Datuak Babesteko
Euskal Bulegoa
Agencia Vasca de
Protección de Datos

**CN20-005**

**DICTAMEN Nº D20-016**

**DICTAMEN RELATIVO A LA APLICACIÓN INFORMÁTICA "COVID-19.eus"**

## I
## ANTECEDENTES

**PRIMERO.-** El Director de Régimen Jurídico, Económico y Servicios del Departamento de Salud, solicita informe sobre la aplicación COVID-19.eus. En concreto, se consulta a la Agencia si la finalidad de la APP cumple con lo dispuesto por el Reglamento UE 2016/679 de 27 de abril (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre. Para ello, adjunta a su escrito las Condiciones de Uso y la Política de Privacidad que incluye la información que facilita a los usuarios de la APP. Asimismo, solicita que se aclare la edad legal mínima para que los interesados puedan otorgar su consentimiento para el tratamiento de datos sin el consentimiento de sus progenitores o tutores legales.

**SEGUNDO.-** Al objeto de resolver la consulta planteada, la AVPD solicita a la Administración sanitaria información detallada y documentada sobre esta iniciativa.

En ese mismo escrito la AVPD informa al Departamento sobre la edad necesaria para ser usuario de la aplicación, señalando que el 9.4 de 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, reconoce a los mayores de 16 años la capacidad legal para entender la información médica y decidir sobre su propia salud, y siendo ésta la edad necesaria para consentir en el ámbito sanitario, es también la edad que la AVPD entiende debe ser exigida para que un menor se dé de alta en la aplicación.

**TERCERO.-** El Departamento de Salud remite a la AVPD la información elaborada por el responsable del tratamiento a requerimiento de la Agencia.

## II
## INTERVENCIÓN DE LA AGENCIA VASCA DE PROTECCIÓN DE DATOS

El artículo 17.1 de la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos, en su apartado n) atribuye a la Agencia Vasca de Protección de Datos la siguiente función:

*"Atender a las consultas que en materia de protección de datos de carácter personal le formulen las administraciones públicas, instituciones y corporaciones a que se refiere el artículo 2.1 de esta Ley, así como otras personas físicas o jurídicas, en relación con los tratamientos de datos de carácter personal incluidos en el ámbito de aplicación de esta Ley".*

Corresponde a esta Agencia Vasca de Protección de Datos, en virtud de la normativa citada, la emisión del dictamen en respuesta a la consulta formulada.

## III

## APP “COVID-19.eus”

La situación de emergencia sanitaria derivada de la propagación del Covid-19, ha llevado a las Autoridades Sanitarias a la adopción de numerosas medidas para luchar contra esa pandemia y proteger la vida y la salud de la población, entre ellas, la puesta en marcha de aplicaciones móviles orientadas a controlar y reducir el contagio. Es el caso de la aplicación para los teléfonos móviles “COVID-19.eus”, que el Departamento de Salud ha puesto a disposición de la ciudadanía junto con la empresa vasca EricTel, con el objetivo de tejer una RED CIUDADANA que ayude en la contención del coronavirus, contribuyendo a su prevención, detección y seguimiento.

Según las condiciones de uso de la aplicación, la utilización de la app es voluntaria y gratuita, y para utilizar los servicios que ésta ofrece es requisito indispensable estar registrado como usuario y facilitar una serie de datos personales. Ello nos obliga a analizar la incidencia de esta app en el derecho de las personas a la protección de sus datos personales, dado que durante el uso de esta aplicación es necesario que se garantice su privacidad y, se respeten los principios que rigen el tratamiento de esos datos personales.

## IV

## INCIDENCIA DE LA APP “COVID-19.eus” EN EL DERECHO FUNDAMENTAL DE LAS PERSONAS A LA PROTECCIÓN DE SUS DATOS

El marco normativo en materia de protección de datos personales, se contiene en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), directamente aplicable en los Estados miembros desde el 25 de mayo de 2018, y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), en vigor desde el 7 de diciembre de 2018 ( LOPDGDD, en adelante). Así mismo, resulta de aplicación en esta Comunidad Autónoma, la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal y de Creación de la Agencia Vasca de Protección de Datos y su normativa de desarrollo, en todo aquello que no se haya visto desplazada por la normativa anterior.

En esta materia hay dos conceptos esenciales, el concepto de dato personal y el de tratamiento de datos.

El Reglamento General de Protección de Datos (RGPD), define, en su artículo 4.1, 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;”*.

En relación a este concepto, el Considerando 26 del RGPD precisa lo siguiente:

> *"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".***

Además de otros datos personales, esta aplicación trata datos relacionados con la salud de los usuarios. Estos datos se definen en el art. 4 15) RGPD como los "*datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud".*

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

El Reglamento establece un concepto amplísimo de datos de salud, y le otorga un régimen específico, el correspondiente a las denominadas "categorías especiales de datos" a que se refiere el artículo 9 del texto.

Finalmente, interesa destacar la definición del tratamiento de datos personales (artículo 4.2 RGPD) como: *"Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra".*

Definidos y delimitados estos conceptos básicos, pasamos ahora a analizar la adecuación de la app a los principios que rigen el tratamiento de los datos personales.

**Principio de Licitud**

El RGPD regula en su artículo 5 los principios relativos al tratamiento de datos personales, disponiendo en primer lugar que los datos serán tratados de manera lícita, leal y transparente (art. 5.1a).

Todo tratamiento de datos personales supone una injerencia en el derecho fundamental a la protección de datos personales, y por ello sólo será lícito si se ampara en alguna base jurídica que legitime el uso de los datos.

En este caso, según la información remitida por el Departamento de Salud, en la app se tratan datos de carácter identificativo, datos de salud y características personales.

Además, se informa a esta Agencia que una de las funcionalidades de la app es la utilización de datos de localización GPS, totalmente anonimizados, para detectar donde ha circulado el usuario con el fin de poder establecer un vector de transmisión de la epidemia. Dada la relevancia de estos datos de ubicación a través de la geolocalización, abordaremos el tratamiento de los mismos en un apartado específico de este informe.

Según la información remitida, los datos se recogen de los propios usuarios de la app, y su tratamiento se ampara en el consentimiento de los interesados, así como en otras dos bases jurídicas: el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos y, por otro lado, la protección de intereses vitales de los interesados o de otras personas. Los datos recogidos serán analizados por los epidemiólogos del Servicio de Vigilancia Epidemiológica y Vacunaciones de la Dirección de Salud Pública y Adicciones (responsable del tratamiento). Así mismo, estas personas serán los encargados de realizar los estudios epidemiológicos precisos para conocer con más detalle el virus SARS-Cov-2 y sus consecuencias para la salud pública. Además, los casos probables de positivo en el virus se comunicarán a Osakidetza-Servicio Vasco de Salud para que sean diagnosticados y se les preste asistencia sanitaria. Y los casos positivos se comunicarán al Ministerio de Salud de manera totalmente anonimizada.

