

- **Expediente N°: PS/00373/2021**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: Con fecha 6 de agosto de 2020, la directora de la AEPD, tiene constancia de que en fecha 29 de julio de 2020, se publica en el Boletín Oficial del Principado de Asturias, la "Resolución de 29 de julio de 2020, de la Consejería de Salud, de tercera modificación de las medidas urgentes de prevención, contención y coordinación necesarias para hacer frente a la crisis sanitaria ocasionada por el COVID-19" (en adelante, la Resolución de 29 de julio de 2020).

Esta resolución incorpora en el apartado 3.4. del Anexo la obligación para determinados tipos de establecimientos de contar con un registro de clientes y usuarios a disposición de la Dirección General de Salud Pública, con la finalidad de "facilitar el rastreo y seguimiento de contactos de casos positivos o sospechosos de Covid-19". La propia resolución estipula que "la recogida de tales datos requerirá el consentimiento del interesado, sin perjuicio de condicionar el derecho de admisión por razones de salud pública en caso de no poder contar con el mismo". Asimismo, recomienda la adopción de sistemas de registro similares por parte de los titulares de los establecimientos de hostelería y restauración, discotecas y locales de ocio nocturno.

Al objeto de aclarar este tratamiento, insta a la Subdirección General de Inspección de Datos (en adelante, SGID), a iniciar las actuaciones previas de investigación a las que se refiere el artículo 67 de la Ley Orgánica 3/2018, de 6 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en lo sucesivo, LOPDGDD), por si de tales hechos se desprendieran indicios de infracción en el ámbito competencial de la AEPD.

SEGUNDO: A la vista de estos hechos descritos, la SGID procede a la realización de actuaciones previas de investigación para su esclarecimiento, en virtud de los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD.

En el marco de las actuaciones previas de investigación se practica un primer requerimiento de información dirigido a la CONSEJERÍA DE SALUD DEL GOBIERNO DEL PRINCIPADO DE ASTURIAS (en adelante, la investigada):

En este requerimiento, de fecha 7 de agosto de 2020, se solicita la siguiente información:

“1. Finalidad del tratamiento de datos personales y base jurídica en la que se sustenta.

2. Valoración de la proporcionalidad del tratamiento (juicio de idoneidad, de necesidad, y de proporcionalidad en sentido estricto).

3. Detalle de las categorías de datos personales objeto de tratamiento y valoración del cumplimiento con el principio de minimización de datos.

4. Determinación de las categorías de establecimientos obligados a la implantación de la medida y explicación del motivo de su elección frente a otros.

5. Descripción del proceso que permite la consecución de la finalidad prevista con indicación, para cada uno de los participantes en el mismo, de:

5.1. Vinculación con el tratamiento (responsable, corresponsable, encargado, tercero, interesado) de cada participante. Detalle del contrato o acto jurídico que vincula al encargado del tratamiento con el responsable del mismo, de acuerdo con lo estipulado en el artículo 28 del RGPD.

5.2. Descripción del tratamiento concreto que realiza (registro, consulta, comunicación, supresión, etc.) cada participante. Especificación, en su caso, del formato en que almacenará los datos personales (digital / papel).

5.3. Procedimiento de comunicación de los datos del registro de cada establecimiento a las autoridades sanitarias: detalle del canal de comunicación (postal, correo electrónico, telefónico, etc.) y de los eventos que provocan el envío (frecuencia concreta y/o a petición de las autoridades sanitarias).

5.4. Indicación de la posibilidad o no de que participen “subencargados” de tratamiento (entidades contratadas por los establecimientos para efectuar partes del tratamiento que se les asigna).

5.5. Plazos de conservación de los datos de cada participante y determinación de si, finalizada la prestación del servicio, los encargados deben suprimir o devolver los datos al responsable. Especificar, en su caso, la normativa que requiere a los encargados la conservación de los datos una vez finalizada la prestación.

5.6. Medios utilizados para el cumplimiento del deber de información al interesado.

5.7. Garantías aplicadas para el cumplimiento de las obligaciones impuestas en el Capítulo IV del RGPD en materia de medidas de seguridad.”

El requerimiento se notifica a la investigada en fecha 9 de agosto de 2020, a través del Servicio de Notificaciones Electrónicas y Dirección Electrónica Habilitada, según certificado que figura en el expediente.

TERCERO: En fecha 26 de agosto de 2020, la investigada aduce las alegaciones que estima convenientes y a las que se da respuesta en el informe emitido por la SGID, que se reproduce en el apartado Sexto.

CUARTO: En fecha 15 de abril de 2021, la AEPD practica un segundo requerimiento en los siguientes términos:

“A este respecto, en el marco de las actuaciones practicadas por la Subdirección General de Inspección de Datos y en uso de las facultades conferidas por el artículo 58.1 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (en adelante RGPD), y el art. 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), se solicita que en el plazo de diez días hábiles presente la siguiente información:

1. *Descripción de la situación actual de las medidas relativas a la obligación de registro recogidas en dicha resolución. Referencia a la vigencia de estas y, en su caso, a la tipología de establecimientos afectados.*
2. *Detalle de cualquier otra circunstancia relacionada con el tratamiento de los datos personales objeto de registro cuya puesta en práctica haya diferido de lo especificado en el escrito*****ESCRITO.1.**”*

Asimismo, se informa de que el responsable y el encargado del tratamiento de los datos de carácter personal tienen la obligación de facilitar los documentos, informaciones y cualquier otra colaboración que se precisen para realizar la función de inspección.

El requerimiento se notifica a la investigada en fecha 15 de abril de 2021, a través del Servicio de Notificaciones Electrónicas y Dirección Electrónica Habilitada, según certificado que figura en el expediente.

QUINTO: En respuesta al segundo requerimiento, en fecha 22 de abril de 2021, la investigada aduce las alegaciones que estima convenientes y a las que se da respuesta en el informe emitido por la SGID, que se reproduce en el apartado siguiente.

SEXTO: Con fecha 23 de abril de 2021, una vez realizadas las actuaciones previas de investigación a fin de lograr una mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento, la SGID emite un informe en el que se constatan los siguientes hechos:

“RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

El presente informe se apoya sobre la siguiente información:

- Escrito de la Consejería registrado de entrada en la AEPD (núm.*****ESCRITO.1**) con fecha de 26 de agosto de 2020 (en adelante EscritoConsejería1).
- Escrito de la Consejería registrado de entrada en la AEPD (núm.*****ESCRITO.2**) con fecha de 22 de abril de 2021 (en adelante EscritoConsejería2).

(...)

Se consigna a continuación el siguiente contenido del Comunicado AEPD relacionado con el objeto de las presentes actuaciones:

“[...] A este respecto, es necesario puntualizar que los datos que se recogen, aunque estén relacionados con el control de la pandemia y su tratamiento sea al objeto de poder identificar posibles infectados, no son datos catalogados en el RGPD como “categorías especiales”.

