

- **Procedimiento N°: E/03346/2020**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha de 30 de marzo de 2020 la Directora de la Agencia Española de Protección de Datos acuerda iniciar las presentes actuaciones de investigación al haber tenido conocimiento del desarrollo y puesta en marcha de varias webs/apps en relación al COVID-19 con tratamientos de datos personales, con el fin de determinar una posible vulneración de la normativa de protección de datos.

SEGUNDO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos, teniendo conocimiento de los siguientes extremos:

El día 28/03/2020 se publicó en el BOE la Orden SND/297/2020, de 27 de marzo por la que se encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial (en adelante SEDIA), del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de una aplicación informática para el apoyo en la gestión sanitaria ocasionada por el COVID-19, el desarrollo de un asistente conversacional/chatbot para proporcionar información oficial ante las preguntas de la ciudadanía y un estudio de la movilidad de las personas en los días previos y durante el confinamiento.

1. Sobre la APP “ASISTENCIACOVID19”.

De las actuaciones realizadas en relación con el examen del cumplimiento de los principios de protección de datos recogidos en el RGPD, de las tipologías de datos tratados y de su período de conservación, de las finalidades concretas y de las bases jurídicas del tratamiento de datos, del convenio celebrado con Telefónica para el desarrollo de la aplicación, de la política de privacidad de la aplicación y la evaluación de impacto sobre la protección de datos, han resultado los siguientes hechos:

- Responsable y finalidad del tratamiento.

La mencionada Orden SND/297/2020 resuelve encomendar a la SEDIA el desarrollo urgente y operación de una aplicación informática para el apoyo en la gestión de la crisis sanitaria ocasionada por el COVID-19. Se dispone que dicha aplicación permitirá, al menos:

- realizar al usuario la autoevaluación en base a los síntomas médicos que comunique, acerca de la probabilidad de que esté infectado por el COVID-19,
- ofrecer información al usuario sobre el COVID-19 y

- proporcionar al usuario consejos prácticos y recomendaciones de acciones a seguir según la evaluación.

En la Orden se señala que *“el responsable del tratamiento será el Ministerio de Sanidad y el encargado del tratamiento y titular de la aplicación será la Secretaría General de Administración Digital. El Ministerio de Sanidad, como responsable del tratamiento, autoriza a la Secretaría General de Administración Digital a recurrir a otros encargados en la ejecución de lo previsto en este apartado”*.

La Secretaria General de Administración Digital (en adelante SGAD) depende de la SEDIA según el Organigrama publicado en la web de Ministerio de Asuntos Económicos y Transformación Digital. De acuerdo con lo previsto en el artículo 9.1 del Real Decreto 403/2020, de 25 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Asuntos Económicos y Transformación Digital, la SGAD es el órgano directivo bajo la autoridad de la persona titular de la SEDIA al que corresponde la dirección, coordinación y ejecución de las competencias atribuidas al Departamento en materia de transformación digital de la Administración.

A los requerimientos de información de la Subdirección de Inspección, los representantes de la SEDIA han manifestado que:

“En cumplimiento de lo establecido en la Orden SND/297/2020, de 27 de marzo, por la que se encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de diversas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID19, la SEDIA ha procedido al desarrollo urgente y operación de una aplicación informática para el apoyo en la gestión de la crisis sanitaria ocasionada por el COVID19.

La citada aplicación permite realizar la autoevaluación del usuario con base en los síntomas médicos que comunique acerca de la probabilidad de que esté infectado por el COVID-19, con el objetivo de descongestionar las líneas de atención telefónica, ofrecer información oficial al usuario sobre el COVID-19 y proporcionarle consejos prácticos y recomendaciones de acciones a seguir según la evaluación.

Es importante destacar que la aplicación no realiza rastreo de dispositivos móviles, sino que recaba datos personales y sanitarios para el correcto autodiagnóstico, así como datos de geolocalización vía GPS, siempre bajo autorización y en el momento de realizar la autoevaluación, para verificar la comunidad autónoma en la que se encuentra la persona.

Los únicos tratamientos que se realizan son los contenidos en la política de privacidad, con fines estrictamente de interés público en el ámbito de la salud pública, y ante la situación de emergencia sanitaria decretada, a fin de proteger y salvaguardar un interés esencial para la vida de las personas, de acuerdo con las bases legitimadoras establecidas en el Reglamento General de Protección de Datos. Además, los datos se podrán tratar, adoptando las medidas técnicas y organizativas necesarias, incluida su anonimización, con fines estadísticos, de investigación biomédica, científica o histórica, y para archivo en interés público.

El responsable del tratamiento es el Ministerio de Sanidad y el encargado del tratamiento y titular de la aplicación la Secretaría General de Administración Digital (SGAD). El Ministerio de Sanidad, como responsable del tratamiento, autoriza a la Secretaría General de Administración Digital a recurrir a otros encargados del tratamiento.

Se indica que, con objeto de garantizar el máximo respeto por la protección de los datos personales de los usuarios, se ha contado en todo momento con la participación de la propia AEPD a través de la solicitud y consideración sucesiva de los siguientes informes:

- *Informe AEPD 28/2020, de 2 de abril, sobre el convenio entre Telefónica y SGAD/SEDIA para la operación de la app, la política de privacidad y las condiciones de uso*
- *Informes AEPD 30/2020, de 6 de abril, y 32/2020, de 7 de abril, sobre el convenio entre SGAD y las Comunidades Autónomas”.*

Adjunta diversos documentos tales como la Evaluación de Impacto en Protección de Datos (PIA) TRATAMIENTO: "AsistenciaCovid19" de Telefónica Digital España, S.A.U., Política de privacidad de la aplicación "ASISTENCIACOV19"; Protocolo de envío de datos a Comunidades Autónomas; Análisis de riesgos de la aplicación COVID19, entre otros.

-Política de privacidad de la aplicación. La política de privacidad contiene entre otros aspectos la siguiente información:

-El responsable del tratamiento: señalando que es el Ministerio de Sanidad, de acuerdo con lo establecido en el punto primero, apartado 1, párrafo cuarto, de la Orden SND/297/2020, de 27 de marzo.

-El Delegado de Protección de Datos: delegadoprotecciondatos@mscbs.es. – Dirección: Paseo del Prado, 18-20, 28014 Madrid.

-Las categorías de datos tratados en los siguientes términos:

- Nombre y apellidos.
- Número de teléfono móvil, para que te podamos enviar notificaciones SMS.
- DNI/NIE para posterior cruce con la tarjeta sanitaria, a los efectos de que las autoridades sanitarias puedan integrar y comparar la información de pacientes con posibles síntomas con los sistemas públicos de gestión sanitaria existentes y hacer un seguimiento y atención personalizada.
- Dirección completa y código postal.
- Fecha de nacimiento, con objeto de poder establecer el grupo de población en el que te encuentras y ponderar los síntomas (el rango de edad puede determinar si se trata de un grupo de riesgo).
- Geolocalización (esto es, la localización vía GPS de tu teléfono móvil), opcional para saber dónde te encuentras y poder ofrecerte las mejores medidas preventivas y de evaluación en cada momento. La geolocalización solo se utilizará a la hora de registrarte y realizar tus autoevaluaciones, para poder conocer en qué Comunidad Autónoma te encuentras y poder conectarte con el sistema de atención sanitaria que te corresponda. No se rastrea tu localización para finalidades distintas de las señaladas.
- Género (opcional).

- Datos de salud relacionados con los síntomas que estas experimentando. En concreto, con motivo del uso de la aplicación podremos recabar información sobre ti relacionada con patologías previas, así como la sensación de falta de aire, fiebre de +37,5º C, tos seca, si has estado en contacto con algún paciente positivo confirmado, si tienes mucosidad en la nariz, dolor muscular y/o malestar general.
- Se informa asimismo de que “Toda la información se recogerá con fines estrictamente de interés público en el ámbito de la salud pública, y ante la situación de emergencia sanitaria decretada, a fin de proteger y salvaguardar un interés esencial para la vida de las personas, en los términos descritos en esta política de privacidad.” Enumera a continuación la legislación aplicable
 - Reglamento (UE) 2016/679, 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)
 - Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
 - Ley 14/1986, de 25 de abril, General de Sanidad.
 - Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública.
 - Ley 33/2011, de 4 de octubre, General de Salud Pública.
 - Real Decreto 463/2020 de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitarias ocasionada por el COVID-19 que atribuye al Ministro de Sanidad la necesaria competencia en todo el territorio nacional.
 - Orden ministerial SND/297/2020, de 27 de marzo, por la que se encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de nuevas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19.
- La política de privacidad de la aplicación, señala en su apartado 4, bajo el título ¿Para qué y por qué utilizamos tus datos?, los siguientes fines:

“El objetivo de la aplicación es reducir el volumen de llamadas al número de emergencias sanitarias que trata las dudas sobre la enfermedad infecciosa COVID-19 (de la familia de infecciones del Coronavirus), informar a la población, permitir un triaje o autoevaluación inicial de posibles casos y un seguimiento posterior, y aliviar la carga de los Servicios de Emergencia de las distintas Administraciones Públicas con competencia en materia de salud.

