del RGPD, define «tratamiento» como: "cualquier 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."

El artículo 4.7) del RGPD, define al «responsable del tratamiento» o «responsable» como: "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". A su vez el artículo 4.8) del RGPD determina al «encargado del tratamiento» o «encargado» como la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

Por su parte, las *Directrices 07/2020 del Comité Europeo de Protección de Datos sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento»* (en adelante, Directrices 07/2020) destacan que los conceptos de responsable del tratamiento y encargado del tratamiento son conceptos funcionales, siendo necesario

establecerlos en virtud de sus actividades concretas en el caso analizado y no en función de la designación formal que pueda figurar en el contrato:

> *"12. Los conceptos de «responsable del tratamiento» y «encargado del tratamiento» son conceptos funcionales: su objetivo es asignar responsabilidades en función del papel real de cada parte. Esto implica que la condición jurídica de «responsable del tratamiento» o «encargado del tratamiento» de los participantes debe establecerse en principio en virtud de sus actividades concretas en una situación determinada y no en función de la designación formal de un participante como «responsable del tratamiento» o «encargado del tratamiento» (p. ej., en un contrato).Esto implica que la asignación de la función de responsable o encargado debe derivar normalmente de un análisis de los hechos o circunstancias del caso y, en consecuencia, no es negociable."* (subrayado de la AEPD).

En definitiva, la identificación del responsable debe realizarse atendiendo a criterios materiales de acuerdo con las condiciones y circunstancias reales de cada tratamiento, no puede entenderse como una mera constatación formal de lo que figure, por ejemplo, en un contrato suscrito entre partes. Así, habrá ocasiones en las que los partícipes en una cadena de tratamientos se hayan identificado respectivamente como responsable y encargado y, sin embargo, atendiendo a quién determina la finalidad del tratamiento y los medios esenciales del mismo la figura de responsable le corresponde a quien fue identificado formalmente como tal.

A lo ya expuesto hasta el momento, cabe añadir que dichas Directrices del CEPD destacan:

> *"20. (…) El responsable del tratamiento es quien decide determinados aspectos esenciales del tratamiento de los datos. La responsabilidad del tratamiento puede establecerse en la normativa o deducirse de un análisis de los hechos o las circunstancias del caso. Es necesario dirigir la atención a las actividades de tratamiento concretas de que se trate y comprender quién las determina. Para ello, primero deben examinarse las siguientes cuestiones: «¿por qué tiene lugar el tratamiento?» y «¿quién ha decidido que debe llevarse a cabo el tratamiento para un fin concreto?»."* (subrayado de la AEPD).

Asimismo, las referidas Directrices del CEPD 07/2020 abogan por una interpretación amplia del concepto de responsable del tratamiento con el fin de promover una protección eficaz y completa de los interesados. En este sentido, prevén:

> *"14. Puesto que el objetivo último de la atribución de la función de responsable del tratamiento es garantizar la responsabilidad proactiva y una protección eficaz e integral de los datos personales, el concepto de «responsable» debería interpretarse de un modo suficientemente amplio, de manera que promueva, en la medida de lo posible, una protección eficaz y completa de los interesados , con el fin de garantizar la plena eficacia del Derecho de la Unión en materia de protección de datos, evitar lagunas y prevenir las posibles elusiones de la normativa, sin que todo ello suponga una merma de las atribuciones del encargado del tratamiento."* (subrayado de la AEPD).

Por otra parte, tal y como enuncia el artículo 4.7 del RGPD, es posible que en ocasiones sea una norma la que defina al responsable, ya sea de manera implícita o explícita. Así, puede ocurrir que una norma establezca obligaciones que suponen

tratamientos de datos personales y se lo encomiende a un determinado ente, que tendrá la condición de responsable del tratamiento desde la perspectiva de protección de datos.

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 la dispensación de pañales llevada a cabo por ***A.A.A.*** conlleva un conjunto de operaciones realizadas sobre datos personales como es el acceso a los datos personales que constan en el Sistema Nacional de Salud (SNS), su consulta y cotejo, así como su estructuración y organización.

Conforme a la documentación aportada por ***A.A.A.*** en contestación al requerimiento de actuaciones previas de investigación de esta Agencia, en el Registro de Actividades de tratamiento aportado, esta farmacia aparece como “responsable del tratamiento”. Así lo corrobora el propio investigado en sus contestaciones a dicha investigación.

Atendiendo a lo anterior, ***A.A.A.*** 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.

4. Los datos de salud como dato de categoría especial.

El artículo 9 del RGPD, que regula el tratamiento de categorías especiales de datos personales, establece lo siguiente:

"1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión o de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin

ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional;

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.

4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud."

Hay que señalar que los datos de categoría especial son aquellos datos personales cuyo tratamiento requiere de una protección reforzada, debido a su incidencia especial en la intimidad, las libertades públicas y los derechos fundamentales de la persona. Así considerados, su tratamiento, en principio, está prohibido tanto por el RGPD, salvo que exista alguna de las circunstancias indicadas en el artículo 9.2 del RGPD.

Por tanto, los datos de categoría especial son datos personales que, por su importancia para la privacidad del individuo, han de ser tratados con mayor cuidado y siguiendo unos requisitos especiales.

El Considerando 71 señala : "*sobre las decisiones automatizadas y la elaboración de perfiles, los responsables del tratamiento deben utilizar métodos que corrijan «los factores que introducen inexactitudes en los datos personales y reduzcan al máximo el riesgo de error, asegurar los datos personales de forma que se tengan en cuenta los posibles riesgos para los intereses y derechos del interesado e impedir, entre otras cosas, efectos discriminatorios en las personas físicas por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical, condición genética o estado de salud u orientación sexual, o tratamiento que dé lugar a medidas que produzcan tal efecto".* (el subrayado es de la AEPD).

El artículo 4.15 del RGPD define *"datos relativos a la salud"* como "*datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud".*

El Considerando 35 del RGPD aclara dicha definición señalando que "*Entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo; todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro*."

Conviene señalar que, el Tribunal de Justicia de la Unión Europea (TJUE) ha consignado un concepto amplio de los datos de salud. Así, de conformidad con la STJUE de 4 de octubre de 2024, en el asunto C 21/23 (el subrayado es de la AEPD):

> *"76 Entre estas categorías especiales de datos personales, que se enumeran en el artículo 8, apartado 1, de la Directiva 95/46 y en el artículo 9, apartado 1,*

> *del RGPD, figuran los datos relativos a la salud. Estos incluyen, de conformidad con el artículo 4, punto 15, del Reglamento, en relación con su considerando 35, todos los datos personales que revelen información sobre el estado de salud física o mental pasado, presente o futuro de una persona física, incluidos los datos relativos a la prestación de servicios de atención sanitaria a esa persona.*
>
> *81 A este respecto, el Tribunal de Justicia ya ha declarado que, a la vista del objetivo de la Directiva 95/46 y del RGPD, de asegurar un alto nivel de protección de las libertades y de los derechos fundamentales de las personas físicas, en particular, de su intimidad, en relación con el tratamiento de los datos personales que las afectan, el concepto de «datos relativos a la salud» previsto en el artículo 9, apartado 1, de dicho Reglamento y en el artículo 8, apartado 1, de la citada Directiva debe interpretarse de forma amplia (véanse, en este sentido, las sentencias de 6 de noviembre de 2003, Lindqvist, C 101/01, EU:C:2003:596, apartado 50, y de 1 de agosto de 2022, Vyriausioji tarnybinės etikos komisija, C 184/20, EU:C:2022:601, apartado 125)".*