De conformidad con el principio de licitud del tratamiento, los tratamientos de datos personales deberán ampararse en alguna de las posibles seis bases jurídicas enunciadas en el artículo 6 RGPD, entre ellas, el consentimiento del interesado (art. 6.1 a ), la protección de intereses vitales de los interesados o de otras personas ( art. 6.1d), o el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable ( art. 6.1e), si bien en este último caso, el tratamiento será legítimo cuando derive de una competencia atribuida por una norma con rango de ley ( art. 8.2 de la LOPDGD).

Pero cuando esa información personal se refiera a categorías especiales de datos, como los datos de salud, cuyo tratamiento se encuentra, como regla general, prohibido por el artículo 9.1 RGPD, la base jurídica legitimadora del tratamiento debe incardinarse en alguna de las excepciones del artículo 9.2 del RGPD.

La Agencia Vasca de Protección de Datos ya ha tenido ocasión de pronunciarse recientemente sobre esta cuestión en su dictamen D20-012, emitido a instancia del

Departamento de Salud, donde mantiene que en el actual escenario de pandemia mundial, donde los valores esenciales que deben protegerse son la vida y la salud de las personas, el RGPD permite a la Administración Sanitaria el tratamiento de datos de salud sin el consentimiento de los interesados, entre otros supuestos, por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud (9.2 i) RGPD) sobre la base del Derecho de la Unión o de los Estados miembros.

En relación con esta base legitimadora, y en este contexto, según el Considerando 54 del RGPD, salud pública debe interpretarse como "*todos los elementos relacionados con la salud, concretamente el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de la asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad".*

El RGPD permite también el tratamiento de los datos de salud para la protección de intereses vitales del interesado o de otra persona (art. 9.2 c) RGPD. En relación con esta base legitimadora, el Considerando 46 del RGPD, señala lo siguiente:

> *"(46) El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente L 119/8 ES Diario Oficial de la Unión Europea 4.5.2016 (1) Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores (DO L 95 de 21.4.1993, p. 29). deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente. Ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano".*

Otras bases legitimadoras del tratamiento de datos de salud las encontramos en los apartados h) y j) de este mismo el artículo 9.2 del RGPD:

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

Por su parte, el artículo 9 de la LOPDGDD, dedicado a las categorías especiales de datos, dispone en su apartado segundo 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 este sentido, la propia Disposición Adicional Decimoséptima de la LOPDGDD, dedicada al tratamiento de datos de salud, establece que se encuentran amparados en las letras g), h) i) y j) del artículo 9.2 RGPD, los tratamientos de datos regulados en las Leyes sanitarias que esta Disposición recoge en su apartado 1, estableciendo en su apartado 2 los criterios por los que han de regirse los tratamientos de datos en la investigación en la salud.

Además de ello, La LOPGDD, en sus disposiciones final quinta y novena, respectivamente, modifica dos normas sanitarias: la Ley General de Sanidad, a la que añade un artículo 105 bis (tratamiento de datos en la investigación) y la Ley de autonomía del paciente y de derechos obligaciones en materia de información y documentación clínica, modificando el apartado 3 de su artículo 16, referido al uso de la historia clínica.

Analizada la legislación sectorial, estatal y autonómica en materia sanitaria, la Agencia Vasca de Protección de Datos encuentra en el propio RGPD y la LOPDGDD, junto con la 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, la Ley 41/2002, de 14 de octubre, básica reguladora de la autonomía del paciente y de los derechos y obligaciones en materia de información y documentación clínica; la Ley 14/1986, de 25 de abril, General de Sanidad y la Ley de Ordenación Sanitaria de Euskadi, amparo legal suficiente para que la Administración Sanitaria lleve a cabo los tratamientos de datos de salud necesarios para la lucha contra la propagación del COVID-19 y la preservación de la salud pública. Son, precisamente, estas leyes sanitarias, junto con el consentimiento de los interesados, las bases jurídicas invocadas por la Administración sanitaria como legitimadoras de los tratamientos de datos derivados de la puesta en marcha de esta aplicación.

Lo que no queda suficientemente claro en la información remitida, en concreto, a la vista del apartado " categorías de destinatarios", es si además del Ministerio de Sanidad (con datos anonimizados) y Osakidetza-Svs (para su tratamiento por los profesionales sanitarios que presten asistencia a los usuarios de la app), podrán ser destinatarios de la información otras entidades sanitarias y órganos de la Administración del Estado o de la Administración de la CAPV, ni, en su caso, la base jurídica que legitimaría esas comunicaciones de datos.

Por otro lado, figuran también como destinatarios de la información los contactos de las personas usuarias que han dado positivo. La app COVID-19.eus permite crear círculos de relaciones del usuario con personas cercanas (familia, amigos, compañeros), con el objetivo primordial de concienciar del distanciamiento físico para evitar el contagio, de forma que si una persona del círculo se contagia, los contactos de primer nivel entrarán en aislamiento, utilizando para ello un código de colores. Si para crear esos círculos hay que facilitar el número del móvil de las personas que quieres añadir, y luego todas las personas que están dentro del círculo sabrán el riesgo de contagio que tienen los demás, entendemos que la base jurídica que legitimaría esos tratamientos sería el consentimiento de los interesados.

En este sentido, resulta obligado recordar que para que el consentimiento actúe como base legitimadora del tratamiento es necesario que cumpla las exigencias impuestas por el RGPD, esto es, debe darse mediante un acto afirmativo claro, que refleje una manifestación de voluntad libre, específica, informada e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen para la finalidad o finalidades

concretas pretendidas. Por lo tanto, el silencio, las casillas ya marcadas o la inacción no constituyen consentimiento. Además, cuando se traten datos de salud, ese consentimiento deberá ser explícito. Por último, conviene destacar que cuando el tratamiento tenga varios fines, el consentimiento deberá darse para todos ellos, y el interesado tendrá derecho a retirarlo en cualquier momento (C 32, artículos 6.1 a), 7 y 9.2 a) RGPD).

**Principio de limitación de la finalidad**

El artículo 5.1b) del RGPD regula el principio de limitación de la finalidad, consistente en que los datos serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente para finalidades distintas o de manera incompatible con dichos fines.

La app es una herramienta para poner freno a la pandemia causada por el Covid-19, y proteger la salud de la población, que tiene numerosas funcionalidades: ofrecer información sobre el COVID-19, incluyendo el envío de notificaciones a través de la aplicación en relación con las medidas preventivas y de evaluación en cada momento; analizar los síntomas reportados en la autoevaluación y actualizados con nuevas evidencias; proporcionar consejos prácticos y recomendaciones; si es necesario, gestionar la cita para una posible prueba diagnóstica y facilitar el contacto con el sistema sanitario; conocer datos complementarios como duración de la patología, y apoyar al sistema sanitario en la localización de los casos.

Además de para esas funcionalidades, se prevé que los datos puedan tratarse para finalidades no directamente relacionadas con esas funcionalidades, pero siempre relacionadas con la pandemia del COVID-19, como serían finalidades históricas, estadísticas o científicas o de investigación epidemiológica **y actividades análogas.**

El cumplimiento de este principio exige que las finalidades del tratamiento estén claramente determinadas, lo que impediría el tratamiento de los datos de la app para una finalidad distinta de la inicial que motiva su recogida, salvo que cuente con una base jurídica que lo legitime.