La información y datos recogidos a través de la aplicación serán tratados con fines estrictamente de interés público en el ámbito de la salud pública, ante la actual situación de emergencia sanitaria como consecuencia de la pandemia del COVID-19 y la necesidad de su control y propagación, así como para garantizar intereses vitales tuyos o de terceros, de conformidad con la normativa de protección de datos vigente.

A tal efecto, utilizamos tus datos para prestarte el servicio de «ASISTENCIACOV19» y para que puedas hacer uso de sus funcionalidades

de acuerdo con sus condiciones de uso (<https://asistencia.covid19.gob.es/condiciones-de-uso>). Esto implica:

- Ofrecerte información sobre el COVID-19, incluyendo el envío de notificaciones a través de la aplicación en relación con las mejores medidas preventivas y de evaluación en cada momento.
- Realizar tu autoevaluación en base a los síntomas médicos que nos comuniqués acerca de la probabilidad de que estés infectado por el virus COVID-19 o «coronavirus».
- Proporcionarte consejos prácticos y recomendaciones de acciones a seguir según evaluación. – Si es necesario, selección de cita para posible prueba, según diagnóstico.
- Recepción de resultados de la prueba y recomendaciones de actuación para la cuarentana o autocuarentena o cita con centro médico.
- Autoevaluación continua diaria: Monitorización de la temperatura y parámetros básicos, cada doce horas desde que se inicie la aplicación, incluyendo un recordatorio en forma de alarma para que lo vayas introduciendo.
- Conocer tu localización GPS en el momento de la autoevaluación exclusivamente para poder conocer en qué Comunidad Autónoma te encuentras y en su caso conectarte con los servicios de salud correspondientes. No se rastrea tu localización para finalidades distintas de las señaladas. Se podrá utilizar la dirección del domicilio proporcionada en el registro, con la finalidad de prestación de servicios sanitarios si fuera necesario. En cualquier caso, la aplicación no realiza geofencing para determinar si el usuario se encuentra en su domicilio.

Adicionalmente, conforme a lo establecido en la normativa aplicable, podremos tratar tus datos para las siguientes finalidades no directamente relacionadas con las funcionalidades de la «ASISTENCIACovid19», adoptando las medidas técnicas y organizativas necesarias, en particular, para garantizar el respeto al principio de minimización de datos personales, incluyendo su anonimización:

- Para finalidades estadísticas;
- Para investigación biomédica, científica o histórica; y
- Para archivo en interés público.

Estas finalidades permitirán hacer tanto un análisis anonimizado descriptivo de la situación, que permita conocer qué y por qué está ocurriendo (p.ej. las dinámicas actuales de la sintomatología en la población), así como un análisis anonimizado predictivo sobre la evolución de esta (p.ej. cómo podrían evolucionar dichas dinámicas en el futuro).

Además, estas finalidades son especialmente relevantes, no solo para conocer y predecir la situación de emergencia sanitaria actual, sino también para futuras investigaciones médicas, científicas e históricas que sean precisas llevar a cabo, entre otros objetivos, para prevenir y detectar situaciones similares que puedan tener lugar en el futuro.”

-Plazo de conservación de los datos.

Se señala que “Existen diversos motivos que nos legitiman para conservar tus datos, aunque solo los conservaremos y trataremos mientras sean necesarios para las finalidades indicadas en el punto 4 anterior, por lo que solo los conservaremos durante el tiempo que perdure la crisis sanitaria, con la excepción de las finalidades estadísticas, de investigación o archivo en interés público, cuyo plazo de conservación será de un máximo de dos años, todo ello de conformidad con los principios legales de tratamiento de datos, en particular el de minimización de datos. En el momento en que finalice el periodo de conservación de tus datos, estos serán anonimizados y/o bloqueados conforme a los requisitos establecidos en la normativa aplicable.

-Destinatarios de los datos.

Se aporta la siguiente información “Además del Responsable, tienen acceso a tus datos personales los profesionales sanitarios y las autoridades con las que colaboramos y nos relacionamos para el cumplimiento de las finalidades arriba indicadas. El acceso a tus datos, que proporcionamos a estos terceros, es siempre para finalidades lícitas y solo durante el periodo de tiempo estrictamente necesario para ello. Entre otros, esto implica dar acceso a tus datos a:

- Los profesionales sanitarios para que se pongan en contacto directamente contigo en caso de que, del resultado de la autoevaluación realizada a través de la aplicación, se determine que necesitas atención médica ante la posibilidad de estar infectado por el coronavirus.
- Las autoridades competentes de las Comunidades Autónomas en materia de sanidad (los datos de salud podrán formar parte de tu historia clínica) y otras autoridades nacionales y/o internacionales (p.ej. órganos judiciales), con las que necesitemos compartir tu información.”

-Se informa también sobre cuáles son los derechos de los interesados de la siguiente forma: “¿Cuáles son tus derechos y cómo puedes controlar tus datos?”

La normativa te otorga una serie de derechos en relación con los datos e información que tratamos sobre ti. Concretamente, los derechos de acceso, rectificación, supresión, limitación y oposición.

Puedes consultar el alcance y detalle completo de estos derechos en la página web de la Agencia Española de Protección de Datos (AEPD) aquí.

Con carácter general, podrás ejercitar todos estos derechos (en cualquier momento y de forma gratuita). Puedes dirigirte al Responsable de Tratamiento por vía electrónica, a través de este formulario, o presencialmente a través de la red de oficinas de asistencia en materia de registros utilizando este modelo de solicitud (versión editable e imprimible).

Aparte de todo lo anterior, tenemos obligación de indicarte que te asiste en todo momento el derecho para presentar una reclamación ante Agencia Española de Protección de Datos.”

-Encargados y subencargados del tratamiento.

Las relaciones entre responsable y encargados o subencargados del tratamiento se encuentran desarrolladas en el *Convenio entre la Secretaría de Estado de*

Digitalización e Inteligencia Artificial y Telefónica Digital España, S.L.U., para la operación de la aplicación «ASISTENCIACOV19» en el contexto de la situación de crisis sanitaria ocasionada por el COVID-19, suscrito el 4 de abril de 2020 y publicado en el BOE el 5 de mayo de 2020. En este sentido señala en el número tercero de su cláusula primera que “A los efectos del presente Convenio, y de conformidad con lo dispuesto en la resolución primera apartado 1, párrafo cuarto, de la Orden del Ministro de Sanidad SND/ 297/2020, de 27 de marzo, por la que se encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de diversas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19, el Ministerio de Sanidad tendrá la consideración de Responsable del Tratamiento, la SGAD tendrá la consideración de Encargado del Tratamiento y Telefónica tendrá la consideración de Subencargado del Tratamiento.”

La cláusula cuarta de dicho convenio enumera las obligaciones del encargado y Subencargado del tratamiento

“A los efectos del encargo del tratamiento se cumplirán las disposiciones establecidas en el artículo 28.3 del RGPD, incluyendo:

1. El Encargado del Tratamiento informará lo antes posible al Responsable del Tratamiento si considera que, en su opinión o porque así se lo haya comunicado el Subencargado del Tratamiento, alguna de las instrucciones del Responsable del Tratamiento infringe el RGPD, la Ley Orgánica 3/2018, de 5 de diciembre o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros.

2. El Encargado y Subencargado del Tratamiento, en lo relativo al Tratamiento indicado, asumen las siguientes obligaciones:

a) Acceder y tratar a los datos de carácter personal responsabilidad del Responsable del Tratamiento únicamente cuando sea necesario para el buen desarrollo de los servicios objeto del convenio.

b) Utilizar los datos personales de forma reservada de acuerdo a las instrucciones proporcionadas por el Responsable del Tratamiento conforme a lo establecido en la normativa aplicable.

c) En caso de que el tratamiento incluya la recogida de datos personales en nombre y por cuenta del Responsable del Tratamiento, el Encargado del Tratamiento y el Subencargado del Tratamiento deberán seguir los procedimientos e instrucciones documentadas que, a estos efectos, reciban del Responsable del Tratamiento, especialmente en lo relativo al deber de información y, en su caso, la obtención del consentimiento de los afectados.

d) No destinar, aplicar o utilizar los datos de carácter personal responsabilidad del Responsable del Tratamiento a un fin distinto del indicado en el presente Convenio con o sin su autorización, o de cualquier otra forma que suponga un incumplimiento de las instrucciones documentadas del Responsable del Tratamiento.

e) Restringir el acceso a la información a sus empleados y subcontratados, salvo en la medida en que razonablemente puedan necesitarla para el cumplimiento de sus tareas acordadas.

f) Impedir la copia o revelación de esa información a terceros, salvo que goce de aprobación escrita de las partes y únicamente en términos de tal aprobación.

