

- **Procedimiento N°: E/03771/2020**

940-0419

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 27 de abril 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 la Web/app “*****WEB/APP.1**”, de la que es responsable el Departamento de Salud del Gobierno de Navarra, con el fin de determinar si de tales hechos se desprendieran indicios de infracción en el ámbito competencial de la Agencia Española 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:

1. Con fecha 28 de abril de 2020 se requiere al Departamento de Salud del Gobierno de Navarra información y documentación sobre la web/app “*****WEB/APP.1**”. Se obtiene respuesta en los siguientes términos:

*1.1. *****WEB/APP.1** es un proyecto llevado a cabo por el Servicio Navarro de Salud-Osasunbidea (SNS-O) con la finalidad de reducir el volumen de llamadas al número de emergencias sanitarias que trata las dudas sobre la enfermedad infecciosa COVID-19, tranquilizar a la población, permitir un triaje inicial de posibles casos y un seguimiento posterior.*

1.2. Para lograr la finalidad anteriormente mencionada, se tratan las siguientes categorías de datos en fases diferenciadas:

Fase I: a todos los usuarios al darse de alta en la APP se les solicitan las siguientes categorías de datos: Número de teléfono móvil, DNI/NIE o CIPNA (nº tarjeta individual sanitaria), Comunidad Autónoma, Edad y Género.

Fase II: cuando el resultado del test es de “posible positivo”, se tratan las siguientes categorías de datos: Nombre y Apellidos, E-mail de contacto (opcional), Dirección completa, Datos de salud relacionados con los síntomas que rellena el usuario al realizar el test (Resultado del test (posible positivo / posible negativo), Sensación de falta de aire (Si / No), Fiebre de +37.7°C (Si / No), tos seca (Si / No), dolor de cabeza (Si / No), diarrea (Si / No), dolores musculares (Si / No), dolor de garganta (Si / No), pérdida de gusto u olfato (Si / No), síntomas repentinos (Si / No).

Fase III: si el resultado del test es de “posible positivo”, se le ofrece al usuario realizar seguimiento tratando los siguientes datos: Resultado de Seguimiento Positivo/Negativo y Temperatura corporal.

Fase IV: si el usuario se registra como “contacto estrecho” se tratan los siguientes datos realizando un seguimiento: Resultado del test (posible positivo / posible negativo), temperatura corporal y fecha último contacto. No se almacenan datos de ubicación/geolocalización.

1.3. Los datos recabados serán conservados mientras dure el actual escenario sanitario relacionado con el COVID-19. Los datos serán integrados con la Historia Clínica de Atención Primaria únicamente cuando el resultado del test es de “posible positivo”. En este caso se genera una citación automática en la agenda del Centro de Salud previa confirmación de que el usuario está de acuerdo con la notificación a su centro para que le llamen. Previamente se ha informado al usuario de esta posibilidad.

*1.4. Respecto a las terceras entidades intervinientes en los tratamientos, a pesar de que se indique en la Política de Privacidad publicada que “la utilización de *****WEB/APP.1** implica dar acceso a tus datos a terceros como proveedores y Colaboradores, así como a las empresas que estos subcontraten”, a fecha de hoy no existen estas cesiones de datos ni se encuentran previstas.*

1.5. Respecto al cumplimiento de los principios de protección de datos se indica lo siguiente:

Limitación de la finalidad: los datos personales recabados se utilizan únicamente cuando el usuario acepta recibir una cita previa en su centro de salud siempre que el triaje inicial según su sintomatología refleje un “posible positivo”.