Para poner en marcha el registro de clientes que acuden a locales de ocio, tratándose de una medida para la contención del coronavirus, debe acreditarse su necesidad por las autoridades sanitarias y tiene que ser obligatoria, ya que si fuera voluntaria perdería efectividad. Adicionalmente, si se acudiera a la base jurídica del consentimiento, para poder apreciar un consentimiento libre, sería necesario que no se derivara ninguna consecuencia negativa, es decir, que no se impidiera la entrada al establecimiento.

Teniendo en cuenta que ya no está vigente el estado de alarma, la obligatoriedad de tomar datos por parte de los establecimientos tiene que establecerse por una norma con rango de ley. En tal caso, la base jurídica sería el 6.1.c) (“el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento”).

En todo caso, debe señalarse que el hacer un seguimiento adecuado de la evolución de los contagios y de la obligación de tomar datos y cederlos a las autoridades sanitarias tiene su fundamento en la garantía de un interés público de controlar la pandemia, por lo que la base jurídica sería, con carácter preferente, el artículo 6.1.e) del RGPD (“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”).

A estos efectos, debe hacerse especial incidencia en la necesidad de justificar que no existan otras medidas más moderadas para la consecución del propósito perseguido con igual eficacia. Por ello deberían identificarse bien y limitarse a aquellos sitios en los que exista una mayor dificultad para el cumplimiento de estas medidas (no es lo mismo una discoteca, en la que las personas quieren estar cerca, que un museo, en el que se pueden habilitar espacios adecuados para que circule la gente y limitar mucho los contactos). A tal efecto, deberían ser las autoridades sanitarias quienes valoren motivadamente en qué lugares sería obligatorio identificarse.

Por otro lado, la recogida y la cesión de datos debería organizarse de una forma que el registro permita identificar los posibles contactos (es decir, que exista una probabilidad de que hayan coincidido, al estar en la misma hora, en el mismo sitio, etcétera). En otro caso, como podría suceder en un museo, si hay un infectado y se avisa a las miles de personas que ese día lo pudieron haber visitado, aparte de ser un tratamiento excesivo, podrían producirse dificultades o incluso un colapso en la asistencia sanitaria. Cuestión que también tienen que valorar las autoridades sanitarias de las Comunidades Autónomas.

Adicionalmente, debe cumplirse con el principio de minimización, en virtud del cual podría ser suficiente con obtener un número de teléfono, junto con los datos del día y la hora de asistencia al lugar. Este criterio, junto con el de la anonimización de los

titulares del dispositivo, ha sido el asumido por el Comité Europeo de Protección de Datos en la Recomendación sobre el uso de datos de localización y aplicaciones de seguimiento de contactos en el contexto de la pandemia; criterio que puede extrapolarse a esta situación con las adaptaciones pertinentes.

En consecuencia, no sería necesario solicitar el nombre y los apellidos, que serían innecesarios para la finalidad de avisar a los posibles contactos, y en ningún caso es necesaria la identificación mediante el DNI por ser desproporcionada.

Asimismo, debe aplicarse estrictamente el principio de limitación de la finalidad, de forma que los datos sólo deben poder utilizarse para la finalidad de lucha contra el virus, excluyendo cualquier otra, así como el principio de limitación del plazo de conservación.

De acuerdo con estos criterios, los establecimientos serían responsables de la recogida de datos en virtud de una obligación legal establecida por una norma con rango de ley y la administración autonómica sería la cesionaria de esos datos por razones de interés público previstos en la ley. La administración autonómica deberá establecer criterios sobre la forma en la que se recogen y comunican esos datos personales a la Administración sanitaria.

Por su parte, los ciudadanos deben recibir una información clara, sencilla y accesible sobre el tratamiento antes de la recogida de los datos personales. En todo caso, la información debe tratarse con las medidas de seguridad adecuadas."

Con respecto a las medidas relacionadas con el registro de los clientes de determinados establecimientos tomadas por la Consejería, se recoge a continuación información sobre los distintos aspectos:

1. Sobre la finalidad de los tratamientos de datos personales.

En relación con la finalidad, el EscritoConsejería1 manifiesta que "La obligación de registrar los datos y el teléfono de contacto de los clientes y usuarios que acuden a hoteles, albergues y otros alojamientos turísticos, peluquerías, barberías, centros de belleza, gabinetes de estética, salones de manicura, pedicura y depilación, saunas, balnearios, spas y gimnasios, tiene como única finalidad facilitar el rastreo y seguimiento de contactos de casos positivos o sospechosos de Covid-19". Además, señala igualmente que "[...] el registro de datos y teléfono de contacto se encontrará exclusivamente a disposición de la Dirección General de Salud Pública y tendrá como única finalidad facilitar el rastreo y seguimiento de contactos de casos positivos o sospechosos de Covid-19".

2. Sobre las categorías de datos personales objeto de tratamiento.

A este respecto el EscritoConsejería1 señala que los datos personales que se tratarán para esta finalidad son "Nombre y/o apellidos y número de teléfono de contacto". Añade además que "los datos que se citan son los estrictamente necesarios para la finalidad pretendida, además de ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. Disponer de un nombre o de un apellido y un número de teléfono son datos mínimos que servirán para disponer de forma inmediata de datos de contactos de las personas para poder afrontar rápidamente el seguimiento de los casos e interrumpir las cadenas de transmisión que puedan originarse en ciertos establecimientos."

3. Sobre el alcance de las medidas.

En el EscritoConsejería1 se aporta el siguiente listado de establecimientos afectados por esta medida:

“Obligatorio: titulares de hoteles, albergues y otros alojamientos turísticos, peluquerías, barberías, centros de belleza, gabinetes de estética, salones de manicura, pedicura y depilación, saunas, balnearios, spas y gimnasios.

Justificación: Todos estos establecimientos funcionan con un sistema de cita previa donde ya consta el nombre y teléfono. Disponer de estos no presenta dificultades para los titulares de los mismos, y sin embargo, en estos momentos de crisis sanitaria ocasionada por la COVID-19 proporciona una información muy útil y valiosa para controlar la expansión del virus.

Recomendación: titulares de los establecimientos de hostelería y restauración, discotecas y locales de ocio nocturno

Justificación: En este caso es una recomendación porque estos establecimientos no disponen de un sistema de cita previa y resultaría desproporcionado exigirlo. Sin embargo, con la finalidad de buscar la proporcionalidad de la medida, con bien es sabido, en estos locales circula un número muy elevado de personas cuyo registro, de existir favorecería enormemente la identificación de las personas a los efectos de poder realizar la adecuada investigación epidemiológica y prevenir de forma eficaz la protección de la salud de la población.”