No obstante, no considera desviación de la finalidad, su utilización posterior para fines de investigación científica e histórica o fines estadísticos (art. 5.1.b) in fine del RGPD), si bien, esos tratamientos estarán sujetos a las garantías del artículo 89 del RGPD, que exigen la adopción de medidas técnicas y organizativas que aseguren el respeto del principio de minimización de los datos personales. En este sentido, el apartado 1 del artículo 89 menciona la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines y, además, siempre que esos fines puedan alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo.

Además de este precepto del RGPD, el tratamiento de datos en la investigación en salud dispone de un precepto específico en la LOPDGDD, concretamente en su Disposición Adicional Decimoséptima (apartado 2), que establece los criterios por los que debe regirse ese tratamiento:

> *"2. El tratamiento de datos en la investigación en salud se regirá por los siguientes criterios:*

*a) El interesado o, en su caso, su representante legal podrá otorgar el consentimiento para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica. Tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora.*

*b) Las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública podrán llevar a cabo estudios científicos sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública.*

*c) Se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial.*

*En tales casos, los responsables deberán publicar la información establecida por el artículo 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, en un lugar fácilmente accesible de la página web corporativa del centro donde se realice la investigación o estudio clínico, y, en su caso, en la del promotor, y notificar la existencia de esta información por medios electrónicos a los afectados. Cuando estos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato.*

*Para los tratamientos previstos en esta letra, se requerirá informe previo favorable del comité de ética de la investigación.*

*d) Se considera lícito el uso de datos personales seudonimizados con fines de investigación en salud y, en particular, biomédica.*

*El uso de datos personales seudonimizados con fines de investigación en salud pública y biomédica requerirá:*

*1.º Una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación.*

*2.º Que los datos seudonimizados únicamente sean accesibles al equipo de investigación cuando:*

*i) Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.*

*ii) Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados.*

*Podrá procederse a la reidentificación de los datos en su origen, cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria.*

*e) Cuando se traten datos personales con fines de investigación en salud, y en particular la biomédica, a los efectos del artículo 89.2 del Reglamento (UE) 2016/679, podrán excepcionarse los derechos de los afectados previstos en los artículos 15, 16, 18 y 21 del Reglamento (EU) 2016/679 cuando:*

*1.º Los citados derechos se ejerzan directamente ante los investigadores o centros de investigación que utilicen datos anonimizados o seudonimizados.*

*2.º El ejercicio de tales derechos se refiera a los resultados de la investigación.*

*3.º La investigación tenga por objeto un interés público esencial relacionado con la seguridad del Estado, la defensa, la seguridad pública u otros objetivos importantes de interés público general, siempre que en este último caso la excepción esté expresamente recogida por una norma con rango de Ley.*

*f) Cuando conforme a lo previsto por el artículo 89 del Reglamento (UE) 2016/679, se lleve a cabo un tratamiento con fines de investigación en salud pública y, en particular, biomédica se procederá a:*

*1.º Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 35 del Reglamento (UE) 2016/679 o en los establecidos por la autoridad de control. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos.*

*2.º Someter la investigación científica a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica.*

*3.º Adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados.*

*4.º Designar un representante legal establecido en la Unión Europea, conforme al artículo 74 del Reglamento (UE) 536/2014, si el promotor de un ensayo clínico no está establecido en la Unión Europea. Dicho representante legal podrá coincidir con el previsto en el artículo 27.1 del Reglamento (UE) 2016/679.*

*g) El uso de datos personales seudonimizados con fines de investigación en salud pública y, en particular, biomédica deberá ser sometido al informe previo del comité de ética de la investigación previsto en la normativa sectorial.*

*En defecto de la existencia del mencionado Comité, la entidad responsable de la investigación requerirá informe previo del delegado de protección de datos o, en su defecto, de un experto con los conocimientos previos en el artículo 37.5 del Reglamento (UE) 2016/679.*

*h) En el plazo máximo de un año desde la entrada en vigor de esta ley, los comités de ética de la investigación, en el ámbito de la salud, biomédico o del medicamento, deberán integrar entre sus miembros un delegado de protección de datos o, en su defecto, un experto con conocimientos suficientes del Reglamento (UE) 2016/679 cuando se ocupen de actividades de investigación que comporten el tratamiento de datos personales o de datos seudonimizados o anonimizados".*

El legislador ha abordado de forma extensa el tratamiento de datos de salud con fines de investigación, pudiendo destacarse dos aspectos: el recurso a los datos seudonimizados en la labor investigadora, y la necesidad de adopción de garantías, entre las que podemos destacar la necesidad de realizar una evaluación de impacto y también la necesidad de que la investigación sea sometida a informe previo del comité de ética correspondiente, o, en su defecto del DPO o de un experto en último caso.

Por último, es preciso recordar que el pasado 21 de abril, el Comité Europeo de Protección de Datos (CEPD), organismo europeo independiente que contribuye a la aplicación coherente de la normativa de protección de datos en toda la UE, adoptó las **Directrices**

**03/ 2020, sobre el tratamiento de datos relativos a la salud con fines de investigación científica en el contexto del brote del COVID-19**, donde se contienen las pautas para que esos tratamientos de datos (que en el caso analizado entendemos son de uso secundario, al ser recabados inicialmente para otra finalidad), sean conformes con la normativa de protección de datos personales, entre ellas, las referidas a definiciones específicas, bases legitimadoras del tratamiento, obligaciones de transparencia, limitación de la finalidad y de conservación de los datos, minimización y medidas de seguridad y derechos de los interesados).

Las directrices están disponibles en el siguiente enlace:

https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_en

## Principio de transparencia

Con la entrada en vigor del RGPD, el deber de información se incluye entre los principios aplicables al tratamiento de datos personales. El principio de transparencia se proclama en el artículo 5.1. a) del RGPD, y requiere que toda la información referida al tratamiento de datos personales sea fácilmente accesible, con un lenguaje claro y sencillo. La transparencia de la información exige que las personas sean informadas con carácter previo al tratamiento de sus datos de todas las cuestiones recogidas en los artículos 13 y 14 del RGPD, en función de que los datos se obtengan o no del propio interesado.

En relación con este principio, debe destacarse que esta obligación deberá ser cumplida con carácter previo a que las personas se den de alta en la aplicación.

En todo caso, es necesario advertir que la información contenida en la política de privacidad de la app actualmente publicada en la página web del Departamento, y la información proporcionada a requerimiento de esta Agencia, no son siempre coincidentes en cuestiones relevantes (actividad de tratamiento, origen de los datos, destinatarios…), divergencias que necesariamente deberán ser corregidas**.**

## Principio de minimización

De conformidad con lo dispuesto en el artículo 5.1.c) del Reglamento General de Protección de Datos, deberán ser objeto de tratamiento los datos adecuados, pertinentes y limitados a lo necesario en relación con los fines que motivan ese tratamiento.

