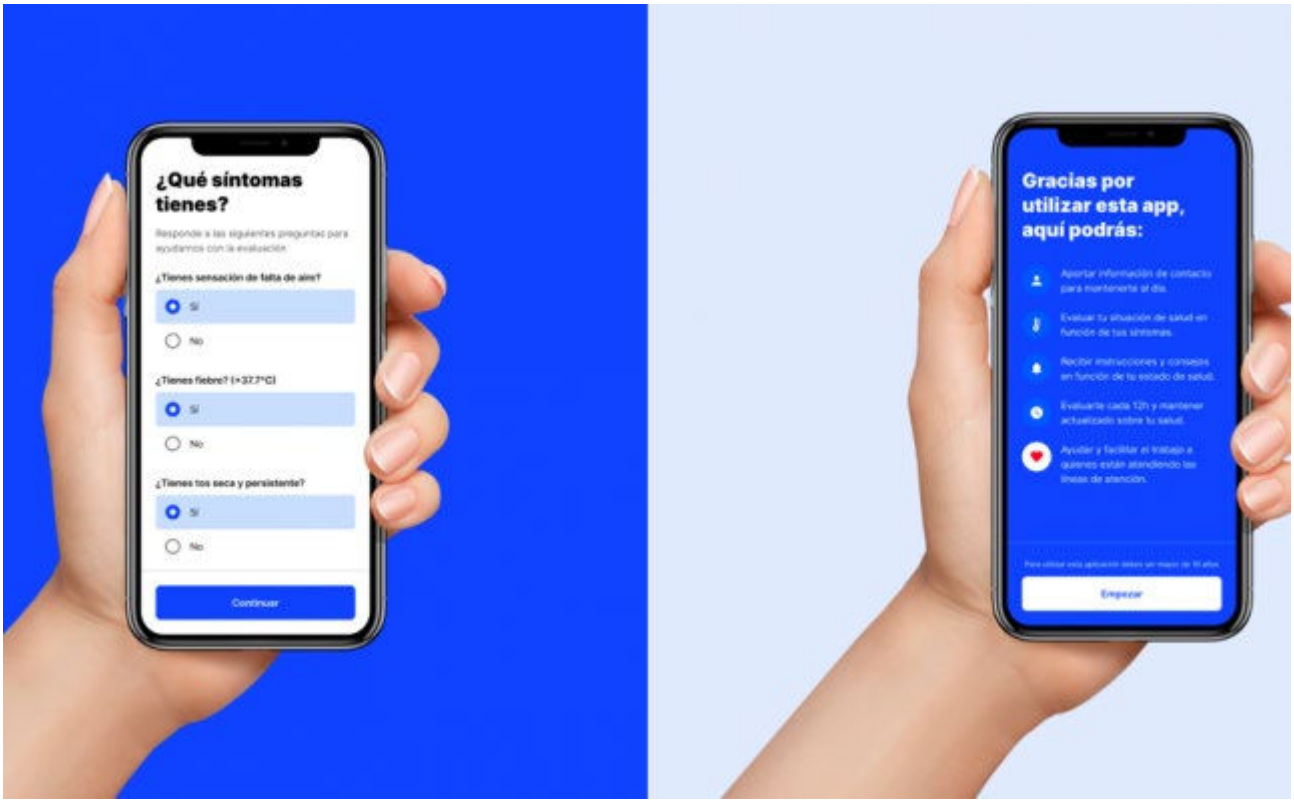
Prodana
Consultores

INFÓRMATE

Comunicación de la Comisión: Orientaciones sobre aplicaciones que apoyan la lucha contra la pandemia de COVID 19 en relación con la protección de datos



COMUNICACIÓN DE LA COMISIÓN

Orientación sobre aplicaciones que apoyan la lucha contra la pandemia de COVID 19 en relación con la protección de datos

1. CONTEXTO

La pandemia de COVID-19 ha creado un desafío sin precedentes para la Unión y los Estados miembros, sus sistemas de salud, forma de vida, estabilidad económica y valores. Las tecnologías y los datos digitales desempeñan un papel valioso en la lucha contra la crisis de COVID-19. Las aplicaciones móviles típicamente instaladas en teléfonos inteligentes (aplicaciones) pueden ayudar a las autoridades de salud pública a nivel nacional y de la UE a monitorear y contener la pandemia de COVID-19 y son particularmente relevantes en la fase de levantar las medidas de contención. Pueden proporcionar orientación directa a los ciudadanos y apoyar los esfuerzos de búsqueda de contactos. En varios países, tanto dentro de la UE como a nivel mundial, las autoridades o desarrolladores nacionales o regionales han anunciado el lanzamiento de aplicaciones con diferentes funcionalidades destinadas a apoyar la lucha contra el virus.