Asimismo, no divulgar ni comunicar sin la autorización del Responsable del Tratamiento la información facilitada o recibida como resultado de la firma del presente convenio.

g) En caso de estar obligado a ello por el artículo 30 del RGPD y 31 de la Ley Orgánica 3/2018, de 5 de diciembre, el Encargado del Tratamiento y el Subencargado del Tratamiento mantendrán un registro de todas las actividades de tratamiento efectuadas por cuenta del Responsable del Tratamiento, que contenga la información exigida por el artículo 30.2 del RGPD.

h) Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

i) Dar apoyo al Responsable del Tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos que en su caso deba realizar, cuando proceda, conforme a la normativa aplicable.

j) Dar apoyo al Responsable del Tratamiento en la realización de las consultas previas a la Autoridad de Control que en su caso deba de realizar, cuando proceda, conforme a la normativa aplicable.

k) Poner a disposición del Responsable del Tratamiento toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen al Responsable del Tratamiento u otro auditor autorizado por este.

l) Adoptar las medidas técnicas y organizativas apropiadas, según lo establecido en el artículo 32 del RGPD, en la disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre y en el Real Decreto 3/2010, de 8 de enero, de acuerdo con el correspondiente análisis de riesgos, que garanticen la seguridad de los datos de carácter personal responsabilidad del Responsable del Tratamiento y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.

m) Comunicar al Responsable del Tratamiento, con suficiente antelación, y en todo caso antes del plazo establecido en el RGPD, la existencia de una brecha de seguridad para que este lo comunique a la autoridad de control.

n) Designar un delegado de protección de datos y comunicar su identidad y datos de contacto al Responsable del Tratamiento, así como cumplir con todo lo dispuesto en los artículos 37, 38 y 39 del RGPD y 35 a 37 de la Ley Orgánica 3/2018, de 5 de diciembre.

Telefónica cuenta con un Delegado de Protección de Datos (DPO) designado, con el que se puede contactar a través de la siguiente dirección de correo electrónico DPO_telefonica@telefonica.com.

La SGAD cuenta con un Delegado de Protección de Datos (DPO) designado, que es el del Ministerio de Asuntos Económicos y Transformación Digital, con el que se puede contactar a través de la siguiente dirección de correo electrónico dpd@economia.gob.es.

o) Respetar todas las obligaciones que pudieran corresponderle como Encargado del Tratamiento o Subencargado del Tratamiento con arreglo al RGPD y la Ley Orgánica 3/2018, de 5 de diciembre, o de cualquier otra disposición o regulación

complementaria en materia de protección de datos que, en su caso, le fuera igualmente aplicable.

p) En caso de que el Encargado del Tratamiento deba transferir o permitir acceso a datos personales responsabilidad del Responsable del Tratamiento a un tercero en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al Responsable del Tratamiento de esa exigencia legal de manera previa, salvo que estuviese prohibido por razones de interés público.”

4. El Encargado del Tratamiento, el Subencargado del Tratamiento y, en su caso, sus subcontratistas ubicarán las actividades del Tratamiento dentro del territorio de la Unión Europea.

5. El acceso y el tratamiento de datos de carácter personal en el marco del Convenio se realiza con el único fin de permitir una adecuada colaboración en las actividades previstas en el Convenio la ejecución del Tratamiento, sin considerarse como una cesión o comunicación de dato”

La cláusula Sexta se refiere a las obligaciones de Telefónica:

“1. En virtud del presente Convenio, Telefónica asume las siguientes obligaciones:

a) La gestión operativa de la aplicación.

b) El alojamiento («hosting») de la aplicación.

c) La implementación y despliegue de la aplicación.

d) El tratamiento de los datos personales de los usuarios de la aplicación en su condición de Subencargado del Tratamiento, en los términos previstos en este Convenio y la normativa vigente sobre protección de datos personales.

e) La adopción de las medidas técnicas y organizativas apropiadas, de acuerdo con el correspondiente análisis de riesgos, para evitar la pérdida, alteración o acceso no autorizado de los datos manejados por la aplicación, según lo establecido en el artículo 32 del Reglamento (UE) 2016/679, en la disposición adicional primera de la Ley Orgánica 3/2018 y en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica.

f) El mantenimiento correctivo y la operación por el espacio máximo de un mes.

2. Tanto el almacenamiento como el resto de actividades del tratamiento de los datos, se ubicarán en el territorio de la Unión Europea, ya sean estos provistos y gestionados por Telefónica o por sus contratistas y colaboradores, y se alojarán en servidores y/o centros de proceso de datos de la propia Telefónica o de sus contratistas.

3. La SGAD encarga y autoriza expresamente a Telefónica y, en su caso, sus colaboradores, para la realización y ejecución de los cometidos descritos en el apartado uno de esta cláusula con las más amplias facultades, si bien con expreso sometimiento a los términos del presente Convenio.

4. En los procesos de alta, baja y modificación de los registros de usuarios, así como las interacciones e intercambios que se lleven a cabo con estos datos, Telefónica actuará exclusivamente en base a las definiciones de procesos y flujos de información que se le faciliten por la SGAD.

5. Telefónica aportará una valoración del riesgo de los tratamientos que realice la aplicación y una evaluación de impacto sobre la protección de datos con carácter

previo a la puesta en marcha de la aplicación por razón de su riesgo para los derechos y libertades de los usuarios.”

La cláusula novena hace referencia al ejercicio de derechos por los interesados ante el Encargado y Subencargado del Tratamiento estipulando que:

“1.El Encargado y Subencargado del Tratamiento deberán dar traslado al Responsable del Tratamiento de cualquier solicitud de ejercicio del derecho de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de los datos y a no ser objeto de decisiones individualizadas automatizadas, efectuada por un interesado del tratamiento cuyos datos hayan sido tratados por el Encargado o Subencargado con motivo del cumplimiento del objeto del presente Convenio, a fin de que el Responsable del Tratamiento la resuelva en los plazos establecidos por la normativa vigente.

El traslado de la solicitud al Responsable del Tratamiento deberá de hacerse con la mayor celeridad posible y, en ningún caso, más allá de tres (3) días hábiles siguientes al de la recepción de la solicitud por el Encargado o Subencargado del Tratamiento, acompañada de otras informaciones que puedan ser relevantes para resolver la solicitud.

2. El Encargado y Subencargado del Tratamiento deberán colaborar con el Responsable del Tratamiento ante cualquier instrucción que les traslade sobre el tratamiento relativa a los derechos de acceso, rectificación, supresión y oposición, de limitación del tratamiento, portabilidad de los datos y a no ser objeto de decisiones individualizadas automatizadas. La ejecución de la instrucción se llevará a cabo con a la mayor celeridad posible, y, siempre que sea factible, en el plazo máximo de tres (3) días hábiles a contar desde la recepción de la instrucción. El Encargado y, en su caso, el Subencargado comunicarán por escrito la recepción de la instrucción y la ejecución de la tarea encomendada una vez finalizada.”

La cláusula décima se refiere a las medidas de seguridad y violación de la seguridad con el siguiente contenido:

“ 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 que conozca y/o le sean informados efectivamente por el Responsable del Tratamiento el Encargado y Subencargado del Tratamiento aplicarán en función del análisis realizado conjuntamente con el Responsable del Tratamiento las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya:

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, así como la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

c) Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

d) *Un catálogo de medidas de seguridad según lo previsto en el Real Decreto 3/2010, de 8 de enero, y a luz del correspondiente análisis de riesgos.*

2. *Al evaluar la adecuación del nivel de seguridad, el Encargado y Subencargado tendrán en cuenta los riesgos que presente el tratamiento de datos detectados en el análisis realizado, 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. *El Encargado y el Subencargado del Tratamiento destinarán sus mejores esfuerzos para permitir y contribuir a la realización de auditorías de protección de datos, incluidas inspecciones, por parte del Responsable del Tratamiento o de otro auditor autorizado por el mismo.*

4. *En caso de modificación de la normativa vigente en materia de protección de datos o de otra normativa relacionada y que resultase aplicable al tratamiento objeto del presente Convenio, el Responsable del Tratamiento lo comunicará con la antelación debida al Encargado del Tratamiento, quien lo trasladará al Subencargado. Ambos destinarán sus mejores esfuerzos para implementar y mantener las mismas.*

5. *En caso de violación de la seguridad de los datos personales en los sistemas de información utilizados por el Encargado y el Subencargado del Tratamiento para la ejecución del tratamiento, estos deberán notificar al Responsable del Tratamiento sin dilación indebida desde que, en su caso, tengan conocimiento efectivo, las violaciones de la seguridad de los datos personales a su cargo de las que tengan conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia de la que dispongan conforme a lo dispuesto en el artículo 33.3 del RGPD.*

En tal caso, corresponderá al Responsable del Tratamiento comunicar aquellas violaciones de seguridad de los datos a la autoridad de protección de datos competente y/o, en su caso, a los interesados conforme a lo establecido en la normativa vigente, manteniendo informado al respecto al Encargado del Tratamiento o al Subencargado antes de realizar dicha comunicación.”

La cláusula decimosexta, relativa a la duración, resolución y extinción del convenio, estipula en su número 6 que “Una vez extinguido o resuelto el Convenio, ni Telefónica ni ninguna de las empresas que subcontrate o colaboren en cualquier actividad relacionada con el objeto de este Convenio, podrán conservar en ningún caso copia de los datos manejados durante el periodo en el que haya estado encargada de su gestión y explotación.