Minimización de datos:

- *Datos identificativos: son los mínimos necesarios para integrarlos en el sistema de citas de la Historia Clínica de Atención Primaria.*
- *Datos de salud: el triaje está basado en un test de preguntas definido por el personal especializado del Instituto de Salud Pública y Laboral de Navarra y de Atención Primaria, intentando minimizar la cantidad de información clínica necesaria para la finalidad indicada.*

*1.6. Manifiestan que la App ha pasado satisfactoriamente dos auditorías de seguridad realizadas por personal especializado de la Dirección General de Transformación Digital del Gobierno de Navarra. Con estas pruebas (tanto automáticas como manuales) se pretendía detectar vulnerabilidades tanto de desarrollo como de infraestructura, que puedan comprometer la aplicación y los datos facilitados por el paciente. Para las pruebas automáticas se han utilizado herramientas comerciales como *****HERRAMIENTAS.1** y éstas se han visto reforzadas por pruebas manuales de manipulación de peticiones e inspección de respuestas*

1. *Aportan un documento de análisis de riesgos y evaluación de impacto, en el que figuran, entre otros aspectos, el ciclo de vida del tratamiento y se definen 39 escenarios de riesgos en base a los artículos de obligado cumplimiento de Reglamento General de Protección de Datos, asociando a cada escenario de riesgo tres grupos de activos: Personal, Hardware, Software y Equipamiento de Infraestructuras. Asimismo, se han establecido las medidas que se van a tomar sobre aquellos riesgos que en el análisis de riesgos de datos personales superan el valor definido del riesgo asumido.*

2. *Del análisis realizado por la Inspección de Datos sobre la aplicación móvil “**APP.1**” y sobre la página web “**URL.1**”:*

*La conexión web al sitio “**URL.1**” se realiza mediante el protocolo cifrado https, con certificado electrónico emitido por Digicert SHA2 Secure Server CA. Al acceder a dicha web, se comprueba que ofrece información sobre la situación actualizada de contagios y la opción de “Hacer test”. Si se selecciona esta opción ofrece la posibilidad de realizar el test para valorar si puede estar infectado de COVID-19. Para hacer el test es necesario aceptar las condiciones de uso e introducir un número de teléfono. Examinada la App de Android se comprueba que solamente pide permiso para acceder al almacenamiento y conexiones de red. No pide permisos para acceder a la geolocalización.*

Una vez instalada, se comprueba que ofrece información sobre la situación actual de contagios y las opciones “Hacer test” y “Soy un contacto estrecho”. Si se selecciona una de estas dos opciones ofrece la posibilidad de realizar el test para valorar si puede estar infectado de COVID-19. Para hacer el test es necesario aceptar las condiciones de uso e introducir un número de teléfono.

3. *El día 11 de noviembre de 2020 se ha verificado por la inspección de datos que se ha actualizado la política de privacidad tanto de la app como del servicio web, quedando de la siguiente manera:*

- Las aplicaciones han sido concebidas con objeto de reducir el volumen de llamadas al número de emergencias sanitarias que atienden los casos de COVID-19, tranquilizar a la población y permitir un triaje.
- La utilización de las aplicaciones implica la aceptación de las condiciones de uso.
- Para utilizar los servicios es necesario estar registrado como usuario, para lo cual es obligatorio facilitar unos datos básicos y verificar el número de teléfono móvil. Los datos que se han de facilitar son:
 - Nombre y apellidos
 - N° de teléfono móvil
 - DNI
 - N° tarjeta sanitaria

- • Edad
- • Email de contacto
- • Dirección postal
- Datos de salud relacionados con los síntomas experimentados.
- El uso de la aplicación es libre, gratuita y voluntaria, estando permitido su uso solamente a mayores de 16 años o contar con el consentimiento de los padres o tutores.
- La conexión con la plataforma está cifrada.
- Los usuarios pueden darse de baja de la plataforma comunicándolo vía email a la dirección que indican.
- Informan de que los datos serán incorporados a los tratamientos ya existentes de “Control y Gestión” del Departamento de salud. Informan sobre la identidad y dirección postal del responsable de los tratamientos (Departamento de Salud del Gobierno de Navarra).
- Los datos recogidos por *****WEB/APP.1** son estrictamente necesarios por razones de interés público ante la actual situación de emergencia sanitaria decretada por las Autoridades Públicas como consecuencia de la pandemia del COVID.19 y la necesidad de su control y propagación, así como para proteger y salvaguardar un interés esencial para tu vida y/o la de terceros.
- Los datos pueden ser accedidos por los profesionales sanitarios para ponerse en contacto con el interesado en caso de que el resultado de la autoevaluación realizada a través de la aplicación se determine la necesidad de atención médica ante la posibilidad de estar infectado por el coronavirus.
- No existen cesiones de datos.
- No existen transferencias internacionales de datos.
- Informan de los derechos de acceso, rectificación, supresión, limitación, oposición. Se hace referencia igualmente a la retirada del consentimiento prestado. Indican que los derechos pueden ejercitarse ante el Departamento de Salud de Navarra, *****DIRECCIÓN.1**. Señalan igualmente una dirección de correo electrónico para ejercer los derechos *****EMAIL.1**.
- Además, informan de que si no son atendidos correctamente pueden solicitar la tutela de la Agencia Española de Protección de Datos.
- Informan de que la conservación de los datos se prevé mientras dure el actual estado sanitario relacionado con el COVID-19.