El 8 de abril de 2020, la Comisión adoptó una Recomendación sobre una caja de herramientas común de la Unión para el uso de tecnología y datos para combatir y salir de la crisis COVID-19, en particular en relación con las aplicaciones

móviles y el uso de datos de movilidad anónimos (la "Recomendación"). El propósito de la Recomendación es, entre otras cosas, desarrollar un enfoque europeo común ("Caja de herramientas") para el uso de aplicaciones móviles, coordinado a nivel de la UE, para capacitar a los ciudadanos a tomar medidas efectivas de distanciamiento social, y para advertir, prevenir y contactar rastreo para ayudar a limitar la propagación de la enfermedad COVID-19. La Recomendación establece los principios generales que deberían guiar el desarrollo de dicha caja de herramientas e indica que la Comisión publicará más orientaciones, incluso sobre la protección de datos personales y las implicaciones de privacidad del uso de aplicaciones en este campo.

Con la Hoja de ruta europea conjunta para levantar las medidas de contención de COVID-19, la Comisión, en cooperación con el Presidente del Consejo Europeo, estableció una serie de principios para guiar la eliminación de las medidas de contención debido al brote de COVID-19. Las aplicaciones móviles, incluidas las funcionalidades de rastreo de contactos, pueden desempeñar un papel importante en este contexto. Dependiendo de las características de las aplicaciones y la medida en que la población las use, pueden tener un impacto significativo en el diagnóstico, tratamiento y manejo de COVID-19 dentro y fuera del entorno del hospital. Son particularmente relevantes cuando se levantan las medidas de contención y cuando el riesgo de infección aumenta a medida que más y más personas están en contacto entre sí. Estas aplicaciones pueden ayudar a interrumpir las cadenas de infección de manera más rápida y eficiente que las medidas generales de contención, y pueden reducir el riesgo de propagación significativa del virus. Por lo tanto, deberían ser un elemento importante en la estrategia de salida, complementando otras medidas como el aumento de las capacidades de prueba. Un requisito previo importante para el desarrollo, la aceptación y la aceptación de tales aplicaciones por parte de las personas es la confianza. Las personas deben tener la certeza de que se garantiza el cumplimiento de los derechos fundamentales y de que las aplicaciones se utilizarán solo para los fines específicamente definidos, que no se utilizarán para la vigilancia masiva y que las personas mantendrán el control de sus datos. Esta es la base de la precisión y efectividad de tales aplicaciones para contener la propagación del virus. Por lo tanto, es esencial identificar soluciones que sean menos intrusivas y cumplan plenamente con los requisitos de protección de datos personales y privacidad establecidos en la legislación de la UE. Además, las aplicaciones deben desactivarse a más tardar cuando se declara que la pandemia está bajo control. Las aplicaciones también deben incluir protecciones de seguridad de la información de última generación.

Esta guía tiene en cuenta la contribución de la Junta Europea de Protección de Datos (EDPB) y las discusiones dentro de la red de eHealth. El EDPB planea publicar Directrices en los próximos días sobre geolocalización y otras herramientas de rastreo en el contexto del brote de COVID-19.

Alcance de la orientación

Para garantizar un enfoque coherente en toda la UE y proporcionar orientación a los Estados miembros y a los desarrolladores de aplicaciones, este documento establece las características y requisitos que deben cumplir las aplicaciones para garantizar el cumplimiento de la legislación de privacidad y protección de datos personales de la UE, en particular el Reglamento general de protección de datos (GDPR) y la Directiva de privacidad electrónica. Esta guía no aborda otras condiciones, incluidas las limitaciones que los Estados miembros podrían haber incluido en sus leyes nacionales con respecto al procesamiento de datos relacionados con la salud.

La guía no es legalmente vinculante. Es sin perjuicio del papel del Tribunal de Justicia de la UE, que es la única institución que puede dar una interpretación autorizada del derecho de la UE.

La presente guía aborda solo las aplicaciones voluntarias que apoyan la lucha contra la pandemia de COVID 19 (aplicaciones descargadas, instaladas y utilizadas de forma voluntaria por individuos) con una o varias de las siguientes funcionalidades:

- Proporcionar información precisa a las personas sobre la pandemia de COVID-19;
- Proporcionar cuestionarios para autoevaluación y orientación a las personas (funcionalidad de verificación de síntomas);
- Alertar a las personas que han estado cerca de una persona infectada durante un cierto tiempo, para proporcionar información como si se debe poner en cuarentena y dónde hacerse la prueba (localización de contactos y funcionalidad de advertencia);

- Proporcionar un foro de comunicación entre pacientes y médicos en situación de autoaislamiento o donde se proporcionen más diagnósticos y consejos de tratamiento (mayor uso de la telemedicina).

De conformidad con la Directiva sobre privacidad electrónica, la imposición del uso de una aplicación que implique la confidencialidad de los derechos de comunicación establecidos en el artículo 5 solo es posible mediante una ley que sea necesaria, apropiada y proporcionada para proteger ciertos objetivos específicos. Dado el alto grado de intrusión de tal enfoque y los desafíos involucrados, incluso en términos de establecer salvaguardas apropiadas, la Comisión considera que se requiere un análisis cuidadoso antes de usar esta opción. Por estas razones, la Comisión recomienda el uso de aplicaciones voluntarias.

Esta guía no cubre aplicaciones destinadas a hacer cumplir los requisitos de cuarentena (incluidas las que son obligatorias).