Asimismo, la misma STJUE determina que cuando el tratamiento de datos personales pueda revelar indirectamente informaciones sensibles de una persona, dichos datos se encuadran en el régimen previsto en el artículo 9 del RGPD:

> *"82 En particular, no cabe interpretar tales disposiciones en el sentido de que el tratamiento de datos personales que puedan desvelar indirectamente informaciones sensibles sobre una persona física queda fuera del régimen de protección reforzado establecido por las mencionadas disposiciones, pues de quedar fuera se menoscabaría el efecto útil de ese régimen y la protección de las libertades y de los derechos fundamentales de las personas físicas que pretende garantizar (sentencia de 1 de agosto de 2022, Vyriausioji tarnybinės etikos komisija, C 184/20, EU:C:2022:601, apartado 127)".*

En la misma línea, la mencionada sentencia determina que las categorías especiales de datos personales están sometidos a la prohibición del art. 9 del RGPD independientemente de que sea información exacta o no y de que el tratamiento tenga por finalidad obtener datos personales que pertenezcan a dicha categoría:

> *"87 Esta prohibición de principio es independiente de que la información revelada por el tratamiento en cuestión sea o no exacta y de que dicho farmacéutico actúe con el fin de obtener información comprendida en alguna de las categorías especiales contempladas en el artículo 8, apartado 1, de la Directiva 95/46 y el artículo 9, apartado 1, del RGPD. En efecto, teniendo en cuenta los riesgos significativos para las libertades fundamentales y los derechos fundamentales de los interesados, generados por cualquier tratamiento de datos personales comprendidos en tales categorías, estas disposiciones tienen por objeto prohibir dichos tratamientos, con independencia de la finalidad que expresen y de la exactitud de la información en cuestión [véase, en este sentido, la sentencia de 4 de julio de 2023, Meta Platforms y otros. (Condiciones generales del servicio de una red social), C 252/21, EU:C:2023:537, apartados 69 y 70]".*

Por su parte, la STS de 8 de octubre, en el recurso de casación 1920/21, reafirma el concepto amplio de datos de salud, al indicar que:

> *"(…) cabe subrayar, al respecto, que la lectura del artículo 4.15 y del considerando 35 del Reglamento general de protección de datos avalan, tal como sostiene la sentencia de la Audiencia Nacional impugnada, la inclusión de la noción de "datos relativos a Ia salud" de los datos referidos al estado de salud de los deportistas, pues, aunque la normativa de la Unión Europea no contiene ninguna previsión especifica acerca de los datos relacionados con la aplicación de las técnicas de control del dopaje, define en un sentido amplio el tratamiento de los datos de salud. El considerando 35 del citado Reglamento (ÜE) 2016/679 incluye específicamente, entre los datos relativos a la salud, todos los datos relativos al estado de salud de! interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro, incluyendo la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad".*

No cabe duda, por tanto, de que los datos referentes a la dispensación de medicamentos o pañales por parte de una farmacia, el CIPA (Código de Identificación Personal Autonómico), el número de tarjeta sanitaria son datos de salud, así como también lo son todos aquellos que revelen de manera indirecta el estado de salud de una persona.

En cualquier caso, las circunstancias que permiten el levantamiento de la prohibición del tratamiento de datos de salud establecida por el artículo 9.1 vienen determinadas en el artículo 9.2 del RGPD. Es decir, es necesario que concurra alguna de las premisas establecidas en el mencionado artículo para que se pueda llevar a cabo el tratamiento de datos de salud. Estas excepciones han de interpretarse de manera restrictiva, tal y como se desprende de los considerandos del 51 al 56 del RGPD.

La dispensación de medicamentos y pañales supone el tratamiento de datos de salud y el levantamiento de la prohibición de tratamiento de estos datos se encontrará en el artículo 9.2 h); en la medida en que el tratamiento es necesario para la prestación de asistencia o tratamiento de tipo sanitario.

Además, el artículo 9.3 exige, para la premisa concreta del artículo 9.2 h) que el tratamiento se realice por un profesional sujeto a la obligación de derecho profesional o bajo su responsabilidad.

El levantamiento de la prohibición contenida en la letra h) del artículo 9.2, así como las previsiones añadidas del artículo 9.3 para la utilización de esta premisa exige una norma del Derecho a la UE o del Estado miembro que lo regule, que, en el caso de España, requiere que la asistencia o tratamiento de tipo sanitario se encuentre recogido en una norma con rango de ley, en la medida en que el derecho a la protección de datos personales es un derecho fundamental.

En este sentido, las diferentes operaciones de tratamiento de datos personales que conlleva la dispensación de medicamentos y pañales por las oficinas de farmacia

encontraría su habilitación en la Ley 14/1986, de 25 de abril, General de Sanidad; la Ley 16/1997, de 25 de abril, de Regulación de Servicios de las Oficinas de Farmacia; el Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios; así como en la legislación autonómica aplicable como, en el caso de Cataluña, la Ley 31/1991, de 13 de diciembre, de Ordenación Farmacéutica de Cataluña.

Así, por ejemplo, las oficinas de farmacia están obligadas, de acuerdo con el artículo 86.3 del Real Decreto Legislativo 1/2015, de 24 de julio, a la *"dispensación de medicamentos que se les demanden tanto por los particulares como por el Sistema Nacional de Salud".*

IV
Obligación incumplida. Artículo 6 del RGPD. Licitud del tratamiento

El primer apartado del artículo 6 del RGPD establece lo siguiente:

"1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:
a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones. "

2. Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX.

3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por:

a) el Derecho de la Unión, o
b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento.

La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

4. Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:
a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;
b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;
c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;
d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;
e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización."

En este sentido, el considerando 32 del RGPD establece que: "El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por

medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta."

A su vez, el artículo 4 del RGPD, relativo a definiciones, establece en el apartado 11:

"11) «consentimiento del interesado»: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;"

Por otra parte, el artículo 24 del RGPD desarrolla el principio de responsabilidad proactiva del responsable del tratamiento, exigiendo que su actuación no solo sea conforme al RGPD sino que, además, sea capaz de demostrarlo:

> *"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".*

En definitiva, el tratamiento de datos personales requiere la existencia de una base legal que lo legitime. La elección de la base más adecuada del tratamiento, en caso de existir varias, corresponde al responsable, igual que compete a este acreditar que el tratamiento se realiza conforme a una base de legitimación.

De conformidad con el artículo 6.1 del RGPD, además del consentimiento, existen otras posibles bases que legitiman el tratamiento de datos sin necesidad de contar con la autorización de su titular, en particular, cuando sea necesario para la ejecución de un contrato en el que el afectado es parte o para la aplicación, a petición de este, de medidas precontractuales, o cuando sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del afectado que requieran la protección de tales datos. El tratamiento también se considera lícito cuando sea necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento, para proteger intereses vitales del afectado o de otra persona física o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

En el presente caso, ***A.A.A.*** dispensa pañales a los residentes de centros geriátricos, para lo que trata los datos personales de estos.