Este principio, junto con el de legitimación y el de transparencia, adquiere especial importancia en el supuesto analizado. El cumplimiento de este principio exige que la Administración Sanitaria trate únicamente aquellos datos personales que sean estrictamente necesarios para lograr la finalidad pretendida con aplicación COVID-19.eus. Cualquier injerencia sobre la privacidad de las personas debe someterse a un juicio de necesidad y proporcionalidad, y corresponde al responsable de la aplicación hacer esa ponderación

Por ello, se aconseja la revisión de los datos que se recogen en la aplicación, evitando aquellos que no resulten imprescindibles para alcanzar su finalidad. En este sentido, es obligado recordar que siempre que la finalidad perseguida pueda lograrse con datos anonimizados, no deberán tratarse datos personales.

**Principio de exactitud**

El RGPD, en su artículo 5.1.d), proclama que los datos serán exactos y, si fuera necesario, actualizados, adoptándose las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales inexactos.

La fiabilidad de la información se constituye en un valor esencial para lograr los objetivos de la app. De hecho, en las condiciones de uso de la aplicación se impone como una obligación de los usuarios que la información que faciliten deberá ser siempre real, veraz y estar actualizada.

Del mismo modo, el responsable de la app deberá garantizar la certeza de la información objeto de tratamiento en la aplicación "COVID-19.eus".

**Principio de integridad y confidencialidad**

El RGPD incluye entre los principios aplicables al tratamiento de los datos personales el principio de integridad y confidencialidad (art. 5 f) que exige que los datos personales sean tratados de tal manera que se garantice una seguridad adecuada 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.

Este principio no alude únicamente a las medidas de seguridad, sino que también se refiere a las políticas de acceso a la información, que deben evitar en todo caso tratamientos no autorizados o ilícitos.

El RGPD configura un sistema de seguridad que no se basa en los niveles de seguridad básico, medio y alto que se contemplaban en el Reglamento de desarrollo de la derogada LOPD, sino que tras una previa valoración de los riesgos (análisis de riesgos) el responsable del tratamiento deberá determinar qué medidas de seguridad técnicas y organizativas son necesarias en función del tratamiento previsto (C 83 y art. 32 RGPD).

Sin embargo, cuando los responsables del tratamiento sean Administraciones Públicas, deberán aplicar a los tratamientos de datos personales las medidas de seguridad que corresponda de las previstas en el Esquema Nacional de Seguridad (apartado 2 de la Disposición Adicional Primera de la LOPDGDD).

Así mismo, de acuerdo con esa misma DA1ª, en los casos en que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con la de la Administración Pública de origen y se ajustarán también, al Esquema Nacional de Seguridad, regulado mediante Real Decreto 3/2010, de 8 de enero.

En este caso, la Administración Sanitaria informa que se han implementado las medidas del Esquema Nacional de Seguridad y que todas las comunicaciones entre las aplicaciones y los servidores están cifradas. También, que el acceso a los sistemas se realiza mediante VPN cifrada en un sistema militarizado, disponible sólo para un número limitado de personas y que las bases de datos están en un sistema aislado al cual sólo se puede acceder por VPN.

En relación con este principio, y en lo referente a las brechas de seguridad, conviene, igualmente, recordar la obligación impuesta por el artículo 33.1 del RGPD *" En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación".*

Además, y de acuerdo con lo dispuesto en el artículo 34.1 LOPDGDD, cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento debe comunicarla al interesado sin dilación indebida.

**Principio de limitación del plazo de conservación** consagrado en el artículo 5.1. e) del RGPD dispone que *"los datos serán 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…"*.

El Reglamento vincula este principio con la finalidad perseguida, y la app analizada respeta este principio, al señalar que solo se conservarán los datos el tiempo necesario para cumplir con las finalidades perseguidas por la aplicación, y siempre con el límite de un año.

**Principio de responsabilidad proactiva**

El principio de responsabilidad proactiva supone la gran innovación del RGPD, al disponer en su artículo 5.2 que el responsable del tratamiento será responsable del cumplimiento del resto de principios y debe ser capaz de demostrarlo.

A estos efectos es preciso traer a colación dos principios que son manifestación del principio de responsabilidad proactiva; nos referimos a los principios de responsabilidad desde el diseño y por defecto regulados en el artículo 25 del RGPD.

De acuerdo con **el principio de protección de datos desde el diseño**, el responsable del tratamiento aplicará desde el momento inicial, esto es, tanto en el momento de determinar los medios del tratamiento como en el momento del propio tratamiento, las medidas técnicas y organizativas apropiadas, para aplicar de forma efectiva los principios exigidos por el Reglamento y proteger los derechos del interesado. En cuanto al **principio de responsabilidad por defecto,** las medias tanto técnicas como organizativas adoptadas deberán garantizar que por defecto los datos personales no sean accesibles sin la intervención de la persona a un número indeterminado de personas físicas.

En definitiva, el cumplimiento de los principios de protección de datos debe ser tenido en cuenta desde el diseño inicial de la aplicación "COVID-19.eus".

**Evaluación de impacto relativa a la protección de datos**

La evaluación de impacto es uno de los instrumentos que el legislador comunitario ha puesto a disposición de los responsables de tratamiento a fin de que puedan cumplir con el principio de responsabilidad proactiva, que obliga no solo a cumplir las prescripciones del reglamento sino también a estar en disposición de poder acreditar que se cumple.

Esta evaluación se exige en aquellos supuestos en los que sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas, y en esos casos, el responsable del tratamiento deberá evaluar ese impacto antes de iniciar el tratamiento de los datos.

El RGPD detalla una serie de operaciones que precisan en todo caso esa evaluación de impacto, y entre ellas, el tratamiento a gran escala categorías especiales de datos (art. 35.3b) RGPD).

En este caso, dado que la puesta en marcha de la app "COVID-19.eus", puede conllevar un tratamiento a gran escala datos de salud, sería a nuestro juicio necesario que el responsable de la aplicación contase con esa evaluación de impacto, con el contenido exigido por el artículo 35.7 del RGPD. Sin embargo, desconocemos si esa evaluación se ha realizado o no, dado que pese a haberlo solicitado, no se ha remitido a la Agencia información alguna al respecto.

## V
## DATOS DE GEOLOCALIZACIÓN

Además del tratamiento de datos identificativos y de salud, la Administración Sanitaria plantea la posibilidad de utilizar datos de localización GPS, totalmente anonimizados, para detectar por donde ha circulado el usuario de la app, con el fin de establecer un vector de transmisión de la pandemia.

Según la información remitida, estos datos estarían separados de los datos identificativos y de los de carácter clínico asistencial, y en ningún caso se utilizarían para determinar el usuario que se encuentra en su domicilio. La Administración sanitaria señala también que los datos de ubicación no se guardan, ni a día de hoy se están usando, y que para continuar usando la aplicación no es necesario que los usuarios deban aceptar que la aplicación acceda a sus datos de ubicación a través de la geolocalización.

A este respecto, lo primero que hay que destacar es que el uso de datos de teléfonos móviles para luchar contra la propagación del COVID-19 debe garantizar el derecho de las personas a su privacidad. Algunas aplicaciones desarrolladas en países asiáticos permiten a las autoridades rastrear la ubicación de las personas y sus contactos anteriores y verificar el cumplimiento de sus obligaciones de confinamiento, lo que colisiona gravemente con sus derechos.