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 razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

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

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

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

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 que el artículo 53 de la Ley Orgánica 13/1982, de 10 de agosto, de reintegración y mejoramiento del Régimen Foral de Navarra, atribuye a dicha Comunidad Autónoma en materia de sanidad y las encomendadas al Departamento de Salud del Gobierno de Navarra por la Ley Foral 10/1990, de 23 de noviembre, de Salud.

En lo que al principio de finalidad respecta, recogido en la letra b del artículo 5.1 del RGPD, la información facilitada por el Servicio Navarro de Salud indica que la finalidad es la de “reducir el volumen de llamadas al número de emergencias sanitarias que trata las dudas sobre la enfermedad infecciosa COVID-19, tranquilizar a la población, permitir un triaje inicial de posibles casos y un seguimiento posterior.” Asimismo, se indica que “los datos personales recabados se utilizan únicamente cuando el usuario acepta recibir una cita previa en su centro de salud siempre que el triaje inicial según su sintomatología refleje un “posible positivo”.

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 se solicitan en diferentes fases, así en la primera se solicita a todos los usuarios determinados datos identificativos: Número de teléfono móvil, DNI/NIE o CIPNA (nº tarjeta individual sanitaria), Comunidad Autónoma, Edad y Género. En una segunda fase, cuando el resultado del test es de “posible positivo”, se tratan más datos identificativos (Nombre y Apellidos, E-mail de contacto (opcional), Dirección completa) y los datos de salud relacionados con los síntomas que rellena el usuario al realizar el test: Resultado del test (posible positivo / posible negativo), Sensación de falta de aire (Si / No), Fiebre de +37.7°C (Si / No), tos seca (Si / No), dolor de cabeza (Si / No), diarrea (Si / No), dolores musculares (Si / No), dolor de garganta (Si / No), pérdida de gusto u olfato (Si / No), síntomas repentinos (Si / No). En una tercera fase, si el resultado del test es de “posible positivo”, se le ofrece al usuario realizar seguimiento tratando los si-

guientes datos: Resultado de Seguimiento Positivo/Negativo y Temperatura corporal. Por último, si el usuario se registra como “contacto estrecho” se tratan los siguientes datos realizando un seguimiento: Resultado del test (posible positivo / posible negativo), temperatura corporal y fecha último contacto. En la documentación aportada se aclara que no se almacenan datos de ubicación o geolocalización.

En la documentación aportada se aclara que los datos identificativos objeto de tratamiento son *“los mínimos necesarios para integrarlos en el sistema de citas de la Historia Clínica de Atención Primaria”*. En lo que respecta a los datos de salud se expone que: *“el triaje está basado en un test de preguntas definido por el personal especializado del Instituto de Salud Pública y Laboral de Navarra y de Atención Primaria, intentando minimizar la cantidad de información clínica necesaria para la finalidad indicada.”*

El artículo 5.1.e) recoge el principio de limitación del plazo de conservación, respecto del cual en la aludida documentación se señala que: *“Los datos recabados serán conservados mientras dure el actual escenario sanitario relacionado con el COVID-19. Los datos serán integrados con la Historia Clínica de Atención Primaria únicamente cuando el resultado del test es de “posible positivo”. En este caso se genera una cita automática en la agenda del Centro de Salud previa confirmación de que el usuario está de acuerdo con la notificación a su centro para que le llamen. Previamente se ha informado al usuario de esta posibilidad.”*