Extinguido o resuelto el Convenio, Telefónica hará entrega en el formato que acuerde la Comisión de Seguimiento, de todos los datos de los usuarios de la aplicación que hayan sido objeto de tratamiento tanto por Telefónica como por las empresas que subcontrate o colaboren en cualquier actividad relacionada con el objeto de este Convenio.

En ese acto, Telefónica entregará acreditación documental de la destrucción fehaciente de todos datos manejados para la colaboración en las actividades recogidas en el presente Convenio”

La cláusula decimoctava se refiere al destino de los datos personales al finalizar la relación acordada en el Convenio, determinando que “Una vez terminada y/o resuelta la relación acordada en el Convenio entre el Encargado del Tratamiento y el

Subencargado del Tratamiento, se estará a lo dispuesto en la cláusula decimosexta del presente Convenio en sus apartados 5 y 6.”

La cláusula decimoséptima relativa al régimen de protección de datos, seguridad y confidencialidad, estipula que:

“1. El régimen de protección de datos de carácter personal en las actuaciones que se desarrollen en ejecución del presente Convenio es el previsto en el RGPD, en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y demás normativa de aplicación en materia de protección de datos.

2. Las partes velarán por el cumplimiento del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica.

3. Toda la información facilitada por las partes y toda la información generada como consecuencia de la ejecución del presente Convenio, tendrá el tratamiento de confidencial, sin perjuicio de la información que sea de dominio público, no pudiendo ser divulgada o facilitada a terceros, ni utilizada para un fin distinto del previsto en este documento, de acuerdo con lo previsto en la normativa aplicable.

4. La obligación de confidencialidad para las partes se extenderá indefinidamente aunque el Convenio se hubiera extinguido. Todo ello sin perjuicio de la eventual autorización de las partes o en su caso, de que dicha información pasara a ser considerada como de dominio público.

5. Además del Responsable del Tratamiento, pueden tener acceso a los datos, entre otros, los profesionales sanitarios y las autoridades competentes necesarios para el cumplimiento de las finalidades de la aplicación, cada uno de ellos en el ejercicio de sus funciones o competencias en el cumplimiento de las obligaciones en materia sanitaria o de salud pública que les encomienda la normativa vigente:

a) Los profesionales sanitarios, para contactar directamente con el usuario en caso de que, del resultado de la autoevaluación realizada a través de la aplicación, se determine que necesita atención médica ante la posibilidad de estar infectado por el coronavirus.

b) Las autoridades competentes de las Comunidades Autónomas en materia de sanidad, INGESA, MUFACE, ISFAS y MUGEJU y otras autoridades nacionales y/o internacionales (por ejemplo, órganos judiciales), con las que sea necesario compartir los datos del usuario.

El acceso a los datos por estos terceros será siempre para finalidades lícitas relacionadas con el Convenio y solo durante el periodo de tiempo estrictamente necesario para ello.

El Responsable del Tratamiento garantizará el máximo nivel de protección en el acceso de estos terceros a los datos. A tal efecto podrá suscribir acuerdos de tratamiento de datos o establecer medidas de salvaguarda apropiadas que aseguren la confidencialidad y el tratamiento seguro de los datos.”

Como anexo al convenio figura un acuerdo de subencargo del tratamiento, cuya cláusula segunda prevé lo siguiente:

“Cláusula segunda. Subcontratación por parte de Telefónica.

1. El Responsable del Tratamiento autoriza a Telefónica, como Subencargado del Tratamiento, a subcontratar, ya sea total o parcialmente, la ejecución del tratamiento a los siguientes subcontratistas:

- a) CARTODB Inc. Sucursal en España, CIF W4007666C;
- b) Mendesaltaren, S.L., CIF B87818712; y
- c) Tritium Software, S.L., CIF B64685092.

2. Sin perjuicio de lo anterior, en caso de que Telefónica necesitara subcontratar todo o parte del tratamiento a otros subcontratistas, deberá de comunicarlo previamente y por escrito al Responsable del Tratamiento, con una antelación previa de cinco días naturales, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto.

3. La subcontratación podrá llevarse a cabo si el Responsable del Tratamiento, no manifiesta su oposición en el plazo establecido.

4. En este último caso, el subcontratista, que también tendrá la condición de Subencargado del Tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este acuerdo para Telefónica y las instrucciones documentadas que dicte el Responsable del Tratamiento a tal efecto. Corresponde a Telefónica exigir al subcontratista el cumplimiento de las mismas obligaciones asumidas por él a través del presente acuerdo.

5. Telefónica será responsable solidariamente junto con el subcontratista ante el Responsable del Tratamiento en lo referente al cumplimiento de las obligaciones como Subencargado del Tratamiento, ello de conformidad con la Estipulación sexta del Convenio.”

Transferencias internacionales

En el convenio consta expresamente (cláusula cuarta, número cuatro) que “El Encargado del Tratamiento, el Subencargado del Tratamiento y, en su caso, sus subcontratistas ubicarán las actividades del Tratamiento dentro del territorio de la Unión Europea.”

Asimismo, en el número segundo de la cláusula sexta se estipula que “Tanto el almacenamiento como el resto de actividades del tratamiento de los datos, se ubicarán en el territorio de la Unión Europea, ya sean estos provistos y gestionados por Telefónica o por sus contratistas y colaboradores, y se alojarán en servidores y/o centros de proceso de datos de la propia Telefónica o de sus contratistas.”

Análisis de Riesgos (AR). Evaluaciones de Impacto sobre Protección de Datos (EIPD) y protocolos de acceso de las Comunidades Autónomas

Tal y como se estipula en el punto quinto de la cláusula séptima del convenio al que se viene haciendo referencia, “TELEFÓNICA aportará una valoración del riesgo de los tratamientos que realice la aplicación y una Evaluación de Impacto sobre la Protección de Datos con carácter previo a la puesta en marcha de la aplicación por razón de su riesgo para los derechos y libertades de los usuarios.”

Consta entre la documentación aportada a solicitud de la Subdirección de inspección el análisis de riesgos y la Evaluación de impacto sobre Protección de Datos de la aplicación AsistenciaCovid19. Se ha aportado también el protocolo de acceso a los datos por parte de las Comunidades Autónomas.

A este respecto cabe señalar que en el análisis de riesgos realizado se utilizan varias metodologías, entre otras IRAM2, como base para realizar el BIA (Business Impact Assessment), ISO 27005/ISO 31000 para el modelo de gobierno de riesgo y MAGERIT para realizar el catálogo de activos y amenazas.

En lo que se refiere a la evaluación de impacto del tratamiento "AsistenciaCovid19" para la aplicación, el documento incluye una descripción previa del funcionamiento, de las categorías de datos personales tratados, estudio de la base legitimadora, los roles y responsabilidades de los intervinientes desde el punto de vista de protección de datos y un análisis de la necesidad y proporcionalidad del tratamiento. El apartado de gestión de los riesgos se basa en una metodología de análisis y gestión de los riesgos de privacidad mediante catálogo de potenciales escenarios de riesgos que implican un daño o perjuicio para las personas afectadas por el tratamiento de los datos.

Respecto a los protocolos de acceso a los datos por parte de las CCAA, se describen en el mismo el procedimiento de exportación de datos a las comunidades autónomas y los mecanismos para que los datos de una comunidad autónoma solamente sean accesibles para la misma, se describen también las medidas adoptadas para autenticar a las personas que tienen acceso a la base de datos y al establecimiento de logs de autenticación y administración para realizar un seguimiento de seguridad.

2. ASISTENTE CONVERSACIONAL (Chatbot)- HISPABOT-COVID19.

La Orden encomienda a la SEDIA, el desarrollo de un asistente conversacional o chatbot para ser utilizado vía Whatsapp y otras aplicaciones de mensajería instantánea, que proporcionará información oficial ante las preguntas de la ciudadanía.

En la Orden se cita que *"El responsable del tratamiento será el Ministerio de Sanidad y el encargado del tratamiento y titular del chatbot será la Secretaría de Estado de Digitalización e Inteligencia Artificial a través de la Subdirección General de Inteligencia Artificial y Tecnologías Habilitadoras Digitales."*

Los representantes de la SEDIA han manifestado lo siguiente:

"La Orden SND/297/2020 mencionada ut supra encomienda a la SEDIA el desarrollo de un asistente conversacional o chatbot, para ser utilizado vía Whatsapp y otras aplicaciones de mensajería instantánea, que proporcionará información oficial ante las preguntas de la ciudadanía de acuerdo con información oficial del Ministerio de Sanidad."

El responsable del tratamiento será el Ministerio de Sanidad y el encargado del tratamiento y titular del chatbot será la Secretaría de Estado de Digitalización e Inteligencia Artificial.

El servicio prestado por el asistente conversacional o chatbot es de carácter meramente informativo, para responder de forma automatizada a preguntas frecuentes relativas al nuevo coronavirus SARS-Cov-2 y enfermedad COVID-19. Sus respuestas no tienen la consideración de vinculantes a efectos legales. Las respuestas que ofrece el chatbot se han elaborado con las fuentes oficiales y confiables en un esfuerzo por proporcionar información que sea actualizada, veraz y completa. La utilización del chatbot no constituye en ningún caso un servicio de

diagnóstico médico, de atención de urgencias o de prescripción de tratamientos farmacológicos. Además, se advierte y pone en conocimiento del usuario, que su utilización no puede en ningún caso sustituir la consulta presencial personal frente a un profesional médico debidamente cualificado.