Así consta en el acta ******ACTA.1*** de la Inspección de Farmacia que señala: ***"(…)"***, y así lo ha confirmado la propia parte denunciada a esta Agencia, facilitando los periodos en los que realizó estas actuaciones y el número de residentes afectados, si bien de su respuesta se desprende que, cuando contestó al requerimiento de información, seguía prestando el servicio de dispensación de pañales a dos residencias geriátricas ***(***RESIDENCIA.4 y ***RESIDENCIA.5***).

De acuerdo con la información por ella aportada a de 4 de noviembre de 2024 la relación de residencias a las que presta o ha prestado servicios es: "******RESIDENCIA.4*** *desde 2019 hasta actualidad (6 residentes),* ******RESIDENCIA.5*** *desde junio 2024 hasta actualidad (19 residentes)*, ******RESIDENCIA.2*** *desde 20/1/21 hasta 25/4/23 (un promedio de 20 residentes)*, ******RESIDENCIA.6*** *desde 10/5/23 hasta 23/11/23 (un promedio de 20 residentes)".*

La manera de acceder a los datos de los residentes se orquestaba a través de las claves de acceso al programa ******PROGRAMA.1*** que les remitía otra farmacia, sin perjuicio de que esta misma farmacia les remitiera correos electrónicos sin cifrar que contenían los datos de los residentes (incluyendo datos de salud). Así se recoge en la mencionada acta: ***"(…)".***

Por tanto, desde 2019 hasta la actualidad (o, al menos hasta el 4 de noviembre de 2024), ***A.A.A.*** ha dispensado pañales a diferentes residencias para un número variable de afectados, que ascienden, en la totalidad del periodo a 65 personas. A día de hoy, continúa dispensando pañales para aproximadamente 25 pacientes.

A este respecto, la parte denunciada asegura que actuaba como responsable del tratamiento, amparado en el artículo 6.1 c), y que el tratamiento era necesario para el cumplimiento de una obligación legal.

No obstante, ni la mencionada base de legitimación ni la correspondiente al ejercicio de una misión de interés público, reconocidas en una norma con rango de ley, se consideran suficientes. Tal y como se ha señalado previamente, las previsiones normativas recogidas en la legislación sectorial específica levantarían la prohibición del tratamiento de datos de salud por parte de las oficinas de farmacia, conforme al artículo 9.2 h), pero no puede considerarse que las mencionadas previsiones normativas amparen el tratamiento de una farmacia concreta en detrimento de otra y que, por tanto, puedan constituir por sí mismas una base de legitimación.

Asimismo, repasando las diferentes bases de legitimación posibles, no consta la existencia de un contrato suscrito entre ***A.A.A.*** y los residentes afectados, en tanto que titulares del derecho fundamental.

Conviene recordar que la normativa sectorial específica consagra el principio de libertad de elección de farmacia de usuario o paciente, tal y como se ha determinado en las Cuestiones Previas de este documento, lo que significa que el paciente o usuario es libre de elegir la farmacia que desea que proceda a la dispensación de su medicación.

Dicho esto, en el presente supuesto no consta el consentimiento de los pacientes para el tratamiento de sus datos por ***A.A.A.*** para la dispensación de pañales. Se subraya, no obstante, que en el RAT facilitado por la parte denunciada en contestación al requerimiento efectuado por esta Agencia, se señalaba: *"en el caso que el titular de la oficina de farmacia pretenda hacer un uso más allá de lo que prevé la normativa vigente, deberá recabar el consentimiento del afectado".*

En cuanto al interés vital, el considerando 46 del RGPD establece la excepcionalidad de esta base legal y su singularidad, cuando manifiesta que solo deben tratarse datos personales sobre esta base cuando el tratamiento no pueda basarse manifiestamente

en una base jurídica diferente. Asimismo, menciona que ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado como, por ejemplo, cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano.

Y es que la consideración de interés vital necesariamente viene referida a la existencia de un riesgo cierto, plausible, no simplemente potencial basado en datos generales, no concretos en atención a la necesidad de este tratamiento concreto que pase por encima de otras bases jurídicas del tratamiento, como podría ser el consentimiento.

Por último, el interés legítimo de ***A.A.A.*** exigiría la existencia en primer término de este, y posteriormente, una ponderación del mismo con los derechos y libertades de los afectados, algo que no se aprecia en el presente caso.

En definitiva, no se aprecia la existencia de base legal que ampare el tratamiento de dispensación de medicamentos y pañales realizados por ***A.A.A.*** respecto a los datos personales de los residentes de los centros geriátricos anteriormente mencionados.

Por tanto, de conformidad con las evidencias de las que se dispone en este momento de acuerdo de inicio de procedimiento sancionador, se considera que los hechos conocidos podrían ser constitutivos de una infracción, imputable a ***A.A.A.*** por vulneración del artículo 6 del RGPD.

V

Tipificación de la infracción del artículo 6.1 del RGPD y calificación a efectos de prescripción

El artículo 83.5 del RGPD tipifica como infracción administrativa la vulneración del artículo siguiente, que se sancionará, 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;"

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".

A los solos efectos del plazo de prescripción, el artículo 72.1 de la LOPDGDD establece lo siguiente:

"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:
b) El tratamiento de datos personales sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el artículo 6 del Reglamento (UE) 2016/679."

VI

Propuesta de sanción por incumplimiento del artículo 6 del RGPD.

A fin de determinar la multa administrativa a imponer se han de observar las previsiones de los artículos 83.1 y 83.2 del RGPD, preceptos que señalan:

"1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 9 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:
a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;
b) la intencionalidad o negligencia en la infracción;
c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;
d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;
e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;
f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;
g) las categorías de los datos de carácter personal afectados por la infracción;
h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;
i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;
j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y
k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción".

Por su parte, el artículo 76 *"Sanciones y medidas correctivas"* de la LOPDGDD dispone:

"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.

2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:
a) El carácter continuado de la infracción.
b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.
c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.
f) La afectación a los derechos de los menores.
g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.
h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado".

En el presente caso, considerando la gravedad de la posible infracción, atendiendo especialmente a las consecuencias que su comisión provoca en los afectados, correspondería la imposición de multa, además de la adopción de medidas, si procede.

La multa que se imponga deberá ser, en cada caso individual, efectiva, proporcionada y disuasoria, conforme a lo establecido en el artículo 83.1 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 acuerdo de inicio de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que procede graduar la sanción a imponer de acuerdo con las circunstancias siguientes, contempladas en los preceptos antes citados.

- La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate, así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido (artículo 83.2 letra a), del RGPD): los hechos imputados inciden negativamente en el control de los afectados sobre sus datos personales, siendo el control sobre los datos personales elemento fundamental y eje vertebrador del RGPD. En definitiva, las actuaciones llevadas a cabo por ***A.A.A.*** implican la pérdida de control y disposición de los datos que conciernen al titular del derecho fundamental.

  A este respecto, no puede obviarse el número de afectados y de residencias implicadas, lo que hace que la infracción adquiera connotaciones "sistémicas", aun cuando el número de afectados haya variado a lo largo del tiempo. En total, desde 2019 hasta la actualidad habría 65 residentes afectados.

Por último, se señala que la falta de acreditación de la existencia de una base de legitimación para efectuar el tratamiento supone una violación del principio de responsabilidad proactiva prevista en el artículo 5.2 del RGPD, principio esencial de la normativa de protección de datos.