En relación con la evolución de esta medida, la Consejería, como parte del EscritoConsejería2, manifiesta lo siguiente:

“Por Resolución de 29 de julio de 2020, de la Consejería de Salud, se efectúa la tercera modificación de las medidas urgentes de prevención, contención y coordinación necesarias para hacer frente a la crisis sanitaria ocasionada por el COVID-19, donde se recogía como medida en materia de salud pública, todo ello con la finalidad de facilitar el rastreo y seguimiento de contactos de casos positivos o sospechosos de Covid-19, la obligación de registrar los datos y el teléfono de contacto de los clientes y usuarios que accedan a hoteles, albergues y otros alojamientos turísticos, peluquerías, barberías, centros de belleza, gabinetes de estética, salones de manicura, pedicura y depilación, saunas, balnearios, spas y gimnasios. Se recoge también una recomendación en el mismo sentido para los establecimientos de hostelería y restauración, discotecas y locales de ocio nocturno.

Dentro del contenido de la parte dispositiva de la citada resolución se señala en el apartado tercero relativo al seguimiento y aplicación de la medida que el cumplimiento de las medidas previstas en esta resolución será objeto de seguimiento y evaluación continua con el fin de garantizar su adecuación a la evolución de la situación epidemiológica y sanitaria. A estos efectos, podrán ser objeto de modificación o supresión mediante Resolución de la Consejería competente en materia de sanidad.

Por su parte, el apartado sexto recoge la vigencia de la medida, señalando que la presente resolución producirá efectos desde su publicación en el Boletín Oficial del Principado de Asturias y mantendrá su vigencia hasta que el Gobierno declare la finalización de la situación de crisis sanitaria ocasionada por el COVID-19, al amparo del artículo 2.3 del Real Decreto-ley 21/2020, de 9 de junio, (hoy Ley 2/2021, de 29 de marzo, de medidas urgentes de prevención, contención y coordinación para hacer frente a la crisis sanitaria ocasionada por el COVID-19).

En consecuencia, procede informar que la medida sigue vigente en las mismas condiciones que las establecidas inicialmente, sin que haya sido objeto de modificación alguna.

Por otro lado, la medida mantiene su vigencia hasta que el Gobierno declare la finalización de la crisis sanitaria. Ahora bien, nada impedirá que cuando desaparezca la situación epidemiológica que originó la necesidad de su adopción (pudiendo ser previa a la finalización de la declaración de crisis sanitaria), la misma se deje sin efecto para garantizar en todo momento la idoneidad [sic], necesidad y proporcionalidad que presiden la adopción de estas medidas especiales.”

4. Sobre la base jurídica del tratamiento de datos personales.

En relación con la base jurídica de los tratamientos de datos personales derivados de la imposición de la medida, el EscritoConsejería¹ refiere que:

“La base de legitimación se ha entendido que viene determinada por el artículo 9.2.i) del Reglamento (UE) 2016/6753 (el tratamiento es necesario por razones de interés público en el ámbito de la salud pública), con apoyo legal interno en la Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública, y más específicamente en su artículo 3 cuando dispone que “Con el fin de controlar las enfermedades transmisibles, la autoridad sanitaria, además de realizar las acciones preventivas generales, podrá adoptar las medidas oportunas para el control de los enfermos, de las personas que estén o hayan estado en contacto con los mismos y del medio ambiente inmediato, así como las que se consideren necesarias en caso de riesgo de carácter transmisible”.

Si bien ciertamente los datos que se recogen no son, en sí mismos, datos especialmente protegidos como pertenecientes a categorías especiales de datos, tanto la finalidad de su recogida como su única cesión prevista, determinan un exclusivo uso de carácter sanitario. Así, se señala que el registro de datos y teléfono de contacto se encontrará exclusivamente a disposición de la Dirección General de Salud Pública y tendrá como única finalidad facilitar el rastreo y seguimiento de contactos de casos positivos o sospechosos de Covid-19.

En este sentido, debemos señalar que el considerando 46 del Reglamento 2016/679 establece que el tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no puede basarse manifiestamente en una base jurídica diferente. 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.

Por otro lado, es preciso señalar que el Decreto-Ley se encuentra regulado en el Artículo 86 de la Constitución Española. Es una norma con rango de ley propia del Ejecutivo. Podrá ser dictado por el Gobierno cuando exista un presupuesto habilitante que lo justifique, que ha de ser una extraordinaria y urgente necesidad de regulación de esa materia concreta. Sin embargo, esta figura no está prevista en el ordenamiento jurídico asturiano por lo que para aprobar una Ley sería necesario un periodo de tiempo de varios meses que resultaría incompatible con la situación

de crisis sanitaria actual que demanda de medidas urgentes y extraordinarias en el menor plazo posible.

Igualmente, es preciso traer a colación el Informe de la Agencia de Protección de Datos nº 0017/2020 donde se recoge que existen salvaguardas necesarias para permitir legítimamente los tratamientos de datos personales en situaciones de emergencia sanitaria como la que nos encontramos, respetando los principios establecidos como es la limitación de la finalidad para salvaguardar intereses vitales como son la salud de las personas.”

5. Sobre la proporcionalidad de los tratamientos de datos personales.

En el EscritoConsejería1 se aporta la siguiente valoración a este respecto:

“Idoneidad y necesidad: Como señala la Resolución de 29 de julio de 2020, de la Consejería de Salud, de tercera modificación de las medidas urgentes de prevención, contención y coordinación necesarias para hacer frente a la crisis sanitaria ocasionada por el COVID-19 en el momento actual, nos encontramos en una situación crítica y de excepcional trascendencia para la salud mundial y para la salud de la población asturiana. La evolución de la pandemia será dinámica y muchas de las decisiones que se vayan tomando tendrán que ser consecuentes a los cambios epidemiológicos en cada momento. Aunque la tendencia epidemiológica de incidencia de casos en nuestra comunidad autónoma ha sido muy contenida desde el 11 de junio -siendo una de las regiones europeas con menos casos- tanto la situación actual de brotes en otras comunidades autónomas como el incremento de tránsito de personas de zonas con más incidencia, suponen que haya una alta probabilidad de aparición de nuevos casos y de brotes a lo largo de las próximas semanas. Sería importante mantener una incidencia contenida tanto para establecer un adecuado control en el presente como para poder llegar al otoño con la mejor situación epidemiológica posible y con un sistema de salud pública y sanitario recuperado del impacto que ha supuesto la primera onda epidémica, y así, de esta forma, garantizar los mejores servicios de vigilancia, prevención y atención a la población asturiana.

Proporcionalidad: La obligación de registrar los datos y el teléfono de contacto de los clientes y usuarios que acudan a hoteles, albergues y otros alojamientos turísticos, peluquerías, barberías, centros de belleza, gabinetes de estética, salones de manicura, pedicura y depilación, saunas, balnearios, spas y gimnasios, tiene como única finalidad facilitar el rastreo y seguimiento de contactos de casos positivos o sospechosos de Covid-19.