El objetivo del sistema Hispabot-Covid19 es responder a las preguntas de los ciudadanos. Para hacerlo, utiliza diferentes canales para recibir las preguntas, un motor de procesamiento de Lenguaje Natural para identificarlas y detectar la respuesta; y devolverla al usuario por el canal por el que hizo la pregunta.

1. *El sistema recibe la pregunta por web, Telegram o Whatsapp, y el único dato que obtiene del usuario es el texto que escribe. Es decir, la única información que se trata es la propia conversación.*

2. *El sistema no solicita ni necesita datos personales, lo que se indica claramente en el mensaje de bienvenida al usuario:*

“Este servicio solo aporta información oficial. Almacena de forma anónima tus consultas para ir mejorando las respuestas y aprender a resolver nuevas preguntas. En ningún caso se solicitará ni debes facilitar ningún dato de carácter personal. Puedes consultar la política de privacidad en: <https://www.covid19.gob.es/hispabot-covid19>”

3. *Las conversaciones con el asistente se recuperan del canal que elige el usuario (Web, Whatsapp o Telegram), y se ingresan en el motor de inferencia y entendimiento, y esa es la única información que se almacena.*

Por tanto, en relación con la tipología de datos personales que van a ser recabados, cabe señalar que el servicio no recopila ningún dato de carácter personal (ni de ubicación, ni de salud, ni de contacto, ni identificadores en línea). El servicio se presta de forma totalmente anónima y no requiere la identificación del usuario.

El chatbot únicamente utiliza el contenido de los mensajes de texto (es decir, el texto, ignorando los datos del emisor) que los usuarios envían al sistema, con los siguientes objetivos:

1. *Para que se detecten nuevas áreas de interés del ciudadano, a partir del análisis de las preguntas realizadas. Y poder trasladar estas inquietudes a los expertos, para que valoren su inclusión en la base de conocimiento si procede.*
2. *Para que se mejore el motor de inferencia heurística, de manera que se garantice que las respuestas del asistente son las adecuadas según la pregunta del ciudadano.*
3. *Para que aquellas consultas que no se consideren oportunas en el ámbito de Hispabot-Covid19 tengan en cualquier caso una respuesta apropiada.*

Adicionalmente, se podrían tratar las conversaciones para las siguientes finalidades:

- o *Para finalidades estadísticas.*
- o *Para investigación biomédica, científica o histórica.*
- o *Para archivo en interés público.*

Al no almacenar ni tratar datos personales de los usuarios, no se requieren protocolos de acceso a los mismos por las Comunidades Autónomas. Además, no se contempla que accedan a los registros de las conversaciones.

Por otro lado, el sistema no realiza decisiones automatizadas como las que se recogen en el artículo 22 del RGPD (decisiones basadas únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar).

En cuanto a otras operaciones relacionadas con el tratamiento de datos por parte de una inteligencia artificial:

- *Validación. El sistema necesita una validación para comprobar que el modelo de inferencia se ha realizado apropiadamente y se ha dado una respuesta correcta al ciudadano. Sin embargo, la validación se hace sobre mensajes de texto de una conversación, y no sobre datos personales.*
- *Despliegue. Aunque el asistente virtual se publica en diferentes canales de diferentes organismos, simplemente son componentes de “canal” porque el motor de inferencia es único.*
- *Inferencia. No se realiza inferencia a partir de datos personales del usuario, simplemente se procesa un mensaje de texto para categorizar una duda en una categoría de pregunta para encontrar una respuesta.*
- *Evolución. En el modelo de refinado de la inferencia, como se ha mencionado anteriormente, no se procesan datos personales.*

Como se ha mencionado, aunque la base de conocimientos (preguntas y respuestas) del chatbot es única, con el fin de llegar a un amplio espectro de la población, el bot se ha desplegado en diferentes canales: webs de Administraciones públicas y principales aplicaciones de mensajería instantánea. A continuación se relacionan los canales en los actualmente se encuentra desplegado:

Páginas Web:

- *Web del Gobierno de La Rioja: <https://web.larioja.org/> (icono verde en extremo inferior derecho de la portada)*
- *Web de la Consejería de Salud de La Rioja <https://www.riojasalud.es/> (icono verde en extremo inferior derecho de la portada)*

- *Web de recursos digitales oficiales del Ministerio de Asuntos Económicos y Transformación Digital: <http://covid19.gob.es> (icono azul en extremo inferior derecho de la portada)*

Whatsapp:

- *Canal oficial de Facebook del Ministerio de Sanidad, verificado por Facebook/Whatsapp Business, accesible en el teléfono +34 600 802 802.*

Telegram:

- *Bot oficial, accesible a través del usuario @hispabotcovid19_bot. “*

Consta en diligencia de la Inspección que en fecha 24 de julio de 2020, cuando se realizó la comprobación, el Chatbot HISPABOT.COVID19, no respondía a las peticiones de información, respondiendo con un mensaje que informaba que el mencionado chatbot dejó de estar activo el 12 de junio de 2020.

3 ESTUDIO DE MOVILIDAD- DataCOVID.

La aludida Orden SND/297/2020 encomienda a la SEDIA, siguiendo el modelo emprendido por el Instituto Nacional de Estadística en su estudio de movilidad y a través del cruce de datos de los operadores móviles, de manera agregada y anonimizada, el análisis de la movilidad de las personas en los días previos y durante el confinamiento.

Se cita que *“En la ejecución de este estudio, se velará por el cumplimiento de lo establecido 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; la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y los criterios interpretativos dados por la Agencia Española de Protección de Datos.”*

La Orden cita que el responsable del tratamiento será el Instituto Nacional de Estadística. Los encargados del tratamiento serán los operadores de comunicaciones electrónicas móviles, con los que se llegue a un acuerdo. El Instituto Nacional de Estadística, como responsable del tratamiento, autoriza a los operadores a recurrir a otros encargados en la ejecución de lo previsto en este apartado.

Los representantes de la SEDIA han manifestado lo siguiente:

“La Orden SND/297/2020 encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, siguiendo el modelo emprendido por el Instituto Nacional de Estadística en su estudio de movilidad y a través del cruce de datos de los operadores móviles, de manera agregada y anonimizada, el análisis de la movilidad de las personas en los días previos y durante el confinamiento. El responsable del tratamiento es el Instituto Nacional de Estadística. Los encargados del tratamiento son los tres grandes operadores de comunicaciones electrónicas móviles, con los que se ha llegado a un acuerdo.

El modelo de estudio de movilidad ya fue objeto de análisis por la AEPD, mediante reclamación remitida por dicho organismo, con Ref: E/10436/2019, de fecha 29 de octubre de 2019 (INE_Doc_1), que fue contestada por el INE en fecha 20 de

noviembre de 2019 (INE_Doc_2), donde, en síntesis, se explicaban las características del proyecto, exponiendo que sólo se usaban datos agregados y anonimizados, sin datos personales que permitieran la identificación directa o indirecta de los usuarios, entendiéndose por tanto que no era de aplicación la normativa de protección de datos.

Por último, con fecha 23 de diciembre de 2019 la AEPD remitió comunicación al INE (INE_Doc_3), mediante la cual se notifica que la Directora de la Agencia Española de Protección de Datos ha acordado inadmitir a trámite la reclamación presentada, entendiéndose que no hay vulneración del art. 6 del RGPD.

Descripción del estudio de movilidad

El objetivo que se pretende con este estudio es tener una buena aproximación a la movilidad e inmovilidad de la población española a partir del 15 de marzo con respecto a una situación normal, es decir, estimar cuántas personas están dejando sus áreas de residencia durante el horario de trabajo en estos días, así como a que áreas se desplazan durante las horas de trabajo, en relación con los flujos que pueden observarse en un día normal.

Los indicadores son:

- Población residente en cada área (cifras oficiales del Padrón a 1-1-2019)
- Número de personas que se estima que se quedan en su área de residencia
- Número de personas que se ausentan de su área de residencia
- Principales destinos (áreas de movilidad) a los que se dirigen los que salen de su área y cuántas personas se estima que se desplazan a ellos (flujos mayores o iguales de 100 personas entre áreas).

Para este estudio se divide España en 3.214 "áreas de movilidad" que son agrupaciones de población de entre 5.000 y 50.000 habitantes (mucho más homogéneas que los municipios). Un área en zona despoblada será la suma de varios municipios pequeños o muy pequeños (hasta sumar 5.000 habitantes) pero en las ciudades, las áreas serán los distritos o incluso desagregaciones de aquellos.

Para cada área de movilidad, cada operador proporciona el recuento del número de terminales que se considera como población residente en ella: una persona (un teléfono móvil) se considerará residente en el área donde el teléfono ha pasado la mayor parte del tiempo en el horario de 0h a 6h. De esta manera, cada teléfono móvil tiene asociada un área de residencia.