- La intencionalidad o negligencia en la infracción (artículo 83.2 letra b)): se aprecia negligencia grave en la medida en que el tratamiento de datos de salud se realiza en incumplimiento de la normativa sectorial específica, basada en la libre elección de farmacia de los pacientes, así como al Código de Deontología de la profesión farmacéutica aprobado por el Consejo General de Colegios Farmacéuticos, que establece que *"toda actuación en el ámbito de la salud que tenga como destinatario un paciente o usuario requiere del consentimiento informado, libre y voluntario de éste. El farmacéutico deberá respetar su decisión, en los términos establecidos en la legislación".*

- Las categorías de los datos de carácter personal afectados por las infracciones (artículo 83.2, letra g), del RGPD): las Directrices 04/2022 del Comité Europeo de Protección de Datos, sobre el cálculo de las multas bajo el RGPD, adoptadas el 24 de mayo de 2023, en su apartado 57, señalan lo siguiente en cuanto al requisito de tener en cuenta las categorías de los datos personales afectados: "(…)*el RGPD destaca claramente los tipos de datos que merecen una protección especial y, por tanto, una respuesta más estricta en lo que respecta a las multas. Esto se refiere, como mínimo, a los tipos de datos a que se refieren los artículos 9 y 10 del RGPD y a los datos fuera del ámbito de aplicación de estos artículos cuya difusión provoque daños y perjuicios inmediatos al interesado (por ejemplo, datos de localización, datos sobre comunicación privada, números de identificación nacionales o datos financieros, como resúmenes de transacciones o números de tarjetas de crédito"*). En el presente caso, los datos personales objeto de tratamiento incluyen datos de salud, como, por ejemplo, la pauta médica de los afectados o el número de la tarjeta sanitaria o CIPA.

Asimismo, se consideran los siguientes factores de graduación en calidad de agravantes:

- La vinculación de la actividad del infractor con la realización de tratamientos de datos personales (artículo 83.2 k) del RGPD en conexión con el artículo 76.2, letra b), de la LOPDGDD): la farmacia ***A.A.A.*** como consecuencia de su actividad en tanto que establecimiento sanitario privado, de interés público, realiza de forma habitual y continua tratamientos de datos de carácter personal de un elevado número de interesados (todos sus pacientes o usuarios) imprescindible para el desarrollo de su negocio. La realización de actividades de dispensación de productos médicos y farmacéuticos, que es su actividad principal, implica necesariamente operaciones de tratamiento de datos personales. Así, las acciones infractoras se producen en el marco de un tratamiento de datos personales que habitualmente realiza ***A.A.A.*** en su negocio y ligado a este.

- Los beneficios obtenidos como consecuencia de la comisión de la infracción (artículo 83.2 k) del RGPD en conexión con el artículo 76.2, letra c) de la LOPDGDD): la dispensación de productos farmacéuticos para pacientes de

diferentes residencias sin base de legitimación supone que la farmacia ***A.A.A.*** ha prestado un servicio (provisión de pañales) a cambio de una contraprestación económica. En definitiva, la farmacia se ha lucrado por la realización de las actuaciones objeto de infracción.

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 6.1 del RGPD, permite fijar inicialmente, y sin perjuicio de lo que resulte de la instrucción de este procedimiento sancionador, una sanción de multa administrativa de 5.000€ euros.

VII

Obligación incumplida. Artículo 14 del RGPD. Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado

Según lo establecido en el artículo 14 del RGPD:

"1. Cuando los datos personales no se hayan obtenido del interesado, el responsable del tratamiento le facilitará la siguiente información:
a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
b) los datos de contacto del delegado de protección de datos, en su caso;
c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;
d) las categorías de datos personales de que se trate;
e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
f) en su caso, la intención del responsable de transferir datos personales a un destinatario en un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de ellas o al lugar en que se hayan puesto a disposición.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente respecto del interesado:
a) el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo;
b) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable del tratamiento o de un tercero;
c) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
d) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada;

e) el derecho a presentar una reclamación ante una autoridad de control;
f) la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;
g) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. El responsable del tratamiento facilitará la información indicada en los apartados 1 y 2:
a) dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos;
b) si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado, o
c) si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

4. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de los datos personales para un fin que no sea aquel para el que se obtuvieron, proporcionará al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y cualquier otra información pertinente indicada en el apartado 2.

5. Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que:
a) el interesado ya disponga de la información;
b) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información;
c) la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, o
d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza legal."

Cuando se obtengan datos personales relativos a una persona, y no se hubieran obtenido directamente de esta, el responsable del tratamiento debe facilitarle toda la información sobre el tratamiento de sus datos tal como se indica en el artículo 14 del RGPD. El RGPD exige que esa información se proporcione a la mayor brevedad y, en cualquier caso, no más tarde de un mes, o en el caso de que tuviera que hacérsele una comunicación, no más tarde en el momento de esa primera comunicación o en el momento en que se vayan a comunicar a otro destinatario, como tarde. En este sentido se pronuncia el considerando 61:

> *61) "Se debe facilitar a los interesados la información sobre el tratamiento de sus datos personales en el momento en que se obtengan de ellos o, si se obtienen de otra fuente, en un plazo razonable, dependiendo de las circunstancias del caso. Si los datos personales pueden ser comunicados legítimamente a otro destinatario, se debe informar al interesado en el momento en que se comunican al destinatario por primera vez. El responsable del tratamiento que proyecte tratar los datos para un fin que no sea aquel para el que se recogieron debe proporcionar al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y otra información necesaria. Cuando el origen de los datos personales no pueda facilitarse al interesado por haberse utilizado varias fuentes, debe facilitarse información general".*

Conviene resaltar que la obligación de informar en el artículo 14 del RGPD ha de entenderse en el marco de los derechos de los interesados en relación con la transparencia, principio que debe regir el tratamiento de los datos conforme al artículo 5.1 a) del RGPD. En este sentido, el artículo 12.1 del RGPD determina que:

> "*(…) El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14 (…) en forma concisa, transparente, inteligible y de fácil acceso con un lenguaje claro y sencillo (…)".*

A este respecto, resulta esencial hacer referencia al considerando 39 del RGPD que establece que:

> *"(39) Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales, así como del modo de hacer valer sus derechos en relación con el tratamiento. En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica.*

Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento".

Además de lo establecido en el considerando 60, que determina:

60) "(…) Los principios de tratamiento leal y transparente exigen que se informe al interesado de la existencia de la operación de tratamiento y sus fines. El responsable del tratamiento debe facilitar al interesado cuanta información complementaria sea necesaria para garantizar un tratamiento leal y transparente, habida cuenta de las circunstancias y del contexto específicos en que se traten los datos personales (…)".

En el presente caso, los datos personales de los residentes le eran proporcionados a ***A.A.A.*** por la Farmacia ***B.B.B.***. De acuerdo por lo afirmado en la contestación a la Inspección de Farmacia y a esta Agencia.

No consta documentación que acredite que ***A.A.A.*** haya facilitado a los afectados, cuyos datos personales trataba, a efectos de dispensación de pañales, información alguna sobre ninguno de los elementos contenidos en el artículo 14 del RGPD. Tampoco consta que dicha información se haya facilitado a aquellos cuyos datos continúa tratando.