Además, la medida no implica en general una carga significativa para los establecimientos afectados dado que en la actualidad muchos de ellos llevan registros de sus clientes o usuarios o emplean sistemas de cita previa. Esta medida tiene carácter voluntario para los titulares de establecimientos de hostelería y restauración, discotecas y locales de ocio nocturno.

La [sic] medidas que se adoptan contienen la regulación imprescindible para la consecución de los objetivos de facilitar el rastreo y seguimiento de contactos de casos positivos o sospechosos de Covid-19, ya que resultan proporcionadas al bien público que se trata de proteger.

La identificación, cuarentena y seguimiento de los contactos de casos de COVID-19. constituye uno de los pilares básicos para conseguir interrumpir las cadenas de transmisión que pueden originarse en establecimientos donde coinciden en el

tiempo personas no convivientes en condiciones en las que no siempre se puede asegurar una adecuada distancia interpersonal. En este sentido, la posibilidad de disponer de forma inmediata de los datos de contacto de las personas que hayan podido coincidir con casos de COVID19 en estos establecimientos, durante los periodos de riesgo de transmisibilidad de la infección de estos casos, supone una mejora importante en la rapidez y la efectividad de la adopción de medidas de control sobre estos contactos.

Igualmente, es preciso señalar que la recogida de tales datos requerirá el consentimiento del interesado. Bien es cierto que incluso el considerando 54 del RGPD admite que el tratamiento de categorías, especiales de datos personales puede ser necesario por razones de interés público en el ámbito de la salud pública sin contar con el consentimiento del interesado. Nuevamente, podemos observar como la medida establecida por esta Consejería resulta proporcionada a la finalidad perseguida y pretende respetar en todo momento el principio de minimización del dato.”

6. Sobre los plazos de conservación de los datos personales.

Sobre esta materia el EscritoConsejería1 refiere únicamente lo siguiente:

“Por ello, solo será necesario acudir a los datos registrados (nombre y/o apellidos y teléfono) cuando estemos ante un caso positivo o sospechoso de Covid-19. Los datos deberán ser suprimidos pasados un mes desde el acceso ya que transcurrido dicho plazo, pierden su finalidad, cual es la de hacer frente a la crisis sanitaria a la nos enfrentamos.”

SÉPTIMO: De conformidad con las evidencias de las que se dispone, la SGID considera que el tratamiento de los datos personales que se realiza por la investigada no cumple las condiciones que impone la normativa sobre protección de datos, por lo que procede la apertura del presente procedimiento sancionador.

OCTAVO: Con fecha 22 de julio de 2021, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, con arreglo a lo dispuesto en los artículos 63 y 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), por la presunta infracción de los artículos 5.1.c), 5.1.e), 7 y 13 del RGPD, tipificadas en el artículo 83.5 del RGPD y el artículo 72.1 de la LOPDGDD.

Asimismo, ordenó a la CONSEJERÍA DE SALUD DEL GOBIERNO DEL PRINCIPADO DE ASTURIAS, de acuerdo con lo dispuesto en el artículo 58.2 d) del RGPD, para que en el plazo de DIEZ DÍAS procediera a ordenar al responsable o encargados de los tratamientos, que las operaciones de tratamiento se ajustasen a las disposiciones del RGPD y la LOPDGDD. También requirió para que en el plazo de UN MES acreditase ante la AEPD el cumplimiento de:

- La adopción de todas las medidas necesarias para que la entidad investigada actúe de conformidad con los principios de «minimización de datos» y «limitación del plazo de conservación», del artículo 5.1 apartados c) y e) del RGPD.
- La adopción de las medidas necesarias para facilitar la información prevista en el artículo 13 del RGPD, debiendo facilitar a las personas que accedan al establecimiento correspondiente, con carácter previo a la recogida de los datos per-

sonales de los mismos, toda la información exigida en el citado precepto, para lo que se deberá tener en cuenta lo dispuesto en el artículo 7 del RGPD en relación con las condiciones para el consentimiento y artículo 6 de la LOPDGDD.

NOVENO: El acuerdo de inicio es debidamente notificado electrónicamente a la parte reclamada en fecha 22 de julio de 2021, a través del Servicio de Notificaciones Electrónicas y Dirección Electrónica Habilitada, según certificado que figura en el expediente.

DÉCIMO: Con fecha tanto de emisión como de notificación de 19 de noviembre de 2021, la instructora del procedimiento acuerda la apertura de un período de prueba por un plazo de 10 días hábiles, con el fin de que puedan llevarse a cabo las pruebas que, por su relevancia, a continuación, se declaran pertinentes:

1. Se dan por reproducidos a efectos probatorios todos los documentos obtenidos y generados por los Servicios de Inspección y el Informe de actuaciones previas que forman parte del procedimiento E/06499/2020.
2. Asimismo, se dan por reproducidas a efectos probatorios, las alegaciones al Acuerdo de iniciación del procedimiento sancionador referenciado presentadas por la CONSEJERÍA DE SALUD.

Frente a dicho acuerdo de apertura de período probatorio la parte reclamada no ha realizado manifestación ni ha aportado documento adicional alguno.

UNDÉCIMO: Transcurrido el plazo otorgado para la formulación de alegaciones al acuerdo de inicio del procedimiento, se ha constatado que no se ha recibido alegación alguna por la parte reclamada.

El artículo 64.2.f) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP) -disposición de la que se informó a la parte reclamada en el acuerdo de apertura del procedimiento- establece que si no se efectúan alegaciones en el plazo previsto sobre el contenido del acuerdo de iniciación, cuando éste contenga un pronunciamiento preciso acerca de la responsabilidad imputada, podrá ser considerado propuesta de resolución. En el presente caso, el acuerdo de inicio del expediente sancionador determinaba los hechos en los que se concretaba la imputación, la infracción del RGPD atribuida a la reclamada y la sanción que podría imponerse. Por ello, tomando en consideración que la parte reclamada no ha formulado alegaciones al acuerdo de inicio del expediente y en atención a lo establecido en el artículo 64.2.f) de la LPACAP, el citado acuerdo de inicio es considerado en el presente caso propuesta de resolución.

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

HECHOS PROBADOS

PRIMERO: Con fecha 11 de junio de 2020 entra en vigor el, ya derogado, Real Decreto-ley 21/2020, de 9 de junio, de medidas urgentes de prevención, contención y coordinación para hacer frente a la crisis sanitaria ocasionada por el COVID-19.

Los artículos 5, 23, 26 y 27, disponían:

Artículo 5. Planes y estrategias de actuación para afrontar emergencias sanitarias.