También en el Estado español, como en toda Europa se están desarrollando numerosas aplicaciones para móviles, tanto públicas y privadas, orientadas a poner freno al COVID-19, y lo que se trata de resolver es en qué condiciones estas herramientas tecnológicas respetarán los derechos individuales de las personas.

La Agencia Vasca de Protección de Datos es consciente de que nos enfrentamos a una situación de emergencia sanitaria donde la prioridad es proteger la salud de la población, y para ello puede ser necesario adoptar algunas medidas limitativas de derechos y libertades.

La Ley Orgánica 3/1986, de 14 de abril, de medidas especiales en materia de salud pública, en su artículo segundo, dispone que "*las autoridades sanitarias competentes podrán adoptar medidas de reconocimiento, tratamiento, hospitalización y control cuando se aprecien indicios racionales que permitan suponer la existencia de un peligro para la salud de la población debido a la situación sanitaria concreta de una persona o grupo de personas o por las condiciones sanitarias en que se desarrolle una actividad*".

Lo que la ley está previendo son medidas dirigidas a una persona o a un grupo de personas, que son adoptadas por la autoridad sanitaria por considerarlas necesarias para la garantizar la salud pública, y que en el supuesto de que impliquen privación o restricción de la libertad o de otro derecho fundamental, precisarán la autorización o ratificación judicial (art. 8.6 LJCA).

Por su parte, el artículo tercero de esta misma Ley Orgánica, dispone lo siguiente: "*Con el fin de controlar las enfermedades transmisibles, la autoridad sanitaria, además de realizar las acciones preventivas generales, podrá adoptar las medidas oportunas para el control de los enfermos, de las personas que estén o hayan estado en contacto con los mismos y del medio ambiente inmediato, así como las que considere necesarias en caso de riesgo de carácter transmisible*".

La Autoridad sanitaria puede adoptar medidas individuales para garantizar la salud pública, pero si lo que se pretende es que esas medidas se apliquen a toda la población, deberán estar previstas en una norma con rango de ley que establezca garantías suficientes para los derechos de las personas.

En ese sentido, decíamos anteriormente, que el RGPD y la LOPDGDD, junto con la Ley Orgánica 3/1986, y las otras leyes sanitarias citadas, dan cobertura suficiente a las autoridades sanitarias para tratar los datos de salud estrictamente necesarios para luchar contra el COVID-19 y proteger la salud de la población.

Lo que plantea ahora la Administración sanitaria, es que la app Covid-19.eus pueda tratar datos relativos a los movimientos de los usuarios de la aplicación, que podrían ser geolocalizados a través del teléfono móvil para detectar por donde han circulado, con el fin de establecer un vector de transmisión de la pandemia.

Según la información remitida a esta Agencia, los datos de localización GPS se utilizarían totalmente anonimizados y, en ningún caso, para determinar si el usuario se encuentra en su domicilio.

La Administración sanitaria señala también en su informe que los datos de ubicación no se guardan, ni a día de hoy se están usando, y que para continuar usando la aplicación no es necesario que los usuarios deban aceptar que la aplicación acceda a sus datos de ubicación a través de la geolocalización.

La primera cuestión que se nos plantea es si realmente los datos de localización GPS que se manejarían serían exclusivamente datos anonimizados.

Según la información remitida, esos datos de localización estarán separados de los datos identificativos y de los de carácter clínico-asistencial.

Es muy importante destacar que no es lo mismo dato anonimizado que seudonimizado. Únicamente podremos hablar de datos anonimizados cuando, en ningún caso, sea posible la vinculación del dato con la persona titular del mismo, es decir, cuando sea imposible volver a identificar a la persona a través de ese dato. Pero si los datos de localización del GPS del móvil de los usuarios de la aplicación se tratan sin los datos identificativos, separados de ellos, pero sin suprimir la vinculación entre los datos, no estaremos ante datos anonimizados sino seudonimizados.

El RGPD introduce en nuestra legislación el término "seudonimización", que lo define en su art. 4.5), como *"el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable"*.

Este proceso consiste en separar la información original, de tal modo que sin volverla a unir o asociarla no es posible identificar a personas físicas. Por lo tanto, efectuando un proceso inverso o reversible a la seudonimización se podría volver a obtener el dato de la persona física identificada. El Reglamento General de Protección de Datos lo asimila a una técnica o medida apropiada para añadir seguridad y confidencialidad a los tratamientos de datos personales, que reduce el vínculo existente entre los datos de carácter personal y la persona a la que identifican, de manera que ya no puede atribuirse a una persona sin utilizar información adicional.

La seudonimización se introduce en el RGPD como una medida para proteger los datos personales, destinada a reducir riesgos para los interesados afectados y a ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de datos (Considerando 28). Sin embargo, debe tenerse presente que, aunque la información seudonimizada no permita la identificación directa del interesado, los datos personales seudonimizados *"deben considerarse información sobre una persona física identificable"* (C. 26 RGPD), luego son datos personales, y como tales, son objeto de protección de la normativa de protección de datos.

Conviene también recordar que el propio proceso de anonimización es un tratamiento de datos plenamente sometido a los principios de protección de datos.

Pero además de lo anterior, en este caso, la protección de datos no sería el único derecho afectado, sino que también se vería afectado el derecho al secreto de las telecomunicaciones, garantizado en el art. 18.3 CE, un derecho que no puede ser limitado durante el estado de alarma, como se deriva de la propia Ley Orgánica 4/81, de 1 de junio, en concreto de su artículo 11.

El tratamiento de los datos de localización de dispositivos móviles se rige por la Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

El artículo 5 de esta Directiva, dedicado a la confidencialidad de las comunicaciones, prohíbe, entre otros tratamientos, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas

distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando dichas personas estén autorizadas legalmente a hacerlo de conformidad con el apartado 1 del artículo15.

Por su parte, el artículo 15.1 de la Directiva, regula los supuestos en los que los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y obligaciones que se establecen entre otros, en el artículo 5 de la Directiva, cuando tal limitación constituya una medida necesaria, proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional, la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos.

De acuerdo con ese artículo 15.1 de la Directiva, el tratamiento de datos de geolocalización no podría ampararse en razones de interés público en el ámbito de la salud pública, que no se incluyen en ese precepto, y por lo tanto, tampoco en los artículos 6.1e) y 9.2i) del RGPD, ni en el artículo tercero de la citada Ley Orgánica 3/1986, de 14 de abril, de medidas especiales en materia de salud pública.

**EN CONCLUSIÓN**, como regla general, los datos de localización sólo podrán tratarse previo consentimiento de los usuarios, y esa manifestación de voluntad tendrá que cumplir todas las exigencias establecidas en el RGPD para su validez como base legitimadora del tratamiento (libre, específica, informada e inequívoca por la que el interesado acepta mediante una clara acción afirmativa, el tratamiento de esos datos personales), consentimiento que el interesado tendrá derecho a retirar en cualquier momento. Obviamente, no sería preciso ese consentimiento si se manejasen datos totalmente anónimos.