De hecho, en la contestación sobre este aspecto concreto a esta Agencia durante las actuaciones previas de investigación, el responsable se limitó a afirmar que "*no teníamos ningún contacto con los residentes. Toda la información la recibíamos a través de la farmacia intermediaria."*

En todo momento la ***A.A.A.*** reconoce su condición de responsable del tratamiento, lo que, conforme al artículo 14 del RGPD, hace que se encuentre obligado a transmitir a los titulares de los datos toda la información que consta en el citado artículo en los plazos en este especificados. Nada de esto ha sido acreditado por el responsable.

Por tanto, de conformidad con las evidencias de las que se dispone en este momento de acuerdo de inicio de procedimiento sancionador, se considera que los hechos conocidos podrían ser constitutivos de una infracción, imputable a la farmacia ***A.A.A.*** por vulneración del artículo 14 del RGPD transcrito anteriormente.

VIII
Tipificación de la infracción del artículo 14 del RGPD y calificación a efectos de prescripción

El artículo 83.5 del RGPD tipifica como infracción administrativa la vulneración del artículo siguiente, que se sancionará, 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:

"b) los derechos de los interesados a tenor de los artículos 12 a 22;"

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".

A los solos efectos del plazo de prescripción, el artículo 72.1 de la LOPDGDD establece lo siguiente:

"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:
h) La omisión del deber de informar al afectado acerca del tratamiento de sus datos personales conforme a lo dispuesto en los artículos 13 y 14 del Reglamento (UE) 2016/679 y 12 de esta ley orgánica."

IX
Propuesta de sanción por incumplimiento del artículo 14 del RGPD.

A fin de determinar la multa administrativa a imponer se han de observar las previsiones de los artículos 83.1 y 83.2 del RGPD, y 76 LOPDGDD, preceptos reproducidos anteriormente.

En el presente caso, considerando la gravedad de la posible infracción, atendiendo especialmente a las consecuencias que su comisión provoca en los afectados, correspondería la imposición de multa, además de la adopción de medidas, si procede.

La multa que se imponga deberá ser, en cada caso individual, efectiva, proporcionada y disuasoria, conforme a lo establecido en el artículo 83.1 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 acuerdo de inicio de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que procede graduar la sanción a imponer de acuerdo con las circunstancias siguientes, contempladas en los preceptos antes citados:

- La naturaleza, gravedad y duración de la infracción (artículo 83.2 letra a), del RGPD): se destaca que en este supuesto no se ha facilitado ningún tipo de información a los residentes (ni tan siquiera la más básica cómo quién y para qué se utilizan los datos), cuando la información que se facilita al interesado por parte de un responsable es esencial para que este tenga conocimiento de

la existencia de un tratamiento y sus fines, entre otros aspectos, permitiendo un auténtico control sobre sus datos, incluyendo la posibilidad de que el interesado no los suministre. A este respecto, es necesario destacar la duración de la infracción, que continúa a día de hoy, sin perjuicio de que se iniciara en 2019.

- La intencionalidad o negligencia en la infracción (artículo 83.2 letra b)): se aprecia negligencia grave en la medida en que la falta de información se realiza en incumplimiento del Código de Deontología de la profesión farmacéutica aprobado por el Consejo General de Colegios Farmacéuticos, que establece que "*el farmacéutico deberá proporcionar la información al paciente/usuario de manera objetiva, actualizada, sencilla y adecuada a las posibilidades de comprensión de la persona a la que atiende, debiendo además hacerlo por escrito si así se lo solicitan". Asimismo, se determina que "los pacientes y usuarios tienen el derecho de conocer la identidad y cualificación del profesional que los atiende*".

- Las categorías de los datos de carácter personal afectados por las infracciones (artículo 83.2, letra g), del RGPD): las Directrices 04/2022 del Comité Europeo de Protección de Datos, sobre el cálculo de las multas bajo el RGPD, adoptadas el 24 de mayo de 2023, en su apartado 57, señalan lo siguiente en cuanto al requisito de tener en cuenta las categorías de los datos personales afectados: "(…)el RGPD destaca claramente los tipos de datos que merecen una protección especial y, por tanto, una respuesta más estricta en lo que respecta a las multas. Esto se refiere, como mínimo, a los tipos de datos a que se refieren los artículos 9 y 10 del RGPD y a los datos fuera del ámbito de aplicación de estos artículos cuya difusión provoque daños y perjuicios inmediatos al interesado (por ejemplo, datos de localización, datos sobre comunicación privada, números de identificación nacionales o datos financieros, como resúmenes de transacciones o números de tarjetas de crédito"). En el presente caso, los datos personales objeto de tratamiento incluyen datos de salud, como, por ejemplo, la pauta médica de los afectados o el número de la tarjeta sanitaria o CIPA.

Asimismo, se consideran los siguientes factores de graduación en calidad de agravantes:

- La vinculación de la actividad del infractor con la realización de tratamientos de datos personales (artículo 83.2 k) del RGPD en conexión con el artículo 76.2, letra b), de la LOPDGDD): la farmacia como consecuencia de su actividad en tanto que establecimiento sanitario privado, de interés público, realiza de forma habitual y continua tratamientos de datos de carácter personal de un elevado número de interesados (todos sus pacientes o usuarios) imprescindible para el desarrollo de su negocio. La realización de actividades de dispensación de productos médicos y farmacéuticos, que es su actividad principal, implica necesariamente operaciones de tratamiento de datos personales. Así, las acciones infractoras se producen en el marco de un tratamiento de datos personales que habitualmente realiza la farmacia en su negocio y ligado a este.

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 acuerdo de inicio de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, 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 14 del RGPD, permite fijar inicialmente una sanción de multa administrativa de 3.000,00€ (TRES MIL EUROS).

X

Obligación incumplida. Artículo 32 del RGPD. Seguridad del tratamiento.

El artículo 32 del RGPD establece:

"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 obligación de adoptar todas las medidas técnicas y organizativas impuesta por el artículo 32 del RGPD al responsable del tratamiento es una manifestación de los dos pilares esenciales del RGPD: la responsabilidad proactiva consagrada en el artículo 5.2 y desarrollada en el artículo 24.1 del RGPD y el enfoque de riesgos. Así, el artículo 32, si bien establece un conjunto de medidas que podrían considerarse mínimas a adoptar por el responsable, como la seudonimización o el cifrado de datos, en ningún caso puede entenderse como un *numerus clausus* puesto que estas deben atender a la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad que afecten a los datos personales.

Como se puede observar se ha pasado de un sistema reactivo a uno proactivo, basado en la prevención y no en la corrección y que debe operar durante todo el ciclo de vida de los datos personales, no únicamente en la recogida. A este respecto se pronuncia el Considerando 74 del RGPD cuando señala (el subrayado es de la AEPD):

> *"74 Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas físicas".*

Por su parte, el Considerando 75 determina:

> *"(75) Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados".*

En el presente caso, la farmacia**.** en tanto que establecimiento sanitario privado con interés público realiza de manera mayoritaria tratamientos de datos especialmente sensibles, como son los datos de salud. Esta circunstancia debe ser tenida en cuenta a la hora de establecer las medidas de seguridad adecuadas al riesgo.

El enfoque de riesgos en materia de protección de datos supone adoptar e implementar medidas destinadas a proteger la confidencialidad, la disponibilidad y la integridad de los datos personales en las que el riesgo para los derechos y libertades actúe como interruptor o modulador de las medidas a adoptar.