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, se declara en la documentación facilitada que *“la App ha pasado satisfactoriamente dos auditorías de seguridad realizadas por personal especializado de la Dirección General de Transformación Digital del Gobierno de Navarra. Con estas pruebas (tanto automáticas como manuales) se pretendía detectar vulnerabilidades tanto de desarrollo como de infraestructura, que puedan comprometer la aplicación y los datos facilitados por el paciente. Para las pruebas automáticas se han utilizado herramientas comerciales como **HERRAMIENTAS.1** y éstas se han visto reforzadas por pruebas manuales de manipulación de peticiones e inspección de respuestas.”*

De todo ello cabe concluir que el tratamiento de datos efectuado mediante la aplicación móvil **APP.1**, con las finalidades explícitas y determinadas señaladas en su contestación al requerimiento de información formulado por esta Agencia, se encontraría legitimado en lo previsto en los artículos 9 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, 53 de la Ley Orgánica 13/1982, de 10 de agosto, de reintegración y mejoramiento del Régimen Foral de Navarra y las previsiones de la Ley Foral 10/1990, de 23 de noviembre, de Salud. Los datos a tratar se encuentran limitados a los adecuados y pertinentes para los fines declarados. Asimismo, la conservación de los datos obtenidos a través de la app se limita a la duración del actual escenario relacionado con la Covid-19, sin perjuicio de que los datos que deban integrarse en la historia clínica queden sujetos a los plazos legales fijados para la conservación de los mismos en su normativa específica. Por último, 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.”*

Por su parte, la LOPDGDD en su Título III, tal y como señala la exposición de motivos de dicha Ley *“adapta al Derecho español el principio de transparencia en el tratamiento del reglamento europeo, que regula el derecho de los afectados a ser informados acerca del tratamiento y recoge la denominada «información por capas» ya generalmente aceptada en ámbitos como el de la videovigilancia o la instalación de dispositivos de almacenamiento masivo de datos (tales como las «cookies»), facilitando al afectado la información básica, si bien, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.”*

A este respecto, el artículo 11 de la LOPDGDD prevé lo siguiente:

“1. Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

2. La información básica a la que se refiere el apartado anterior deberá contener, al menos:

- a) La identidad del responsable del tratamiento y de su representante, en su caso.*
- b) La finalidad del tratamiento.*
- c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.*

Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679.”

Se verifica que las condiciones generales aplicables tanto a la web como a la aplicación *****APP.1**, informan sobre la identidad y dirección postal del responsable de los tratamientos (Departamento de Salud del Gobierno de Navarra), de las categorías de datos objeto de tratamiento (Nombre y apellidos, nº de teléfono móvil, DNI, nº tarjeta sanitaria, edad, género, e-mail de contacto, dirección postal, datos de salud relacionados con los síntomas experimentados); de las finalidades del tratamiento (reducir el volumen de llamadas al número de emergencias sanitarias que atienden los casos de COVID-19, tranquilizar a la población y permitir un triaje); de la base jurídica del tratamiento (interés público y salvaguarda de un interés esencial para la vida del interesado o de terceros). Se informa sobre los destinatarios de los datos

(profesionales sanitarios), del período de conservación de los datos, de la posibilidad de ejercicio de los derechos de acceso, rectificación, supresión, limitación, oposición y el derecho a retirar el consentimiento prestado. Se facilita una dirección de correo electrónico para ejercitar los derechos. 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.

VI

Por lo tanto, del examen de la documentación aportada relativa a la aplicación oficial **APP.1**, del Departamento de Salud del Gobierno de Navarra, entidad responsable del tratamiento, no se desprenden indicios racionales de infracción de la normativa sobre protección de datos personales analizada en los párrafos anteriores.

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 al Departamento de Salud del Gobierno de Navarra.

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