Pero la cuestión no sólo estriba en la necesidad de consentimiento de los afectados, sino en determinar si la geolocalización es una medida necesaria y proporcionada para lograr los objetivos pretendidos por la app COVID-19.eus, y la respuesta debe encontrase en las recomendaciones, orientaciones y directrices emitidas por la Comisión Europea y el Comité Europeo de Protección de Datos.

Nos referimos concretamente a la **Recomendación (UE) 2020/518, de la Comisión, de 8 de abril, de 2020**, **relativa a un conjunto de instrumentos comunes de la Unión para la utilización de la tecnología y los datos a fin de combatir y superar la crisis del Covid-19, en particular por lo que respecta a las aplicaciones móviles y a la utilización de datos de movilidad anonimizados.**

Esta Recomendación, que recoge gran parte de las consideraciones realizadas en marzo de este año tanto por el Comité Europeo de Protección de Datos, como por el Supervisor Europeo de Protección de Datos, establece los principios generales que deben guiar el desarrollo de un enfoque común para la utilización de tecnologías y datos digitales en respuesta a la crisis actual, centrando la atención en dos aspectos:

1.- Un enfoque coordinado paneuropeo para el uso de aplicaciones móviles, coordinado a nivel de la Unión, con el fin de capacitar a los ciudadanos para adoptar medidas de distanciamiento social eficaces y más específicas, así como con el fin de alertar, prevenir y hacer un seguimiento de contactos, con miras a limitar la propagación de la enfermedad COVID-19.

2.- Un plan común para el uso de datos anonimizados y agregados sobre la movilidad de la población a fin de modelizar y predecir la evolución de la enfermedad, controlar la eficacia

de la toma de decisiones de las autoridades de los Estados miembros en lo referente a medidas como el distanciamiento social y el confinamiento, y obtener información de cara a una estrategia coordinada para la salida de la crisis de la COVID-19.

La Comisión sostiene que lo primordial en todo proceso para el desarrollo de los instrumentos para el uso de la tecnología y los datos, debe ser el respeto de los derechos fundamentales, especialmente la privacidad y la protección de datos, la prevención de la vigilancia y la estigmatización, y para lograrlo se deberá: - limitar el tratamiento de datos personales a la finalidad de combatir el COVID-19; - revisar periódicamente la necesidad del tratamiento de datos, y garantizar que cuando el tratamiento ya no sea estrictamente necesario se pondrá fin al mismo y se destruirán los datos.

La Comisión mantiene que el enfoque paneuropeo exige especificaciones para garantizar la eficacia de las aplicaciones móviles de información, alerta y seguimiento, desde el punto de vista técnico; exige medidas para prevenir la proliferación de aplicaciones incompatibles con el Derecho de la Unión; la identificación de buenas prácticas y mecanismos para el intercambio de información sobre el funcionamiento de las aplicaciones, y exige compartir datos con organismos epidemiológicos públicos pertinentes e instituciones de investigación sobre salud pública. Además, considera la Comisión que se debe asegurar la interoperabilidad de las aplicaciones cuando se prevean escenarios transfronterizos.

En lo referente a las app móviles de advertencia y prevención del COVID-19, alude la Comisión a que es necesario garantizar el respeto de los derechos fundamentales y evitar la estigmatización; a la preferencia por las medidas menos intrusivas pero efectivas (por ej. datos de proximidad) y tecnologías adecuadas (por ej. Bluetooth de baja energía); a la necesidad de aplicar técnicas de encriptación y al almacenamiento de datos en el dispositivo móvil; y a que se debe evitar el tratamiento de datos de localización, y utilizar datos anónimos y agregados cuando sea posible. Apunta también la Comisión la necesidad de transparencia en la configuración de la privacidad, no sólo como obligación en materia de protección de datos, sino también como forma de generar confianza en la ciudadanía, y que es preciso eliminar los datos personales cuando la pandemia esté bajo control.

Esta recomendación está disponible en el siguiente enlace:

https://ec.europa.eu/digital-single-market/en/news/coronavirus-recommendation-use-mobile-data-response-pandemic.

En esta Recomendación la Comisión Europea anunció que iba a publicar unas orientaciones adicionales, especialmente en lo relativo a las consecuencias del uso de las aplicaciones para la intimidad y la protección de datos personales en este ámbito, y finalmente, el pasado 17 de abril, se publicó en el Diario Oficial de la Unión Europea **la Comunicación de la Comisión con orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de COVID-19 en lo referente a la protección de datos** (2020/C 124 I/01).

Estas orientaciones se elaboran teniendo en cuenta la contribución del Comité Europeo de Protección de Datos, y determinan las características y los requisitos que deberían reunir las aplicaciones para asegurar el cumplimiento de la legislación de la UE en materia de privacidad y protección de datos, en particular del RGPD y la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, sobre privacidad y comunicaciones electrónicas (DO L 201 de 31.7.2002).

Se trata de orientaciones que no son jurídicamente vinculantes, y se entienden sin perjuicio del papel del Tribunal de Justicia de la UE, que es la única institución que puede interpretar de manera preceptiva el Derecho de la UE.

Estas orientaciones se refieren a aplicaciones de carácter voluntario para la lucha contra el COVID-19, que tengan una o varias de las funcionalidades siguientes: Informar a las personas sobre la pandemia; ofrecer cuestionarios de autoevaluación y orientación; alertar a las personas que han estado cerca de una persona infectada o proporcionar un foro de comunicación entre médicos y pacientes

Los requisitos que entiende la Comisión necesarios para garantizar que los ciudadanos de la UE confíen en estas aplicaciones y las usen sin reservas serían las siguientes:

- Las autoridades sanitarias deberían ser los responsables del tratamiento.
- Los usuarios deben mantener el control de sus datos personales, por ello:
    - La instalación de la aplicación debe sea voluntaria, sin consecuencias negativas para quienes decidan no descargar o usar la aplicación.
    - El usuario debería poder dar su consentimiento a cada funcionalidad de la app de forma independiente, ya que la finalidad del tratamiento será distinta para cada una de ellas.
    - Cuando sea necesario atender a fines como los de investigación científica y fines estadísticos, deberían incluirse en la lista original de fines y comunicarse claramente a los usuarios.
    - Si se utilizan datos de proximidad, deberían ser almacenados en el dispositivo del usuario y compartirse con las autoridades sanitarias sólo cuando se confirme que la persona está infectada y siempre con su consentimiento.
    - Las autoridades sanitarias deben proporcionar a los usuarios toda la información necesaria en relación con el tratamiento de sus datos (artículos 12 y 13 del RGPD y artículo 5 de la Directiva sobre privacidad y comunicaciones electrónicas).
    - Los usuarios de la app podrán ejercer sus derechos de acuerdo con el RGPD y toda restricción de esos derechos además de necesaria y proporcionada, deberá estar legalmente prevista.
    - Las aplicaciones deberían desactivarse, a más tardar, cuando la pandemia esté controlada. La desactivación no debería depender de la desinstalación del usuario.
- El tratamiento de datos amparado por el interés público en el ámbito sanitario requiere de una ley que recoja las medidas específicas y adecuadas para salvaguardar los derechos y libertades de los titulares de los datos, pero las personas siguen siendo libres para decidir si instalan la aplicación y si comparten sus datos con las autoridades sanitarias, Por tanto, si el usuario se desinstala la aplicación, ello no podrá tener consecuencias negativas para él.