En esta línea la STJUE de 14 de diciembre de 2023, Natsionalna agentsia za prihodite, asunto C-340/21, EU:C:2023:986 señala:

> *"[*la adopción de medidas de seguridad en materia de protección de datos de carácter personal] *no se cumple con la adopción de cualquier medida, pues deben ser las necesarias para garantizar aquellos objetivos que marca el precepto, y por supuesto, no basta con la aprobación formal de las medidas de seguridad, ya que resulta exigible que aquéllas se instauren y pongan en práctica de manera efectiva. Hemos considerado, en consecuencia, que se impone una obligación de resultado, consistente en que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros. En definitiva, todo responsable de un fichero (o encargada de tratamiento) es, por disposición legal, una deudora de seguridad en materia de datos debiendo asegurarse de que dichas medidas o mecanismos se implementen de manera efectiva en la práctica."*

En el presente caso, existen elementos que pondrían de manifiesto que la parte denunciada carecía de las medidas técnicas y organizativas adecuadas al nivel de riesgo para garantizar la protección de los datos personales de los residentes tratados, especialmente la confidencialidad de los mismos.

De acuerdo con lo recogido en el acta ******ACTA.1*** de la Inspección de Farmacia, el intercambio de datos personales se realizaba de manera habitual mediante la remisión de archivos que contenían datos de salud en correos electrónicos sin cifrar

"(…)".

Es decir, desde la cuenta ******EMAIL.1*** y sin cifrar, se remitía a ***A.A.A.***, en hojas Excel, los datos personales de los pacientes que requerían pañales, incluyendo datos de salud, y posteriormente la parte denunciada enviaba un correo electrónico a la citada cuenta, con la relación de aportación monetaria de los residentes, que posteriormente le abonaban desde la otra farmacia***.***

Se señala que respecto a este medio de intercambio de datos personales constan en el expediente, al menos, dos correos que ponen de manifiesto la ausencia de encriptado, recogidos por la Inspección de Farmacia:

Un correo electrónico de fecha 16/11/2023 que contiene un intercambio de correos entre la dirección de correo ******EMAIL.1*** y ******EMAIL.2*** en el que se adjunta un documento Excel llamado ***"***EXCEL.1"*** que contiene el nombre y apellido de los residentes de la residencia ******RESIDENCIA.3*** que tienen pañales disponibles esa semana.

Un correo electrónico de fecha 17/11/2023 enviado desde la cuenta de correo ******EMAIL.2*** a la dirección de correo ******EMAIL.1*** y con copia a ******EMAIL.4*** con el texto: "*Adjunto ventas y aportación del17 de noviembre*". El correo lleva adjunto un documento Excel llamado ***"***EXCEL.2"*** que contiene, entre otra información, el nombre y apellido de residentes de ******RESIDENCIA.3.***

Esto pone de manifiesto, que ***A.A.A.*** carecía de un sistema seguro de envío y recepción de datos personales de los pacientes en residencias. Así, el canal de

comunicación establecido para el intercambio de información y datos personales entre ambas farmacias adolecía de una falta de medidas de seguridad adecuadas al riesgo. Se destaca, asimismo, que estas prácticas contravienen lo previsto en el RAT de la parte denunciada, remitido a esta Agencia en contestación al requerimiento de información durante las actuaciones previas de investigación, que señalaba:*"(…) se deben adoptar las medidas de seguridad de carácter técnico y organizativo de nivel alto (…)".*

Con relación a la seguridad del correo electrónico, el "Informe de buenas prácticas" de mayo de 2021, CNN-CERT BP02, del Centro Criptológico Nacional, servicio adscrito al Centro Nacional de Inteligencia, cuya misión es contribuir a la mejora de la ciberseguridad española, recoge una serie de vulnerabilidades del correo electrónico y de las diversas formas en que éstos pueden ser atacados, así como recomendaciones de seguridad. En el apartado 4.2 de dicho Informe se describe la "Seguridad de las comunicaciones vía email", con las siguientes aseveraciones en sus páginas 37 a 39: *"El protocolo involucrado en este proceso de envío es SMTP. Este protocolo ha sido utilizado desde 1982 y cuando fue implementando no se tuvieron en cuenta medidas de seguridad tales como el cifrado o la autenticación de las comunicaciones. Esto quiere decir que todo el proceso de envío descrito anteriormente se realizaría en texto plano, es decir, que en cualquier punto de la trasmisión un atacante podría ver y manipular el contenido de los correos. Debido a estas carencias en SMTP se han ido desarrollando diversas tecnologías y extensiones que permiten incorporar medidas de seguridad para garantizar la autenticación, integridad y cifrado a las comunicaciones vía correo electrónico. Algunas de las tecnologías más conocidas son STARTTLS, SPF, DKIM y DMARC…Aunque los proveedores de correo más conocidos como Google, Yahoo y Outlook cifran y autentican los emails utilizando este tipo de tecnologías, muchas organizaciones siguen haciendo un uso descuidado del correo electrónico. Téngase en cuenta, además, que estas tecnologías deben ser implementadas tanto en el origen como en el destino para que puedan utilizarse. Asimismo, algunas de estas medidas son susceptibles de ser atacadas. Por ejemplo, STARTTLS es susceptible a ataques downgrade, en donde un atacante en una situación man-in-the-middle puede forzar a que no que lleve a cabo la negociación TLS (bastaría con reemplazar la cadena STARTTLS).*

Incluso en el caso de que se establezca la comunicación TLS de forma satisfactoria, los servidores de correo por los que pasa el email hasta alcanzar el destino tendrían acceso a su contenido. Debido a estos hechos, se deduce que no es suficiente con delegar la seguridad del correo electrónico a las tecnologías subyacentes encargadas de hacer llegar el mismo a su destinatario."

Por tanto, de conformidad con las evidencias de las que se dispone en este momento de acuerdo de inicio de procedimiento sancionador, se considera que los hechos conocidos podrían ser constitutivos de una infracción, imputable a ***A.A.A.***, por vulneración del artículo 32 del RGPD transcrito anteriormente.

XI

Tipificación de la infracción del artículo 32 del RGPD y calificación a efectos de prescripción

De confirmarse, la citada infracción del artículo 32 del RGPD, podría suponer la comisión de las infracciones tipificadas en el artículo 83.4 del RGPD que dispone:

"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 este respecto, la LOPDGDD, en su artículo 71 establece 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"*.

A efectos del plazo de prescripción, 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."

XII

Propuesta de sanción por incumplimiento del artículo 32 del RGPD.

A fin de determinar la multa administrativa a imponer se han de observar las previsiones de los artículos 83.1 y 83.2 del RGPD y artículo 76 LOPDGDD, anteriormente citados.

En el presente caso, considerando la gravedad de la posible infracción, atendiendo especialmente a las consecuencias que su comisión provoca en los afectados, correspondería la imposición de multa, además de la adopción de medidas, si procede.

La multa que se imponga deberá ser, en cada caso individual, efectiva, proporcionada y disuasoria, conforme a lo establecido en el artículo 83.1 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 acuerdo de inicio de procedimiento sancionador, y sin perjuicio de lo que resulte de la

instrucción, se considera que procede graduar la sanción a imponer de acuerdo con las circunstancias siguientes, contempladas en los preceptos antes citados.