Los operadores calculan para cada teléfono celular, el área de destino, como el área más frecuente donde se detecta el teléfono durante el período de 10h a 16h del día objeto de estudio, siempre y cuando haya estado en ella al menos durante dos horas. Esta área puede ser la misma área de residencia, cualquier otra o incluso ninguna, si la persona se mueve continuamente o si el teléfono está apagado o fuera de cobertura.

Los operadores proporcionan, para cada área de residencia, el número de movimientos a las áreas de destino si este número supera las 10 o las 15 unidades

(dependiendo del operador), para proteger la privacidad y respetar el secreto estadístico.

Por tanto, cada operador entrega al INE un único fichero diario que contiene recuentos de las parejas residencia-destino para cada una de las 3.214 áreas de movilidad, siempre que estos recuentos alcancen el umbral antes citado.

El estudio de movilidad sigue los principios generales de eficacia, necesidad y proporcionalidad, utilizando únicamente datos de geolocalización de redes móviles previamente anonimizados. El INE no recibe, por lo tanto, información individual de ningún tipo, únicamente datos diarios anónimos y agregados de movimientos entre áreas.”

Se accede al documento del Instituto Nacional de Estadística titulado “Análisis de la movilidad de la población durante el estado de alarma por COVID_19 a partir de la posición de los teléfonos móviles”, publicado en la URL https://www.ine.es/covid/exp_movilidad_covid_proyecto.pdf donde se explican algunos aspectos de este estudio, tales como el ámbito geográfico y temporal y la información que se publica (que coincide con los indicadores expresados por la SEDIA en su contestación). Cabe reproducir el punto 6 donde se responde a la pregunta ¿Se puede saber con estos datos quién está en casa y quién está trabajando? siendo la respuesta:

“No. Lo que realmente se puede determinar, y siempre con cierto margen de error, es qué parte de la población se mantiene la mayor parte del tiempo en su área de residencia; pero los movimientos dentro de ella no se pueden detectar con esta metodología.

Además, los movimientos que se observan entre áreas limítrofes deben tomarse con cautela porque pueden estar provocados por el error que se comete al fijar la posición de cada terminal, lo que puede dar lugar a que se cuente un terminal que está inmóvil en dos áreas adyacentes diferentes en distintos momentos.

Tampoco se pueden detectar movimientos esporádicos que impliquen salir de las zonas de residencia durante muy poco tiempo (menos de dos horas).

Así, se estima como población que se queda en su área de residencia la que no la abandona o, si lo hace, no está fuera de ella más de dos horas continuadas.

Por otro lado, se cuenta como población que sale de su área a quienes no se localizan en ella de manera más frecuente en horario de 10 a 16 h. Es una aproximación a la población que trabaja, con las limitaciones que esta metodología impone.”

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para

resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

II

De conformidad con lo establecido en el artículo 55 del RGPD, la Agencia Española de Protección de Datos es competente para desempeñar las funciones que se le asignan en su artículo 57, entre ellas, la de hacer aplicar el Reglamento y promover la sensibilización de los responsables y los encargados del tratamiento acerca de las obligaciones que les incumben, así como tratar las reclamaciones presentadas por un interesado e investigar el motivo de las mismas.

Corresponde, asimismo, a la Agencia Española de Protección de Datos ejercer los poderes de investigación regulados en el artículo 58.1 del mismo texto legal, entre los que figura la facultad de ordenar al responsable y al encargado del tratamiento que faciliten cualquier información que requiera para el desempeño de sus funciones.

Correlativamente, el artículo 31 del RGPD establece la obligación de los responsables y encargados del tratamiento de cooperar con la autoridad de control que lo solicite en el desempeño de sus funciones. Para el caso de que éstos hayan designado un delegado de protección de datos, el artículo 39 del RGPD atribuye a éste la función de cooperar con dicha autoridad.

Del mismo modo, el ordenamiento jurídico interno también prevé la posibilidad de abrir un período de información o actuaciones previas. En este sentido, el artículo 55 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, otorga esta facultad al órgano competente con el fin de conocer las circunstancias del caso concreto y la conveniencia o no de iniciar el procedimiento.

III

El artículo 5 del RGPD consagra un conjunto de principios a los que debe ajustarse todo tratamiento de datos personales, estableciendo lo siguiente:

“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; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

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 razona-

bles 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»).

De conformidad con dispuesto en la letra a) de dicho precepto los datos personales deben ser tratados de manera lícita. Se tiene en cuenta a este respecto lo señalado en el considerando 40 del RGPD, según el cual: “Para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho, ya sea en el presente Reglamento o en virtud de otro Derecho de la Unión o de los Estados miembros a que se refiera el presente Reglamento, incluida la necesidad de cumplir la obligación legal aplicable al responsable del tratamiento o la necesidad de ejecutar un contrato en el que sea parte el interesado o con objeto de tomar medidas a instancia del interesado con anterioridad a la conclusión de un contrato.”

En el análisis de la licitud del tratamiento debe examinarse en primer lugar el tipo de datos que se tratan y si estos forman parte de las categorías especiales de datos a que se refiere el artículo 9 del RGPD. En este sentido, el considerando 35 del RGPD aclara 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 (1); 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* “

El artículo 9 del RGPD dispone en su número 1 que *“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”*. No obstante, establece en su número segundo que dicho apartado no será de aplicación cuando concurra alguna de las circunstancias que a continuación enumera, de las cuales interesan en el presente supuesto las dos siguientes, contenidas en las letras h) e i) de dicho artículo:

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,”

Ambas circunstancias vendrían a amparar el levantamiento de la prohibición de tratar categorías especiales de datos, debiendo complementarse la licitud del tratamiento con la existencia de alguna de las bases legitimadoras reguladas en el artículo 6 del RGPD, según el cual “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. “

Asimismo, el número 2 del artículo 6 del RGPD dispone que *“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.

En este sentido, el artículo 8 de la LOPDGDD establece respecto del tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos, que:

“1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.

2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley.”

Asimismo, el número segundo del artículo 9 de la misma ley dispone que “Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.

En particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte.”

Complementa estas previsiones lo establecido en la disposición adicional decimoséptima de dicha Ley según la cual:

“1. Se encuentran amparados en las letras g), h), i) y j) del artículo 9.2 del Reglamento (UE) 2016/679 los tratamientos de datos relacionados con la salud y de datos genéticos que estén regulados en las siguientes leyes y sus disposiciones de desarrollo:

- a) La Ley 14/1986, de 25 de abril, General de Sanidad.*
- b) La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.*
- c) La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.*
- d) La Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.*
- e) La Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias.*
- f) La Ley 14/2007, de 3 de julio, de Investigación biomédica.*

- g) La Ley 33/2011, de 4 de octubre, General de Salud Pública.
- h) La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.
- i) El texto refundido de la Ley de garantías y uso racional de los 105 medicamentos y productos sanitarios, aprobado por Real Decreto Legislativo 1/2015, de 24 de julio.
- j) El texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado por Real Decreto Legislativo 1/2013 de 29 de noviembre.”

En el presente caso, la licitud del tratamiento viene determinada por lo previsto en los artículos 6 y 9 del RGPD y la disposición adicional decimoséptima de la LOPDGDD en relación con las competencias atribuidas a la Administración General del Estado, o en particular al Ministerio de Sanidad, en materia sanitaria en las siguientes leyes: artículo 65 de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud; artículos 26 y 40 de la Ley 14/1986, de 25 de abril, General de Sanidad; artículo 3 Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública y artículos 13 y 14 de Ley 33/2011, de 4 de octubre, General de Salud Pública, y con las competencias atribuidas al Ministerio de Sanidad en el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria.

En lo que al principio de finalidad respecta, recogido en la letra b del artículo 5.1 del RGPD, señala la SEDIA “Los únicos tratamientos que se realizan son los contenidos en la política de privacidad, con fines estrictamente de interés público en el ámbito de la salud pública, y ante la situación de emergencia sanitaria decretada, a fin de proteger y salvaguardar un interés esencial para la vida de las personas, de acuerdo con las bases legitimadoras establecidas en el Reglamento General de Protección de Datos. Además, los datos se podrán tratar, adoptando las medidas técnicas y organizativas necesarias, incluida su anonimización, con fines estadísticos, de investigación biomédica, científica o histórica, y para archivo en interés público.” Estos fines vienen reflejados en la política de privacidad y a ellos hace referencia igualmente el convenio suscrito el 4 de abril de 2020 al enumerar las funcionalidades de la aplicación.

La política de privacidad señala entre fines de la aplicación “El objetivo de la aplicación es reducir el volumen de llamadas al número de emergencias sanitarias que trata las dudas sobre la enfermedad infecciosa COVID-19 (de la familia de infecciones del Coronavirus), informar a la población, permitir un triaje o autoevaluación inicial de posibles casos y un seguimiento posterior, y aliviar la carga de los Servicios de Emergencia de las distintas Administraciones Públicas con competencia en materia de salud. Más específicamente señala los siguientes fines:

- Ofrecerte información sobre el COVID-19, incluyendo el envío de notificaciones a través de la aplicación en relación con las mejores medidas preventivas y de evaluación en cada momento.
- Realizar tu autoevaluación en base a los síntomas médicos que nos comuniqués acerca de la probabilidad de que estés infectado por el virus COVID-19 o «coronavirus».
- Proporcionarte consejos prácticos y recomendaciones de acciones a seguir según evaluación. – Si es necesario, selección de cita para posible prueba, según diagnóstico.