Con arreglo a lo previsto por el artículo 65 de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud, se procederá a la adopción de planes y estrategias de actuación para afrontar emergencias sanitarias, mediante actuaciones coordinadas en salud pública, atendiendo a los distintos niveles de riesgo de exposición y de transmisión comunitaria de la enfermedad COVID-19 para el desarrollo de las distintas actividades contempladas en este real decreto-ley.

Artículo 23. Obligación de información.

1. Se establece la obligación de facilitar a la autoridad de salud pública competente todos los datos necesarios para el seguimiento y la vigilancia epidemiológica del COVID-19 que le sean requeridos por esta, en el formato adecuado y de forma diligente, incluidos, en su caso, los datos necesarios para la identificación personal.

2. La obligación establecida en el apartado anterior es de aplicación al conjunto de las administraciones públicas, así como a cualquier centro, órgano o agencia dependiente de estas y a cualquier otra entidad pública o privada cuya actividad tenga implicaciones en la identificación, diagnóstico, seguimiento o manejo de los casos COVID-19.

En particular, será de aplicación a todos los centros, servicios y establecimientos sanitarios y servicios sociales, tanto del sector público como del privado, así como a los profesionales sanitarios que trabajan en ellos.

Artículo 26. Provisión de información esencial para la trazabilidad de contactos.

Los establecimientos, medios de transporte o cualquier otro lugar, centro o entidad pública o privada en los que las autoridades sanitarias identifiquen la necesidad de realizar trazabilidad de contactos, tendrán la obligación de facilitar a las autoridades sanitarias la información de la que dispongan o que les sea solicitada relativa a la identificación y datos de contacto de las personas potencialmente afectadas.

Artículo 27. Protección de datos de carácter personal.

“1. El tratamiento de la información de carácter personal que se realice como consecuencia del desarrollo y aplicación del presente real decreto-ley se hará de acuerdo a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y en lo establecido en los artículos ocho.1 y veintitrés de la Ley

14/1986, de 25 de abril, General de Sanidad. En particular, las obligaciones de información a los interesados relativas a los datos obtenidos por los sujetos incluidos en el ámbito de aplicación del presente real decreto-ley se ajustarán a lo dispuesto en el artículo 14 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, teniendo en cuenta las excepciones y obligaciones previstas en su apartado 5.

2. El tratamiento tendrá por finalidad el seguimiento y vigilancia epidemiológica del COVID-19 para prevenir y evitar situaciones excepcionales de especial gravedad, atendiendo a razones de interés público esencial en el ámbito específico de la salud pública, y para la protección de intereses vitales de los afectados y de otras personas físicas al amparo de lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. Los datos recabados serán utilizados exclusivamente con esta finalidad.

3. Los responsables del tratamiento serán las comunidades autónomas, las ciudades de Ceuta y Melilla y el Ministerio de Sanidad, en el ámbito de sus respectivas competencias, que garantizarán la aplicación de las medidas de seguridad preceptivas que resulten del correspondiente análisis de riesgos, teniendo en cuenta que los tratamientos afectan a categorías especiales de datos y que dichos tratamientos serán realizados por administraciones públicas obligadas al cumplimiento del Esquema Nacional de Seguridad.

4. El intercambio de datos con otros países se regirá por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, teniendo en cuenta la Decisión n.º 1082/2013/UE del Parlamento Europeo y del Consejo, de 22 de octubre de 2013, sobre las amenazas transfronterizas graves para la salud y el Reglamento Sanitario Internacional (2005) revisado, adoptado por la 58.ª Asamblea Mundial de la Salud celebrada en Ginebra el 23 de mayo de 2005.”

SEGUNDO: Con fecha 19 de junio de 2020 se publica en el Boletín Oficial del Principado de Asturias (BOPA) la “Resolución de 19 de junio de 2020, de la Consejería de Salud (BOPA 19.06.2020), por la que se establecen medidas urgentes de prevención, contención y coordinación necesarias para hacer frente a la crisis sanitaria ocasionada por la COVID-19 tras la expiración de la vigencia del estado de alarma, una vez superada la fase III del Plan para la transición hacia una nueva normalidad”.

TERCERO: Dicha resolución de 19 de junio de 2020 ha sufrido cinco modificaciones a través de las resoluciones enumeradas a continuación:

1. Resolución del Consejero de Salud de 14 de julio de 2020,
2. Resolución de fecha 23 de julio de 2020,
3. Resolución de fecha 29 de julio de 2020,
4. Resolución de fecha 18 de agosto de 2020,
5. Resolución de fecha 9 de octubre de 2020.

CUARTO: La Resolución de 29 de julio de 2020, de la Consejería de Salud, de tercera modificación de las medidas urgentes de prevención, contención y coordinación necesarias para hacer frente a la crisis sanitaria ocasionada por el COVID-19, recoge, en el apartado 3.4. de su Anexo, la obligación para determinados tipos de establecimientos

de contar con un registro de clientes y usuarios a disposición de la Dirección General de Salud Pública, con la finalidad de "facilitar el rastreo y seguimiento de contactos de casos positivos o sospechosos de Covid-19".

La propia resolución estipula que "la recogida de tales datos requerirá el consentimiento del interesado, sin perjuicio de condicionar el derecho de admisión por razones de salud pública en caso de no poder contar con el mismo". Asimismo, recomienda la adopción de sistemas de registro similares por parte de los titulares de los establecimientos de hostelería y restauración, discotecas y locales de ocio nocturno.

QUINTO: Dicho apartado no vuelve a ser modificado en ulteriores resoluciones, mas allá de ser reproducido en la Resolución de 18 de noviembre de 2020, de la Consejería de Salud, por la que se ordena la publicación del texto refundido de carácter informativo de las medidas urgentes de prevención, contención y coordinación necesarias para hacer frente a la crisis sanitaria ocasionada por la COVID-19 tras la expiración de la vigencia del estado de alarma.

SEXTO: De la documental que obra en el expediente y de todo lo anteriormente expuesto, quedan probados y acreditados los hechos imputados a la parte reclamada consistentes en:

- Exigir una cantidad de datos excesiva para la consecución del fin último perseguido con ellos, el cual sería poder localizar rápidamente a un eventual contacto, lo que supone un incumplimiento del artículo 5.1 c) del RGPD que preceptúa que los datos personales tratados sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»).
- La resolución fija un plazo de un mes desde el acceso, sin recoger expresamente los motivos para ese ámbito temporal, lo cual resulta contrario a lo establecido en el artículo 5.1 e) del RGPD que determina que los datos se conservarán *"durante no más tiempo del necesario para los fines del tratamiento"*. Asimismo, el Considerando 39 del RGPD dice: *"Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación."*
- No cumplir con lo establecido en los artículos 4.11) y 7 del RGPD puesto que el consentimiento prestado para la finalidad de facilitar el rastreo y seguimiento de contactos de casos positivos o sospechosos de Covid-19, no puede considerarse "libre" ya que, para ello, sería necesario que no se derivara ninguna consecuencia negativa, es decir, que no se condicionara la admisión al establecimiento, lo que, precisamente, sí se produce en el caso analizado.
- No haber acreditado el cumplimiento del deber de información al interesado establecido en el artículo 13 del RGPD.