- Las categorías de los datos de carácter personal afectados por las infracciones (artículo 83.2, letra g), del RGPD): las Directrices 04/2022 del Comité Europeo de Protección de Datos, sobre el cálculo de las multas bajo el RGPD, adoptadas el 24 de mayo de 2023, en su apartado 57, señalan lo siguiente en cuanto al requisito de tener en cuenta las categorías de los datos personales afectados: "(…)el RGPD destaca claramente los tipos de datos que merecen una protección especial y, por tanto, una respuesta más estricta en lo que respecta a las multas. Esto se refiere, como mínimo, a los tipos de datos a que se refieren los artículos 9 y 10 del RGPD y a los datos fuera del ámbito de aplicación de estos artículos cuya difusión provoque daños y perjuicios inmediatos al interesado (por ejemplo, datos de localización, datos sobre comunicación privada, números de identificación nacionales o datos financieros, como resúmenes de transacciones o números de tarjetas de crédito"). En el presente caso, los datos personales objeto de tratamiento incluyen datos de salud, como, por ejemplo, la pauta médica de los afectados o el número de la tarjeta sanitaria o CIPA, sin perjuicio que el TJUE haya establecido un concepto amplio de datos salud.

Asimismo, se consideran los siguientes factores de graduación en calidad de agravante:

- La vinculación de la actividad del infractor con la realización de tratamientos de datos personales (artículo 83.2 k) del RGPD en conexión con el artículo 76.2, letra b), de la LOPDGDD): ***A.A.A.*** como consecuencia de su actividad en tanto que establecimiento sanitario privado, de interés público, realiza de forma habitual y continua tratamientos de datos de carácter personal de un elevado número de interesados (todos sus pacientes o usuarios) imprescindible para el desarrollo de su negocio. La realización de actividades de dispensación de productos médicos y farmacéuticos, que es su actividad principal, implica necesariamente operaciones de tratamiento de datos personales. Así, las acciones infractoras se producen en el marco de un tratamiento de datos personales que habitualmente realiza la farmacia en su negocio y ligado a este.

De acuerdo con los preceptos transcritos, y sin perjuicio de lo que resulte de la instrucción del procedimiento, la valoración inicial que alcanza la cuantía de la multa es de 3.000,00€ euros (TRES MIL EUROS), por infracción del artículo 32 del RGPD.

XIII
Medidas correctivas

De confirmarse la infracción, la resolución que se dicte podrá establecer las medidas correctivas que la entidad infractora deberá adoptar para poner fin al incumplimiento de la legislación de protección de datos personales, en este caso de los artículos 9 y 28 del RGPD de acuerdo con lo establecido en el citado artículo 58.2.d) del RGPD, según el cual cada autoridad de control podrá "*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…"

Así, se podrá requerir a la entidad responsable para que adecúe su actuación a la normativa de protección de datos personales, con el alcance expresado en los anteriores Fundamentos de Derecho.

En el presente acto se establece cuál es la presunta infracción cometida y los hechos que podrían dar lugar a esa posible vulneración de la normativa de protección de datos, de lo que se infiere con claridad cuáles son las medidas a adoptar, sin perjuicio de que el tipo de procedimientos, mecanismos o instrumentos concretos para implementarlas corresponda a la parte sancionada, pues es el responsable del tratamiento quien conoce plenamente su organización y ha de decidir, en base a la responsabilidad proactiva y en enfoque de riesgos, cómo cumplir con el RGPD y la LOPDGDD.

No obstante, en este caso, con independencia de lo anterior, de conformidad con las evidencias de que se dispone en el presente momento de acuerdo de inicio de procedimiento sancionador, en la resolución que se adopte se podrá requerir a ***A.A.A.*** para que, en el plazo de 3 meses, a contar desde la fecha de ejecutividad de la resolución finalizadora de este procedimiento, adopte las medidas siguientes:

- Acreditar el cese del tratamiento de datos personales para la dispensación de pañales a los residentes de los centros geriátricos *****RESIDENCIA.4** y *****RESIDENCIA.5,** así como la supresión de los mencionados datos personales, salvo que acredite la existencia de una base de legitimación para dicho tratamiento.
- Acreditar, en caso de contar con una base de legitimación que ampare el tratamiento de sus datos personales, la puesta a disposición de la información contenida en el artículo 14 del RGPD a los residentes de los centros geriátricos ******RESIDENCIA.4*** y ******RESIDENCIA.5.***

La imposición de estas medidas es compatible con la sanción consistente en multa administrativa, según lo dispuesto en el art. 83.2 del RGPD.

Se advierte que no atender la posible orden de adopción de medidas impuestas por este organismo en la resolución del presente procedimiento sancionador podrá ser considerado como una infracción administrativa conforme a lo dispuesto en el RGPD, tipificada como infracción en su artículo 83.5 y 83.6, pudiendo motivar tal conducta la apertura de un ulterior procedimiento administrativo sancionador.

Asimismo, se recuerda que ni el reconocimiento de la infracción cometida ni, en su caso, el pago voluntario de las cuantías propuestas, eximen de la obligación de adoptar las medidas pertinentes para que cese la conducta o se corrijan los efectos de la infracción cometida y la de acreditar ante esta AEPD el cumplimiento de esa obligación.

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

PRIMERO: INICIAR PROCEDIMIENTO SANCIONADOR a ***A.A.A.***, con NIF ******NIF.1***, por:

- Una presunta infracción del artículo 6 del RGPD tipificada en el artículo 83.5.a) del RGPD.
- - Una presunta infracción del artículo 14 del RGPD, tipificada en el artículo 83.5. h) del RGPD.
- Una presunta infracción del artículo 32 del RGPD, tipificada en el artículo y 83.4. a) del RGPD

SEGUNDO: NOMBRAR como instructora a ***R.R.R.*** y, como secretaria, a ***S.S.S.,*** indicando que podrán ser recusados, en su caso, conforme a lo establecido en los artículos 23 y 24 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP).

TERCERO: INCORPORAR al expediente, a efectos probatorios, así como los documentos obtenidos y generados por la Subdirección General de Inspección de Datos en las actuaciones previas al inicio del presente procedimiento sancionador.

CUARTO: QUE a los efectos previstos en el art. 64.2 b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la sanción que pudiera corresponder sería de multa administrativa de:

-Por la presunta infracción del artículo 6 del RGPD, una multa administrativa de 5.000 euros.

-Por la presunta infracción el artículo 14 del RGPD, una multa administrativa de 3.000 euros.

- Por la presunta infracción del artículo 32 del RGPD una multa administrativa de 3.000 euros

Lo anterior supone un total de 11.000 euros, sin perjuicio de lo que resulte de la instrucción.

QUINTO: NOTIFICAR el presente acuerdo a ***A.A.A.***, con NIF ******NIF.1***, otorgándole un plazo de audiencia de diez días hábiles para que formule las alegaciones y presente las pruebas que considere convenientes. En su escrito de alegaciones deberá facilitar su NIF y el número de procedimiento que figura en el encabezamiento de este documento.

De conformidad con lo dispuesto en el artículo 85 de la LPACAP, podrá reconocer su responsabilidad dentro del plazo otorgado para la formulación de alegaciones al presente acuerdo de inicio; lo que llevará aparejada una reducción de un 20% de la sanción que proceda imponer en el presente procedimiento. Con la aplicación de esta reducción, la sanción quedaría establecida en **8.800€** euros, resolviéndose el procedimiento con la imposición de esta sanción.