- Las aplicaciones deben tratar exclusivamente los datos personales que sean adecuados, pertinentes y estrictamente necesarios para los fines perseguidos (principio de minimización).
    - Si las apps son sólo de información, no necesitan tratar dato personal alguno.
    - Si la funcionalidad es la comprobación de síntomas o la telemedicina, no se requiere acceder a la lista de contactos del propietario del dispositivo.
    - Si la funcionalidad es de rastreo de contactos y alertas, y a efectos de medir la proximidad y los contactos estrechos con una persona contagiada, y minimizar el riesgo de falsos negativos, se insiste en la conveniencia de emplear tecnologías como Bluetooth, que proporcionan una evaluación más precisa de los contactos entre las personas, frente a otras tecnologías como el uso de los datos de geolocalización ( GNS/GPS o datos de localización de dispositivos móviles), que no resultan tan precisas.
    - **La Comisión Europea considera que los datos de localización no son necesarios para el rastreo de contactos, y aconseja no utilizarlos en este contexto**, ya que su objetivo no es ni seguir los movimientos de las personas ni controlar el cumplimiento de las restricciones acordadas
    - Únicamente deberían generarse y tratarse datos de proximidad si existiera un riesgo real de infección en función de la cercanía y duración del contacto.
    - Resultaría más acorde con el principio de minimización que los identificadores de las personas infectadas se almacenasen en sus propios dispositivos, y no en un servidor al que tengan acceso las autoridades sanitarias. (el denominado “tratamiento descentralizado”).
    - La identidad de la persona infectada no debería revelarse a aquellas personas con las que hubiera estado en contacto (bastaría con que se les comunicase que han estado en contacto con una persona infectada), así como tampoco deberían almacenarse los datos sobre el momento y el lugar de dichos contactos.
    - La app debe alertar a esas personas que han estado en contacto estrecho con una persona infectada tras su confirmación por la autoridad sanitaria.
- Es preciso garantizar la seguridad de los datos, y para lograrlo se recomienda que los datos se almacenen en el dispositivo terminal del usuario y estén cifrados mediante técnicas criptográficas avanzadas. En caso de que se almacenen en un servidor central, el acceso al servidor, incluido el acceso administrativo, debería estar sujeto a registro previo.
- Los datos de proximidad sólo deberían generarse y almacenarse en el dispositivo terminal de la persona en formato cifrado y seudonimizado. Para garantizar que se excluya el rastreo por terceros, la activación de Bluetooth debería ser posible sin tener que activar otros servicios de localización.
- La Comisión recomienda que el código fuente de la aplicación se haga público y esté disponible para su revisión.
- Todas las transmisiones desde el dispositivo personal a las autoridades sanitarias deberían cifrarse.

- Cuando la legislación nacional establezca que los datos recogidos también puedan tratarse con fines de investigación científica, se debería utilizar, en principio, la seudonimización.
- Los datos personales no deben conservarse más tiempo del necesario.
- Las autoridades de protección de datos deben participar y ser consultadas en el desarrollo de las aplicaciones y seguir su despliegue.

**Comité Europeo de Protección de Datos**

Con fecha 21 de abril de 2020, el Comité Europeo de Protección de Datos ha adoptado las **Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto del brote de COVID-19**.

En estas Directrices se establecen los siguientes principios:

1.Los datos de localización deben usarse para apoyar la respuesta a la pandemia mediante la modelización de la propagación del virus, a fin de evaluar la eficacia global de las medidas de confinamiento;

2.El rastreo de contactos, tiene como objetivo informar a las personas que hayan estado muy cerca de alguien que sea portador confirmado del virus, a fin de romper las cadenas de transmisión lo antes posible.

En cuanto a las fuentes de datos de localización**,** el Comité recuerda que el tratamiento de los datos de localización obtenidos de los proveedores de servicios de comunicaciones electrónicas está sujeto a los límites de los artículos 6 y 9 de la Directiva sobre la privacidad y las comunicaciones electrónica, lo que significa que los datos sólo pueden ser transmitidos a las autoridades o a terceros después de haber sido anonimizados por el proveedor, o en el caso de los datos que indican la posición geográfica del equipo terminal de un usuario, que no son datos de tráfico, si cuenta con el consentimiento previo de los usuarios.

En cuanto a la información, incluidos los datos de localización, obtenida directamente de los equipos terminales, es de aplicación el artículo 5, apartado 3 de la Directiva, por lo que el almacenamiento de información en el dispositivo del usuario o el acceso a la información ya almacenada sólo se permite con su consentimiento y/o cuando sea estrictamente necesario para la prestación del servicio de la sociedad de la información expresamente solicitado por el usuario. Las excepciones sólo son posibles de conformidad con el artículo 15 de esa Directiva sobre la privacidad y las comunicaciones electrónicas.

El CEPD considera que se debe priorizar el tratamiento de datos de localización anonimizados, en lugar de datos personales. Señala que el concepto de anonimización suele confundirse con la seudonimización, y aclara que la anonimización permite utilizar los datos sin ninguna restricción, mientras que los datos seudonimizados siguen estando sujetos al RGPD, y recuerda que, aunque existen muchas opciones para una anonimización eficaz, no se pueden anonimizar datos aislados, sino series de datos completas. Señala también que los datos de localización son difíciles de anonimizar, y que los rastros de movimientos en determinadas circunstancias

pueden ser vulnerables a los intentos de reidentificación. Se recuerda igualmente que un único patrón de datos que rastree la localización de una persona durante un tiempo significativo no puede ser anonimizado por completo y, por último, se recomienda la transparencia respecto a la metodología de anonimización.

En cuanto a las aplicaciones de rastreo de contacto, el CEPD considera que estas apps tienen que ser voluntarias y deben limitarse a la contención del COVID-19. Estas aplicaciones no requieren un seguimiento de la ubicación de los usuarios a título individual; en su lugar, deben utilizarse datos de proximidad. Como se trata de aplicaciones que pueden funcionar sin la identificación directa de las personas, deben establecerse medidas para evitar la reidentificación. Además, la información debe alojarse en el equipo terminal el usuario y solo debe recogerse la que sea absolutamente necesaria.

El Comité, al igual que la Comisión Europea, nos recuerda que el hecho de que la app sea voluntaria no significa que el tratamiento tenga que ampararse en el consentimiento. La base jurídica que legitima el tratamiento de datos por razones de interés público en el ámbito sanitario debe recogerse en una ley que establezca las garantías específicas para salvaguardar los derechos de las personas.

El uso de las apps debe limitarse estrictamente a la contención de la crisis de COVID-19 y no debería permitirse su ampliación a otros fines. Los datos personales deben conservarse únicamente durante la duración de la crisis, después, como regla general, todos los datos personales deben ser borrados o anonimizados.