FUNDAMENTOS DE DERECHO

PRIMERO: En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada Autoridad de Control, y según lo establecido en los artículos 47, 48, 64.2 y 68.1 de la LOPDGDD, la directora de la AEPD es competente para iniciar y resolver este procedimiento.

El artículo 63.2 de la LOPDGDD determina que: *“Los procedimientos tramitados por la Agencia Española de Protección de Datos se registrarán 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.”*

SEGUNDO: El artículo 4 del RGPD, bajo la rúbrica “Definiciones”, dispone lo siguiente:

“1) «datos personales»: 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;

2) «tratamiento»: 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”.

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

15) «datos relativos a la salud»: 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;

Así, un primer aspecto a aclarar es el relativo a la calificación jurídica de los datos objeto de tratamiento por parte de la investigada: fecha, hora del acceso y de salida, nombre y/o apellidos y número de teléfono de contacto de las personas que accedan al establecimiento correspondiente, que sin duda se encuadran en la categoría de “datos personales”.

A este respecto, es necesario puntualizar que los datos que se recogen, aunque estén relacionados con el control de la pandemia y su tratamiento tenga por objeto identificar posibles infectados, en un contexto de crisis de la COVID-19, en el que se publica el Real Decreto-ley 21/2020, de 9 de junio, de medidas urgentes de prevención, contención y coordinación para hacer frente a la crisis sanitaria ocasionada por el COVID-19, así como las medidas adoptadas, en el ámbito autonómico asturiano, por la Consejería de Salud, como autoridad sanitaria, de acuerdo con lo establecido en el artículo 5.b) de la Ley del Principado de Asturias 7/2019, de 29 de marzo, de Salud, no

son datos que en el RGPD estén catalogados como “datos relativos a la salud” (artículo 4.15 RGPD) o “categorías especiales de datos personales” (artículo 9.2 RGPD) en cuyo caso, serían aplicables las previsiones de este último artículo, circunstancia que no concurre en el presente caso.

TERCERO: Asimismo, consta que la CONSEJERÍA DE SALUD DEL PRINCIPADO DE ASTURIAS, con CIF S3333001J, con domicilio en C/Ciriaco Miguel Vigil, N.º 9, 33006, Oviedo (Asturias), es la responsable de los tratamientos de datos referidos en los antecedentes de hecho, toda vez que conforme a la definición del artículo 4.7 del RGPD es la que determina la finalidad de los tratamientos realizados: *“El registro se encontrará exclusivamente a disposición de la Dirección General de Salud Pública y tendrá como única finalidad facilitar el rastreo y seguimiento de contactos de casos positivos o sospechosos de Covid-19, sin perjuicio de que corresponda a los titulares de hoteles, albergues y otros alojamientos turísticos, peluquerías, barberías, centros de belleza, gabinetes de estética, salones de manicura, pedicura y depilación, saunas, balnearios, spas y gimnasios, la recogida de datos en virtud de lo establecido en la Resolución de 29 de julio de 2020.*

Cabe traer a colación la Estrategia de Detección Precoz, Vigilancia y Control de COVID-19, actualizada a 5 de julio de 2021, que respecto al “Estudio y manejo de contactos” dispone que tiene como objetivo realizar un diagnóstico temprano en los contactos estrechos que inicien síntomas y evitar la transmisión en periodo asintomático y paucisintomático. Concretamente, define “Contacto estrecho” como: *“De forma general, a nivel comunitario, se considerará contacto estrecho a cualquier persona que haya estado en el mismo lugar que un caso, a una distancia menor de 2 metros y durante un tiempo total acumulado de más de 15 minutos en 24 horas. En entornos en los que se pueda hacer una valoración del seguimiento de las medidas de prevención podrá realizarse una valoración individualizada por el servicio de prevención de riesgos laborales o el responsable que sea designado para ese fin. A la hora de establecer el riesgo, se tendrán en cuenta determinadas circunstancias como espacios en que haya riesgo elevado de generación de aerosoles u otras características personales o sociales del entorno en que se evalúe la posible transmisión”.*

En este contexto, la Tercera modificación de las medidas urgentes de prevención, contención y coordinación necesarias para hacer frente a la crisis sanitaria ocasionada por la COVID-19, tras la expiración de la vigencia del estado de alarma recogidas en la Resolución de 29 de julio de 2020, fue acordada en virtud del artículo 11.2 del Estatuto de Autonomía del Principado de Asturias; los artículos 1, 2 y 3 de la Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública; el artículo 26.1 de la Ley 14/1986, de 25 de abril, General de Sanidad; el artículo 54 de la Ley 33/2011, de 4 de octubre, General de Salud Pública, y de conformidad con el 5.b) de la Ley del Principado de Asturias 7/2019, de 29 de marzo, de Salud, que atribuye a la Consejería competente en materia de sanidad el ejercicio, como autoridad sanitaria, de las competencias en materias de intervención pública, inspectoras y sancionadoras.

CUARTO: El siguiente de los aspectos a analizar, por lo tanto, será la base jurídica de este tratamiento, puesto que el RGPD contempla diferentes supuestos que pueden dar lugar al tratamiento de datos de carácter personal.

En concreto, de acuerdo con el artículo 6.1 - "Licitud del tratamiento"-, del RGPD:

"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, 4.5.2016 L 119/36 Diario Oficial de la Unión Europea ES 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.”

De hecho, el considerando (46) del RGPD ya reconoce que, en situaciones excepcionales, como una epidemia, la base jurídica de los tratamientos puede ser múltiple, basada tanto en el interés público, como en el interés vital del interesado u otra persona física.

(46) El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente. 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.

Por lo tanto, como base jurídica para un tratamiento lícito de datos personales, sin perjuicio de que puedan existir otras bases, -como por ejemplo el cumplimiento de una obligación legal, artículo 6.1.c), el RGPD reconoce explícitamente las dos citadas: misión realizada en interés público (artículo 6.1.e) o intereses vitales del interesado u otras personas físicas (artículo 6.1.d).

En relación con la base jurídica de los tratamientos de datos personales derivados de la imposición de la medida, la investigada en su respuesta a los requerimientos indica que:

“La base de legitimación se ha entendido que viene determinada por el artículo 9.2.i) del Reglamento (UE) 2016/6753 (el tratamiento es necesario por razones de interés público en el ámbito de la salud pública), con apoyo legal interno en la Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública, y más específicamente en su artículo 3 cuando dispone que “Con el fin de controlar las enfermedades transmisibles, la autoridad sanitaria, además de realizar las acciones preventivas generales, podrá adoptar las medidas oportunas para el control de los enfermos, de las personas que estén o hayan estado en contacto con los mismos y del medio ambiente inmediato, así como las que se consideren necesarias en caso de riesgo de carácter transmisible”.