Del mismo modo podrá, en cualquier momento anterior a la resolución del presente procedimiento, llevar a cabo el pago voluntario de la sanción propuesta, lo que supondrá la reducción de un 20% de su importe. Con la aplicación de esta reducción,

la sanción quedaría establecida en **8.800€** euros y su pago implicará la terminación del procedimiento, sin perjuicio de la imposición de las medidas correspondientes.

La reducción por el pago voluntario de la sanción es acumulable a la que corresponde aplicar por el reconocimiento de la responsabilidad, siempre que este reconocimiento de la responsabilidad se ponga de manifiesto dentro del plazo concedido para formular alegaciones a la apertura del procedimiento. El pago voluntario de la cantidad referida en el párrafo anterior podrá hacerse en cualquier momento anterior a la resolución. En este caso, si procediera aplicar ambas reducciones, el importe de la sanción quedaría establecido en **6.600€ euros**.

En todo caso, la efectividad de cualquiera de las dos reducciones mencionadas estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

En caso de que optara por proceder al pago voluntario de cualquiera de las cantidades señaladas anteriormente (**8.800€** euros o **6.600 euros**), deberá hacerlo efectivo mediante su ingreso en la cuenta nº ***IBAN: ES00-0000-0000-0000-0000-0000 (BIC/Código SWIFT: CAIXESBBXXX)*** abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A., indicando en el concepto el número de referencia del procedimiento que figura en el encabezamiento de este documento y la causa de reducción del importe a la que se acoge.

Asimismo, deberá enviar el justificante del ingreso a la Subdirección General de Inspección junto con la comunicación expresa del desistimiento o renuncia a cualquier acción o recurso en vía administrativa contra la sanción para continuar con el procedimiento en concordancia con la cantidad ingresada.

Por último, se señala que conforme a lo establecido en el artículo 112.1 de la LPACAP, contra el presente acto no cabe recurso administrativo alguno.

1479-130325

Lorenzo Cotino Hueso
Presidente de la Agencia Española de Protección de Datos
>>

SEGUNDO**:** En fecha 16 de abril de 2025, ***A.A.A.*** ha procedido al pago de la sanción en la cuantía de **6.600,00 euros** haciendo uso de las dos reducciones previstas en el acuerdo de inicio transcrito anteriormente, lo que implica el reconocimiento de la responsabilidad en relación con los hechos a los que se refiere el acuerdo de inicio y su calificación jurídica.

TERCERO: En el acuerdo de inicio transcrito anteriormente se señalaba que, de confirmarse la infracción, podría acordarse imponer al responsable la adopción de medidas adecuadas para ajustar su actuación a la normativa mencionada en este acto, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá *"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…".*

Habiéndose reconocido la responsabilidad de la infracción, procede la imposición de las medidas incluidas en el acuerdo de inicio.

FUNDAMENTOS DE DERECHO

I
Competencia

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 resolver este procedimiento la Presidencia 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
Terminación del procedimiento

El artículo 85 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP), bajo la rúbrica "*Terminación en los procedimientos sancionadores*" dispone lo siguiente:

"1. Iniciado un procedimiento sancionador, si el infractor reconoce su responsabilidad, se podrá resolver el procedimiento con la imposición de la sanción que proceda.

2. Cuando la sanción tenga únicamente carácter pecuniario o bien quepa imponer una sanción pecuniaria y otra de carácter no pecuniario pero se ha justificado la improcedencia de la segunda, el pago voluntario por el presunto responsable, en cualquier momento anterior a la resolución, implicará la terminación del procedimiento, salvo en lo relativo a la reposición de la situación alterada o a la determinación de la indemnización por los daños y perjuicios causados por la comisión de la infracción.

3. En ambos casos, cuando la sanción tenga únicamente carácter pecuniario, el órgano competente para resolver el procedimiento aplicará reducciones de, al menos, el 20 % sobre el importe de la sanción propuesta, siendo éstos acumulables entre sí. Las citadas reducciones, deberán estar determinadas en la notificación de iniciación del procedimiento y su efectividad estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

El porcentaje de reducción previsto en este apartado podrá ser incrementado reglamentariamente."

III
Pago voluntario y reconocimiento de responsabilidad

De conformidad con lo dispuesto en el citado artículo 85 de la LPACAP, en el acuerdo de inicio notificado se informaba sobre la posibilidad de reconocer la responsabilidad y de realizar el pago voluntario de la sanción propuesta, lo que supondría dos reducciones acumulables de un 20% cada una. Con la aplicación de estas dos reducciones, la sanción quedaría establecida en **6.600,00 euros** y su pago implicaría la terminación del procedimiento, sin perjuicio de la imposición de las medidas correspondientes.

Tras la notificación del citado acuerdo de inicio, ***A.A.A.*** ha procedido al reconocimiento de la responsabilidad y al pago voluntario de la sanción, acogiéndose a las dos reducciones previstas. De conformidad con el apartado 3 del artículo 85 LPACAP, la efectividad de las citadas reducciones estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

Debe tenerse en cuenta que, de acuerdo con los preceptos de la LPACAP, así como de la jurisprudencia del Tribunal Supremo en esta materia, el ejercicio del pago voluntario por el presunto responsable no exime a la administración de la obligación de resolver y notificar todos los procedimientos, cualquiera que sea su forma de iniciación. De igual forma, el artículo 88 de la citada norma establece que la resolución que ponga fin al procedimiento decidirá todas las cuestiones planteadas por los interesados y aquellas otras derivadas del mismo.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones, la Presidencia de la Agencia Española de Protección de Datos RESUELVE**:**

PRIMERO: DECLARAR la comisión de las infracciones y CONFIRMAR las sanciones determinadas en la parte dispositiva del acuerdo de inicio transcrito en la presente resolución.

La suma de las citadas cuantías arroja una cantidad total **11.000,00 euros.**

Tras haber procedido ***A.A.A.*** al pronto pago y reconocimiento de responsabilidad, se procede, en virtud del artículo 85 de la LPACAP, a la reducción de un 40% del total mencionado, lo cual supone la cantidad definitiva de **6.600,00 euros**.

La efectividad de las citadas reducciones está condicionada, en todo caso, al desistimiento o renuncia de cualquier acción o recurso en vía administrativa.

SEGUNDO: DECLARAR la terminación del procedimiento **EXP202414356**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

TERCERO: ORDENAR a ***A.A.A.*** para que en el plazo de 3 meses desde que la presente resolución sea firme y ejecutiva, notifique a la Agencia la adopción de las medidas que se describen en los fundamentos de derecho del acuerdo de inicio transcrito en la presente resolución.

CUARTO: NOTIFICAR la presente resolución a ***A.A.A.***.

QUINTO: De acuerdo con lo previsto en el artículo 85 de la LPACAP que condiciona la reducción por pago voluntario y reconocimiento de la responsabilidad al desistimiento o renuncia de cualquier acción o recurso en vía administrativa, la presente resolución será firme en vía administrativa y plenamente ejecutiva a partir de su notificación.

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 según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer 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.

No obstante, conforme a lo previsto en el artículo 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://sedeaepd.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.

1259-260325

Lorenzo Cotino Hueso
Presidente de la Agencia Española de Protección de Datos