- Recepción de resultados de la prueba y recomendaciones de actuación para la cuarentana o autocuarentena o cita con centro médico.
- Autoevaluación continua diaria: Monitorización de la temperatura y parámetros básicos, cada doce horas desde que se inicie la aplicación, incluyendo un recordatorio en forma de alarma para que lo vayas introduciendo.
- Conocer tu localización GPS en el momento de la autoevaluación exclusivamente para poder conocer en qué Comunidad Autónoma te encuentras y en su caso conectarte con los servicios de salud correspondientes. No se rastrea tu localización para finalidades distintas de las señaladas. Se podrá utilizar la dirección del domicilio proporcionada en el registro, con la finalidad de prestación de servicios sanitarios si fuera necesario. En cualquier caso, la aplicación no realiza geofencing para determinar si el usuario se encuentra en su domicilio.

Adicionalmente, conforme a lo establecido en la normativa aplicable, podremos tratar tus datos para las siguientes finalidades no directamente relacionadas con las funcionalidades de la «ASISTENCIACOV19», adoptando las medidas técnicas y organizativas necesarias, en particular, para garantizar el respeto al principio de minimización de datos personales, incluyendo su anonimización:

- Para finalidades estadísticas;
- Para investigación biomédica, científica o histórica; y
- Para archivo en interés público.

Estas finalidades permitirán hacer tanto un análisis anonimizado descriptivo de la situación, que permita conocer qué y por qué está ocurriendo (p.ej. las dinámicas actuales de la sintomatología en la población), así como un análisis anonimizado predictivo sobre la evolución de esta (p.ej. como podrían evolucionar dichas dinámicas en el futuro).

Además, estas finalidades son especialmente relevantes, no solo para conocer y predecir la situación de emergencia sanitaria actual, sino también para futuras investigaciones médicas, científicas e históricas que sean precisas llevar a cabo, entre otros objetivos, para prevenir y detectar situaciones similares que puedan tener lugar en el futuro.”

Respecto a las finalidades estadísticas, de investigación y archivo en interés público, debe tenerse en cuenta que el propio artículo 5.1.b del RGPD dispone que *“de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales”*

Por su parte, el número primero del artículo 89 del RGPD establece que *“El tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanza-*

rán de ese modo.”

El artículo 5.1. contempla en su letra c, el principio de minimización de datos. En cumplimiento de tal principio se señala en la documentación aportada que los datos a tratar son los siguientes:

- A) Datos identificativos y de contacto de usuarios, incluyendo entre otros: Nombre y apellidos; Número de teléfono móvil (para el envío de notificaciones); DNI/NIE (*para posterior cruce con la tarjeta sanitaria, a los efectos de que las autoridades sanitarias puedan integrar y comparar la información de pacientes con posibles síntomas con los sistemas públicos de gestión sanitaria existentes y hacer un seguimiento y atención personalizada*); Dirección completa y código postal, Fecha de nacimiento (*con objeto de poder establecer el grupo de población y ponderar los síntomas -el rango de edad puede determinar si se trata de un grupo de riesgo-*); Género.
- B) Geolocalización GPS de los usuarios, *con carácter opcional. Señalan a este respecto los representantes de la SEDIA que “es importante destacar que la aplicación no realiza rastreo de dispositivos móviles, sino que recaba datos personales y sanitarios para el correcto autodiagnóstico, así como datos de geolocalización vía GPS, siempre bajo autorización y en el momento de realizar la autoevaluación, para verificar la comunidad autónoma en la que se encuentra la persona.”*
- C) Datos de salud de los usuarios, *relacionados con los síntomas que experimentan* incluyendo, entre otros, sintomatología como: Tos seca, fiebre de más de 37,5°C, falta de aire, patologías previas, si se ha estado en contacto con algún paciente positivo confirmado de COVID-19, mucosidad nasal, dolor muscular; y/o malestar general.

El artículo 5.1.e) recoge el principio de limitación del plazo de conservación, respecto del cual aclara la *política de privacidad* *“Existen diversos motivos que nos legitiman para conservar tus datos, aunque solo los conservaremos y trataremos mientras sean necesarios para las finalidades indicadas en el punto 4 anterior, por lo que solo los conservaremos durante el tiempo que perdure la crisis sanitaria, con la excepción de las finalidades estadísticas, de investigación o archivo en interés público, cuyo plazo de conservación será de un máximo de dos años, todo ello de conformidad con los principios legales de tratamiento de datos, en particular el de minimización de datos. En el momento en que finalice el periodo de conservación de tus datos, estos serán anonimizados y/o bloqueados conforme a los requisitos establecidos en la normativa aplicable.”*

En lo que se refiere al principio de integridad y confidencialidad de los datos contemplado en la letra f) del artículo 5.1 del RGPD, consta en la cláusula décima del convenio, lo siguiente:

“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 que conozca y/o le sean informados efectivamente por el Responsable del Tratamiento el Encargado y Subencargado del Tratamiento aplicarán en función del análisis realizado conjuntamente con el Responsable del Tratamiento las medidas

técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya:

- 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, así como la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.*
- c) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.*
- d) un catálogo de medidas de seguridad según lo previsto en el Real Decreto 3/2010, de 8 de enero, y a luz del correspondiente análisis de riesgos.*

2.Al evaluar la adecuación del nivel de seguridad, el Encargado y Subencargado tendrán en cuenta los riesgos que presente el Tratamiento de datos detectados en el análisis realizado, 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.”

Asimismo la cláusula sexta, en su número primero letra e) enumera entre las obligaciones de Telefónica “e) La adopción de las medidas técnicas y organizativas apropiadas, de acuerdo con el correspondiente análisis de riesgos, para evitar la pérdida, alteración o acceso no autorizado de los datos manejados por la aplicación, según lo establecido en el artículo 32 del Reglamento (UE) 2016/679, en la disposición adicional primera de la Ley Orgánica 3/2018 y en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica.”

El análisis de riesgos evalúa entre otros aspectos la confidencialidad, integridad y disponibilidad de la información. El protocolo de acceso a los datos por parte de las CCAA, recoge también las correspondientes medidas de seguridad.

De todo ello cabe concluir que el tratamiento de datos efectuado mediante la aplicación móvil ASISTENCIACOV19, con las finalidades explícitas y determinadas señaladas en la política de privacidad, se encontraría legitimado en lo previsto en los artículos 9, apartados h) e i), y 6.1, letras c) y e) del RGPD, en relación con lo previsto en los artículos 8, 9.2 y disposición adicional decimoséptima de la LOPDGDD en relación con las competencias atribuidas a la Administración General del Estado, o en particular al Ministerio de Sanidad, en materia sanitaria en las siguientes Leyes: artículo 65 de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud; artículos 26 y 40 de la Ley 14/1986, de 25 de abril, General de Sanidad; artículo 3 Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública y artículos 13 y 14 de Ley 33/2011, de 4 de octubre, General de Salud Pública y las competencias que al Ministerio de Sanidad confiere el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria. Ello sin perjuicio de que pudieran concurrir en el presente supuesto otras bases legitimadoras del tratamiento. Los datos a tratar se encuentran limitados a los adecuados y pertinentes para los fines declarados. Asimismo, la conservación de los datos obtenidos de forma que se permita la identificación de los interesados se limita al tiempo que se mantenga la crisis sanitaria, con la excepción de las finalidades estadísticas, de investigación o archivo en interés

público, cuyo plazo de conservación se fija en dos años y se han adoptado medidas para garantizar la seguridad de los datos tratados.

IV

El RGPD regula en la sección primera de su capítulo III, dentro de los derechos del interesado el relativo a la transparencia de la información. El artículo 13 del mismo detalla la información que deberá facilitarse cuando los datos personales se obtengan del interesado, disponiendo que:

“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.”

Se verifica que la política de privacidad de la aplicación móvil ASISTENCIACOV19, informa sobre la identidad y dirección postal del responsable de los tratamientos (Ministerio de Sanidad); datos de contacto del Delegado de Protección de datos; de las categorías de datos objeto de tratamiento (datos identificativos y de contacto, datos de geolocalización y datos de salud relacionados con los síntomas experimentados); de las finalidades del tratamiento (reducir el volumen de llamadas al número de emergencias sanitarias que trata las dudas sobre la enfermedad infecciosa COVID-19, informar a la población, permitir un triaje o autoevaluación inicial de posibles casos y un seguimiento posterior, y aliviar la carga de los Servicios de Emergencia de las distintas Administraciones Públicas con competencia en materia de salud y adicionalmente, finalidades estadísticas investigación biomédica, científica o histórica y archivo en interés público); de la base jurídica del tratamiento (*interés público y salvaguarda de un interés esencial para la vida de las personas*). Se informa sobre los destinatarios de los datos (profesionales sanitarios, y *autoridades competentes de las Comunidades Autónomas en materia de sanidad, INGESA, MUFACE, ISFAS y MUGEJU y otras autoridades nacionales y/o internacionales, con las que sea necesario compartir los datos del usuario*); del período de conservación de los datos, de la posibilidad de ejercicio de los derechos de acceso, rectificación, supresión, limitación y oposición. Se informa también de la posibilidad de solicitar la tutela de la Agencia Española de Protección de datos si los derechos no son atendidos correctamente.