Ya señalamos en el Fundamento de Derecho Segundo, que los datos personales objeto de tratamiento no se enmarcan en el artículo 9 del RGPD, sino que se catalogan como “Datos personales” conforme a la definición prevista en el artículo 4.1 del RGPD. Por otra parte, en la Resolución de 29 de julio de 2020, consta que: *“La recogida de tales datos requerirá el consentimiento del interesado, sin perjuicio de condicionar el derecho de admisión por razones de salud pública en caso de no poder contar con el mismo.”*

Destacado, por lo tanto, el carácter voluntario del registro de clientes y descartado el tratamiento de una categoría especial de dato personal, se infiere que la base de licitud en la que se ampara la investigada es la prevista en el artículo 6.1.a) del RGPD, relativa al consentimiento dado por los afectados para el tratamiento de sus datos personales para este fin en concreto.

El artículo 4, apartado 11, del RGPD define el “consentimiento del interesado” como: *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;*

El artículo 7 del RGPD, bajo el epígrafe “Condiciones para el consentimiento” dispone lo siguiente:

- 1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.*
- 2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.*
- 3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.*
- 4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.*

Asimismo, el considerando 32 del RGPD, dispone: *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. (...)*

Por su parte, el considerando 42 del RGPD, dispone: (...) *El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno.*

Y añade el considerando 43 del RGPD: *Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibrio claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular. Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aun cuando este no sea necesario para dicho cumplimiento.*

Por último, el artículo 6 de la LOPDGDD bajo la rúbrica “Tratamiento basado en el consentimiento del afectado” dispone:

1. *De conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.*
2. *Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas.*
3. *No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual.*

De lo anteriormente expuesto se deduce que, para poder apreciar un consentimiento libre, sería necesario que no se derivara ninguna consecuencia negativa, es decir, que no se condicionara la admisión al establecimiento, lo que -precisamente-, sí se produce en el caso analizado.

En este sentido, el apartado 3.4 de la Resolución de 29 de julio de 2020, dispone:

“La recogida de tales datos requerirá el consentimiento del interesado, sin perjuicio de condicionar el derecho de admisión por razones de salud pública en caso de no poder contar con el mismo.”

Con lo hasta aquí expuesto, cabe concluir que el consentimiento prestado para la finalidad de facilitar el rastreo y seguimiento de contactos de casos positivos o sospechosos de Covid-19, no es conforme a lo establecido en el artículo 4.11) y 7 del RGPD. Y

ello es así, porque no puede considerarse “libre”. En este sentido, las Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, adoptadas el 4 de mayo de 2020 por el Comité Europeo de Protección de Datos, indican que: *El término «libre» implica elección y control reales por parte de los interesados. Como norma general, el RGPD establece que, si el sujeto no es realmente libre para elegir, se siente obligado a dar su consentimiento o sufrirá consecuencias negativas si no lo da, entonces el consentimiento no puede considerarse válido. La ausencia de tales requisitos determina que el mismo no sea válido de modo que los tratamientos basados en él carecen de legitimación contraviniéndose así lo previsto en el artículo 6 del RGPD.*

Los citados hechos podrían suponer una posible vulneración del artículo 7 del RGPD y 6 de la LOPDGDD.

QUINTO: Asimismo, los tratamientos de datos personales en situaciones de emergencia sanitaria, siguen siendo tratados de conformidad con la normativa de protección de datos personales (RGPD y LOPDGDD), por lo que se aplican todos sus principios, contenidos en el artículo 5 del RGPD, y entre ellos el de tratamiento de los datos personales con licitud, lealtad y transparencia, de limitación de la finalidad (en este caso, facilitar el rastreo y seguimiento de contactos de casos positivos o sospechosos de COVID-19), principio de limitación del plazo de conservación, y por supuesto, y hay que hacer especial hincapié en ello, el principio de minimización de datos. Sobre este último aspecto hay que hacer referencia expresa a que los datos tratados habrán de ser exclusivamente los limitados a los necesarios para la finalidad pretendida, sin que se pueda extender dicho tratamiento a cualesquiera otros datos personales no estrictamente necesarios para dicha finalidad, sin que pueda confundirse conveniencia con necesidad, porque el derecho fundamental a la protección de datos sigue aplicándose con normalidad, sin perjuicio de que, como se ha dicho, la propia normativa de protección de datos personales establece que en situaciones de emergencia, para la protección de intereses esenciales de salud pública y/o vitales de las personas físicas, podrán tratarse los datos de salud necesarios para evitar la propagación de la enfermedad que ha causado la emergencia sanitaria.

En suma, la mera habilitación del ordenamiento para llevar a cabo el tratamiento de datos no implica permisividad absoluta, este debe adecuarse a los principios y resto de contenido previsto en el RGPD y en la LOPDGDD.

El artículo 5 RGPD, referido a los “Principios relativos al tratamiento” dispone:

1. Los datos personales serán:

- a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);*
- b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; (...);*
- c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);*
- d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);*

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

Pues bien, los principios de licitud, lealtad y transparencia se aplican a todo tipo de tratamiento de datos personales.

La licitud requiere que se cumpla al menos una de las condiciones del artículo 6 del RGPD, que tal y como se ha expuesto en el Fundamento de Derecho anterior, la investigada lo fundamenta erróneamente en el artículo 9.2.i) del RGPD, y sobre la base del consentimiento, que deberá incluir una serie de elementos en la manifestación de voluntad de la persona interesada para el tratamiento de sus datos personales (artículo 4, apartado 11, artículo 7 y considerandos 32, 42 y 43, del RGPD y artículo 6 de la LOPDGDD).

En cuanto a la transparencia, este principio establece la obligación de que el responsable del tratamiento adopte las medidas que sean apropiadas para mantener a los interesados —que pueden ser usuarios o clientes— informados acerca de cómo se utilizan sus datos.

El artículo 12.1 del RGPD dispone:

“El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.”

Por su parte, el artículo 13 del RGPD, precepto en el que se determina la información que debe facilitarse al interesado en el momento de la recogida de sus datos, dispone:

“1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

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 y la base jurídica del tratamiento;*
- d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;*
- 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 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 estas o al hecho de que se hayan prestado.*

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

- a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;*
- b) 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, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;*
- c) 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 basado en el consentimiento previo a su retirada;*
- d) el derecho a presentar una reclamación ante una autoridad de control;*
- e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;*
- f) 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. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior,

información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4.Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.”

En este sentido, la investigada tampoco ha facilitado información respecto a los “Medios utilizados para el cumplimiento del deber de información al interesado”, que le fue solicitada en el primero de los requerimientos practicados.