Las apps de contacto no pueden sustituir el rastreo manual de contactos realizado por personal sanitario cualificado. Los algoritmos deben estar sometidos a una estricta supervisión.

El código fuente de la aplicación debe hacerse público.

El CEPD recomienda que antes de empezar a utilizar una aplicación de este tipo ha de llevarse a cabo una evaluación de impacto relativa a la protección de datos, porque el tratamiento puede entrañar un alto riesgo.

Al diseñar las aplicaciones, deberían tenerse en cuenta ciertas recomendaciones y requisitos funcionales:

- Los datos objeto de tratamiento deben reducirse a los mínimos estrictamente necesarios.

- Los datos difundidos por las aplicaciones deben incluir únicamente algunos identificadores únicos y seudónimos, generados por la aplicación y específicos de esta.

- Las aplicaciones de rastreo de contactos pueden seguir un enfoque centralizado o descentralizado, pero con preferencia por el segundo.

- Todo servidor que participe en el rastreo de contactos debe limitarse a recoger el historial de contactos o los identificadores seudónimos de un usuario que haya sido diagnosticado como infectado como resultado de una evaluación adecuada por las autoridades sanitarias y de una acción voluntaria del usuario. Como alternativa, el servidor debe conservar una lista de identificadores seudónimos de usuarios infectados o su historial de contactos

únicamente durante el tiempo necesario para informar de su exposición a los usuarios que puedan haber sido infectados, sin tratar de identificarles.

- Se deben aplicar las técnicas criptográficas más avanzadas para garantizar la seguridad de los datos almacenados.

- La notificación de los usuarios como infectados por el virus COVID-19 en la aplicación debe estar sujeta a la debida autorización.

- Cierta información debe permanecer en el terminal del usuario y sólo debe procesarse cuando sea estrictamente necesario y con su consentimiento previo y específico.

- Se debe facilitar una información clara y explícita sobre el enlace que permita descargar la app oficial.

Estas directrices están disponibles en el siguiente enlace:

https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_en

También **el Parlamento Europeo**, en Resolución de 17 de abril de 2020, ha establecido unos criterios para una respuesta unitaria ante la crisis del Covid-19, y en relación con el desarrollo de aplicaciones móviles para rastreo y/ o diagnóstico del Covid-19, establece que esas aplicaciones no pueden ser obligatorias y que los datos generados a partir del uso de la aplicación no pueden ser almacenados en bases de datos centralizadas, que según sus palabras, presentan un riesgo potencial de abuso y falta de confianza. Establece también la resolución que debe informarse de manera clara a la población sobre el uso de apps de localización de contactos, y publicarse el código fuente (transparencia); y que los datos de localización móvil sólo pueden tratarse de conformidad con la Directiva sobre la privacidad y las comunicaciones electrónicas y el RGPD.

Por su parte, el Supervisor Europeo de Protección de Datos (SEPD) en una carta abierta sobre apps y coronavirus publicada recientemente, ha advertido sobre los riegos para la privacidad que existen, y de la necesidad de que las aplicaciones lo sean de código abierto a fin de que, más allá del cumplimiento formal de la normativa, puede supervisarse todo el procedimiento técnico de captación y tratamiento de datos.

https://edpb.europa.eu/sites/edpd/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

**EN CONCLUSIÓN**, no hay duda que las herramientas tecnológicas son gran ayuda para combatir el Covid-19 y para el conjunto de la sociedad, y que las herramientas basadas en la localización y el control de proximidad pueden ser de utilidad para controlar la pandemia, para predecir su posible evolución y abordar los focos infecciosos que se vayan produciendo, pero todas estas herramientas deberán estar construidas en el marco de una arquitectura absolutamente respetuosa con los derechos de privacidad de las personas, donde la protección de datos esté garantizada desde su diseño. Por ello, es necesario evitar la adopción de medidas que se adentren profundamente en las garantías esenciales del derecho a la protección de datos, contrariando los estándares de protección fijados por la Unión Europea.

Para finalizar este informe debemos referirnos a dos cuestiones más:

## RESPONSABLE Y ENCARGADO DEL TRATAMIENTO

Los conceptos de encargado y responsable del tratamiento son elementos troncales del derecho fundamental.

El responsable del tratamiento se define en el artículo 4.7) del RGPD como "*la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento".*

El encargado se define en el apartado 8 de este artículo 4, como *"la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento*".

En este caso la Dirección de Salud Pública y Adicciones del Departamento de Salud actúa como responsable del tratamiento de los datos, mientras que MAM OBJECTS, S.L. interviene como encargado del tratamiento de los datos.

Según la información remitida, Erictel es la empresa matriz de MAM OBJECTS, S.L., Owasys y Trelec. y es, además, el nombre comercial que se usa para la empresa MAM OBJECTS, S.L., que es la empresa que está detrás de la solución tecnológica en colaboración con el Gobierno Vasco, desarrolla la misma y hace su mantenimiento, y por ello es la encargada del tratamiento.

De conformidad con la normativa de protección de datos, esa empresa tendrá esa consideración, siempre y cuando realice los tratamientos por cuenta de la Administración responsable, y se cumplan las exigencias establecidas en el artículo 28 del RGPD y en el artículo 33 de la LOPDGDD.

En todo caso, el contrato, o negocio jurídico donde se articule el encargo del tratamiento de datos (que no ha sido remitido a esta Agencia), deberá incluir los requisitos propios de un encargo de tratamiento de datos, (objeto, duración y naturaleza; finalidad del tratamiento o tratamientos que se autorizan; tipo de datos personales y categorías de interesados y las obligaciones y derechos del responsable, exigidos en el artículo 28.3 del RGPD, entre ellos, las instrucciones documentadas del responsable; el compromiso de confidencialidad; las medidas de seguridad, que en este caso serán las correspondientes del Esquema Nacional de Seguridad, el régimen de subcontratación, en su caso, y el destino de los datos al finalizar la prestación.

La última consideración de este dictamen, se refiere a una obligación formal del responsable de la app.

## INCLUSIÓN EN EL REGISTRO DE ACTIVIDADES DE TRATAMIENTO

El Reglamento General de Protección de Datos elimina la obligación de creación y declaración de ficheros y la sustituye por el denominado "registro de las actividades de tratamiento", regulando su contenido en el artículo 30.

Cada responsable del tratamiento está obligado a llevar un registro de todas las actividades de tratamiento efectuadas bajo su responsabilidad, con toda la información exigida en el artículo 30.1 RGPD.

Del mismo modo, cada encargado llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable, con el contenido exigido por el artículo 30.2 RGPD.

Además de lo anterior, es necesario recordar que la Disposición Final Undécima de la LOPDGDD ha modificado la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y buen gobierno, introduciendo un artículo 6 bis, que obliga a las Administraciones Públicas a publicar su inventario de actividades de tratamiento.

Estas son las consideraciones que realiza la Agencia Vasca de Protección de Datos en relación con la app COVID-19.eus.

En Vitoria-Gasteiz, a 5 de junio de 2020