V

El artículo 28 del RGPD regula la figura del encargado del tratamiento, estableciendo en su número tercero que *“el tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. (...)”* A continuación especifica las estipulaciones que dicho contrato o acto jurídico debe contener:

a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;

b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;

c) tomará todas las medidas necesarias de conformidad con el artículo 32;

d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;

e) asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;

f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;

g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;

h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

Asimismo dispone en su número 4 que “Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado a que se refiere el apartado 3, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.”

Estos contenidos vienen reflejados en el Convenio entre Secretaría de Estado de Digitalización e Inteligencia Artificial y Telefónica Digital España, S.L.U., para la operación de la aplicación «ASISTENCIACOV19» en el contexto de la situación de crisis sanitaria ocasionada por el COVID-19, suscrito el 4 de abril de 2020, en particular en las cláusulas cuarta, novena, décima, decimosexta, decimoséptima y decimoctava, anteriormente transcritas así como en el anexo al aludido convenio relativo al acuerdo de subencargo del tratamiento.

VI

Por último, debe reseñarse que se ha efectuado una evaluación de impacto previa a la puesta en funcionamiento de la aplicación, de conformidad con lo previsto en el artículo 35.1 del RGPD, según el cual “Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales.”

Asimismo, debe señalarse que de la documentación analizada no se desprende que se vayan a llevar a cabo transferencias internacionales de datos.

VII

La Orden SND/297/2020, de 27 de marzo en su artículo primero, número 2 encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, (SEDIA) el desarrollo de un asistente conversacional o chatbot para ser utilizado vía Whatsapp y otras aplicaciones de mensajería instantánea, que proporcionará información oficial ante las preguntas de la ciudadanía.

Respecto a los posibles tratamientos de datos personales Los representantes de la SEDIA han manifestado lo siguiente:

“La Orden SND/297/2020 mencionada ut supra encomienda a la SEDIA el desarrollo de un asistente conversacional o chatbot, para ser utilizado vía Whatsapp y otras aplicaciones de mensajería instantánea, que proporcionará información oficial ante las preguntas de la ciudadanía de acuerdo con información oficial del Ministerio de Sanidad.

El objetivo del sistema Hispabot-Covid19 es responder a las preguntas de los ciudadanos. Para hacerlo, utiliza diferentes canales para recibir las preguntas, un motor de procesamiento de Lenguaje Natural para identificarlas y detectar la respuesta; y devolverla al usuario por el canal por el que hizo la pregunta.

1. *El sistema recibe la pregunta por web, Telegram o Whatsapp, y el único dato que obtiene del usuario es el texto que escribe. Es decir, la única información que se trata es la propia conversación.*

2. *El sistema no solicita ni necesita datos personales, lo que se indica claramente en el mensaje de bienvenida al usuario:*

“Este servicio solo aporta información oficial. Almacena de forma anónima tus consultas para ir mejorando las respuestas y aprender a resolver nuevas preguntas. En ningún caso se solicitará ni debes facilitar ningún dato de carácter personal. Puedes consultar la política de privacidad en: <https://www.covid19.gob.es/hispabot-covid19>”

3. *Las conversaciones con el asistente se recuperan del canal que elige el usuario (Web, Whatsapp, Telegram), y se ingresan en el motor de inferencia y entendimiento, y esa es la única información que se almacena.*

Por tanto, en relación con la tipología de datos personales que van a ser recabados, cabe señalar que el servicio no recopila ningún dato de carácter personal (ni de ubicación, ni de salud, ni de contacto, ni identificadores en línea). El servicio se presta de forma totalmente anónima y no requiere la identificación del usuario.

El chatbot únicamente utiliza el contenido de los mensajes de texto (es decir, el texto, ignorando los datos del emisor) que los usuarios envían al sistema, con los siguientes objetivos:

- 1. Para que se detecten nuevas áreas de interés del ciudadano, a partir del análisis de las preguntas realizadas. Y poder trasladar estas inquietudes a los expertos, para que valoren su inclusión en la base de conocimiento si procede.*
- 2. Para que se mejore el motor de inferencia heurística, de manera que se garantice que las respuestas del asistente son las adecuadas según la pregunta del ciudadano.*
- 3. Para que aquellas consultas que no se consideren oportunas en el ámbito de Hispabot-Covid19 tengan en cualquier caso una respuesta apropiada.*

No se han hallado indicios que puedan contradecir lo manifestado anteriormente respecto al asistente conversacional, éste ya no se encontraba activo cuando se llevaron a cabo las actuaciones de investigación por parte de la Subdirección de Inspección.

VIII

En lo que se refiere al estudio de movilidad DataCOVID, la Orden SND/297/2020 encomienda a la SEDIA, siguiendo el modelo emprendido por el Instituto Nacional de Estadística en su estudio de movilidad y a través del cruce de datos de los operadores móviles, de manera agregada y anonimizada, el análisis de la movilidad de las personas en los días previos y durante el confinamiento.

El artículo 2 del RGPD, relativo a su ámbito de aplicación material, dispone en su número primero que *“El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.”*

El artículo 4 del RGPD define en su número 1, los datos personales 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 considerando 26 del RGPD aclara a este respecto que “Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la

singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por lo tanto los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación.”

En este mismo sentido, el RGPD dispone en su artículo 89.1 “El tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo.”

En lo que al presente supuesto respecta, señalan los representantes de la SEDIA que “Para este estudio se divide España en 3.214 “áreas de movilidad” que son agrupaciones de población de entre 5.000 y 50.000 habitantes (mucho más homogéneas que los municipios). Un área en zona despoblada será la suma de varios municipios pequeños o muy pequeños (hasta sumar 5.000 habitantes) pero en las ciudades, las áreas serán los distritos o incluso desagregaciones de aquellos.

Para cada área de movilidad, cada operador proporciona el recuento del número de terminales que se considera como población residente en ella: una persona (un teléfono móvil) se considerará residente en el área donde el teléfono ha pasado la mayor parte del tiempo en el horario de 0h a 6h. De esta manera, cada teléfono móvil tiene asociada un área de residencia.

Los operadores calculan para cada teléfono celular, el área de destino, como el área más frecuente donde se detecta el teléfono durante el período de 10h a 16h del día objeto de estudio, siempre y cuando haya estado en ella al menos durante dos horas. Esta área puede ser la misma área de residencia, cualquier otra o incluso ninguna, si la persona se mueve continuamente o si el teléfono está apagado o fuera de cobertura.

Los operadores proporcionan, para cada área de residencia, el número de movimientos a las áreas de destino si este número supera las 10 o las 15 unidades (dependiendo del operador), para proteger la privacidad y respetar el secreto estadístico.

Por tanto, cada operador entrega al INE un único fichero diario que contiene recuentos de las parejas residencia-destino para cada una de las 3,214 áreas de movilidad, siempre que estos recuentos alcancen el umbral antes citado.

El estudio de movilidad sigue los principios generales de eficacia, necesidad y proporcionalidad, utilizando únicamente datos de geolocalización de redes móviles previamente anonimizados. El INE no recibe, por lo tanto, información individual de ningún tipo, únicamente datos diarios anónimos y agregados de movimientos entre áreas.”

Asimismo expone que el modelo de estudio de movilidad ya fue objeto de análisis por la AEPD, mediante reclamación remitida por dicho organismo, con Ref: E/10436/2019, de fecha 29 de octubre de 2019 (INE_Doc_1), que fue contestada por el INE en fecha 20 de noviembre de 2019 (INE_Doc_2), donde, en síntesis, se explicaban las características del proyecto, exponiendo que sólo se usaban datos agregados y anonimizados, sin datos personales que permitieran la identificación directa o indirecta de los usuarios, entendiéndose por tanto que no era de aplicación la normativa de protección de datos.

En consecuencia, en tanto el estudio de movilidad DataCOVID sigue el modelo analizado ya por esta Agencia en el archivo E/10436/2019, en que los datos se reciben de forma anonimizada y agregada, sin que sea posible la reidentificación de los interesados con dicha información, no resultaría de aplicación lo previsto en el RGPD, de conformidad con lo previsto en su artículo 2 al señalar su ámbito de aplicación.

Por lo tanto, de la documentación analizada en los párrafos anteriores, relativa a la aplicación oficial “ASISTENCIACOV19, del asistente conversacional (Chatbot) HISPABOT-COV19 y del estudio de movilidad DataCOVID, no se desprenden indicios racionales de infracción de la normativa sobre protección de datos.

Por lo tanto, de acuerdo con lo señalado, por la directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital

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, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, 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.

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