El artículo 5 del RGPD exige, además, que los datos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»). Los datos que facilitan las personas a la hora de acceder a hoteles, albergues y otros alojamientos turísticos, peluquerías, barberías, centros de belleza, gabinetes de estética, salones de manicura, pedicura y depilación, saunas, balnearios, spas y gimnasios, son: fecha, hora del acceso y de salida, nombre y/o apellidos y número de teléfono de contacto.

Si lo que se pretende es poder localizar rápidamente a un eventual contacto, podría ser suficiente con obtener un número de teléfono, junto con los datos del día y la hora de asistencia al lugar. Este criterio, junto con el de la anonimización de los titulares del dispositivo, ha sido el asumido por el Comité Europeo de Protección de Datos en las Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID-19; criterio que puede extrapolarse a esta situación con las adaptaciones pertinentes.

En consecuencia, no sería necesario solicitar, además, el nombre y los apellidos, que serían innecesarios para la finalidad de rastreo y seguimiento a los posibles contactos.

Por último, el apartado 3.4 de la Resolución de 29 de julio de 2020, dispone: “Los datos deberán conservarse en el registro únicamente durante un plazo de un mes desde el acceso, transcurrido el cual deberá procederse a su supresión.”

La fijación del plazo de conservación no puede ser arbitraria en ningún caso, ya hemos visto que el artículo 5 del RGPD dispone que se conservarán “*durante no más tiempo del necesario para los fines del tratamiento*”. Asimismo, el Considerando 39 del RGPD dice: “*Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación.*”

La resolución fija un plazo de un mes desde el acceso, pero no explica el motivo de hacerlo de ese modo.

Por tanto, la Resolución de 29 de julio de 2020, pese a que indica en el punto 3 del apartado 3.4, que: “*Tanto el registro como el tratamiento de los datos contenidos en el mismo se regirá en todo caso por lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)*”, resulta que no lo hace al no haber motivado debidamente la adecuación y pertinencia de los datos recabados y la necesidad de conservación de dichos datos por el tiempo establecido.

Con lo hasta aquí expuesto, cabe señalar, que la investigada, además, ha incurrido en una vulneración de los principios y garantías relativos al tratamiento previstos en el artículo 5 del RGPD.

SEXTO: De conformidad con las evidencias de las que se dispone se considera que los hechos expuestos vulneran lo dispuesto en los artículos: 5.1.c), 5.1.e), 7 y 13 del RGPD, con el alcance expresado en los Fundamentos de Derecho anteriores, lo que podría suponer la comisión de las infracciones tipificadas en el artículo 83 apartado 5.a) y b) del RGPD que bajo la rúbrica “*Condiciones generales para la imposición de multas administrativas*” dispone que:

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

- a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;*
- b) los derechos de los interesados a tenor de los artículos 12 a 22.”*

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 72 de la LOPDGDD indica:

Artículo 72. Infracciones consideradas muy graves.

“1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

- a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679.*
- c) El incumplimiento de los requisitos exigidos por el artículo 7 del Reglamento (UE) 2016/679 para la validez del consentimiento. (...)*
- 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. (...)*

SÉPTIMO: No obstante, la LOPDGDD en su artículo 77, bajo el epígrafe “Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento”, establece lo siguiente:

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

- a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.*
- b) Los órganos jurisdiccionales.*

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

d) *Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.*

e) *Las autoridades administrativas independientes.*

f) *El Banco de España.*

g) *Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.*

h) *Las fundaciones del sector público.*

i) *Las Universidades Públicas.*

j) *Los consorcios.*

k) *Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.*

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación. Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

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

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

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento

que hubiera cometido la infracción. Cuando la competencia corresponda a una autoridad autonómica de protección de datos se estará, en cuanto a la publicidad de estas resoluciones, a lo que disponga su normativa específica”.

En resumen, la LOPDGDD no faculta a imponer multas administrativas, sino un mero apercibimiento, es decir, sin efecto económico alguno. No obstante, sí establece la posibilidad de que se puedan adoptar las medidas necesarias para que cese la conducta o se corrijan los defectos correspondientes.

OCTAVO: El RGPD se refiere en el artículo 58.2 a los poderes correctivos de la autoridad de control e indica que dispondrá de los siguientes:

- a) dirigir a todo responsable o encargado del tratamiento una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el presente Reglamento;*
- b) dirigir a todo responsable o encargado del tratamiento un apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;*
- c) ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado en virtud del presente Reglamento;*
- d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado;*
- e) ordenar al responsable del tratamiento que comunique al interesado las violaciones de la seguridad de los datos personales;*
- f) imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición;*
- g) ordenar la rectificación o supresión de datos personales o la limitación de tratamiento con arreglo a los artículos 16, 17 y 18 y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales con arreglo a al artículo 17, apartado 2, y al artículo 19;*
- h) retirar una certificación u ordenar al organismo de certificación que retire una certificación emitida con arreglo a los artículos 42 y 43, u ordenar al organismo de certificación que no se emita una certificación si no se cumplen o dejan de cumplirse los requisitos para la certificación;*
- i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular; j) ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.*

Todas estas medidas incluidas en este precepto pueden dictarse en lugar o además de las sanciones a las que se refiere el artículo 83 del RGPD, 76 y 77 de la LOPDGDD.

II

En el texto de la resolución se establecen cuáles han sido las infracciones cometidas y los hechos que han dado lugar a la 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.

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

PRIMERO: IMPONER a CONSEJERÍA DE SALUD DEL GOBIERNO DEL PRINCIPADO DE ASTURIAS, con CIF S3333001J, por una infracción de lo dispuesto en los artículos 5.1.c), 5.1.e), 7 y 13 del RGPD, tipificada en el Artículo 83.5 del RGPD, una sanción de apercibimiento.

SEGUNDO: REQUERIR a la CONSEJERÍA DE SALUD DEL GOBIERNO DEL PRINCIPADO DE ASTURIAS, para que en el plazo de UN MES acredite ante este organismo el cumplimiento de:

- La adopción de todas las medidas necesarias para que la entidad investigada actúe de conformidad con los principios de «minimización de datos» y «limitación del plazo de conservación», del artículo 5.1 apartados c) y e) del RGPD.
- La adopción de las medidas necesarias para facilitar la información prevista en el artículo 13 del RGPD, debiendo facilitar a las personas que accedan al establecimiento correspondiente, con carácter previo a la recogida de los datos personales de los mismos, toda la información exigida en el citado precepto, para lo que se deberá tener en cuenta lo dispuesto en el artículo 7 del RGPD en relación con las condiciones para el consentimiento y en el artículo 6 de la LOPDGDD.

TERCERO: NOTIFICAR la presente resolución a CONSEJERÍA DE SALUD.

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

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [<https://sedeagpd.gob.es/sede-electronica-web/>], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-150222

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