2. CONTRIBUCIÓN DE APLICACIONES A LA LUCHA CONTRA COVID-19

La funcionalidad del verificador de síntomas es una herramienta para que las autoridades de salud pública guíen a los ciudadanos sobre las pruebas de COVID-19, para proporcionar información sobre el autoaislamiento, sobre cómo evitar la transmisión a otros y cuándo buscar atención médica. También puede complementar la vigilancia de atención primaria e informar mejor cuáles son las tasas de transmisión de COVID-19 en la población.

Las funciones de rastreo y advertencia de contactos son herramientas para identificar a las personas que han estado en contacto con una persona infectada por COVID-19 y para informarle sobre los próximos pasos apropiados, como la cuarentena, las pruebas o el asesoramiento sobre qué hacer en caso de síntomas n. Por lo tanto, esta funcionalidad es útil tanto para las personas como para las autoridades de salud pública. También puede desempeñar un papel importante en la gestión de medidas de contención durante los escenarios de reducción de escala. Su impacto puede ser impulsado por una estrategia que respalde pruebas más amplias de personas que presenten síntomas leves.

Ambas funcionalidades también pueden ser una fuente relevante de datos para las autoridades de salud pública y facilitar la transmisión de dichos datos a las autoridades epidemiológicas nacionales y al Centro Europeo para la Prevención y el Control de Enfermedades (ECDC). Esto ayudaría a comprender los patrones de transmisión y, si se combina con los resultados de las pruebas, estimará el valor predictivo positivo de los síntomas respiratorios en una comunidad determinada y proporcionará información sobre el nivel de circulación del virus.

El grado de fiabilidad de las estimaciones está directamente relacionado con el número y la fiabilidad de los datos transmitidos.

Por lo tanto, en combinación con las estrategias de prueba apropiadas, tanto el verificador de síntomas como las funcionalidades de rastreo de contactos pueden proporcionar información sobre el nivel de circulación del virus y ayudar a evaluar el impacto del distanciamiento físico y las medidas de confinamiento. Como se establece en la Recomendación, para permitir la colaboración transfronteriza y garantizar la detección de contactos entre usuarios de diferentes aplicaciones (que es particularmente importante en los movimientos transfronterizos de ciudadanos), debe garantizarse la interoperabilidad entre las soluciones informáticas de los diferentes Estados miembros. Cuando una persona infectada está en contacto con un usuario de una aplicación de otro Estado miembro, la transmisión transfronteriza de los datos personales de ese usuario a las autoridades sanitarias de su Estado miembro debería ser posible en la medida estrictamente necesaria. El trabajo sobre este tema se llevará a cabo como parte de la caja de herramientas anunciada por la Recomendación. La interoperabilidad debe garantizarse mediante requisitos técnicos y mejorando la comunicación y la cooperación entre las autoridades sanitarias nacionales. Un modelo de cooperación particular también podría usarse como modelo de gobernanza para aplicaciones de rastreo de contactos durante la pandemia de COVID-19.

3. ELEMENTOS PARA UN USO CONFIABLE Y RESPONSABLE DE APLICACIONES

Las funcionalidades incluidas en las aplicaciones pueden tener un impacto diferente en una amplia gama de derechos consagrados en la Carta de los Derechos Fundamentales de la UE, como la dignidad humana, el respeto a la vida

privada y familiar, la protección de datos personales, la libertad de movimiento, no -discriminación, libertad para realizar negocios y libertad de reunión y asociación. La interferencia con la privacidad y el derecho a la protección de datos personales puede ser particularmente importante dado que algunas de las funcionalidades se basan en un modelo de uso intensivo de datos.

Los elementos presentados a continuación tienen como objetivo proporcionar orientación sobre cómo limitar la intrusión de las funcionalidades de la aplicación para garantizar el cumplimiento de la legislación de protección de datos personales y privacidad de la UE.

3.1. Autoridades nacionales de salud (o entidades que realizan tareas de interés público en el campo de la salud) como controlador de datos

La identificación de quién decide sobre los medios y propósitos del procesamiento de datos (el controlador de datos) es crucial para establecer quién es responsable del cumplimiento de las normas de protección de datos personales de la UE y, en particular: quién debe proporcionar información a las personas quienes descargan la aplicación sobre lo que sucederá con sus datos personales (ya existentes o que se generarán a través del dispositivo, como un teléfono inteligente, en el que se está instalando la aplicación), cuáles serán sus derechos, quién será responsable de el caso de violación de datos, etc.

Dada la confidencialidad de los datos personales disponibles y el propósito del procesamiento de datos que se describe a continuación, la Comisión considera que las aplicaciones deben diseñarse de tal manera que las autoridades sanitarias nacionales (o entidades que realizan tareas de interés público en el campo de la salud) son los controladores. Los controladores son responsables del cumplimiento del GDPR (principio de responsabilidad). El alcance de dicho acceso debe limitarse según los principios descritos en la sección 3.5 a continuación.

Esto también contribuirá a una mayor confianza entre la población y, por lo tanto, a la aceptación de las aplicaciones (y los sistemas de información subyacentes de las cadenas de transmisión de infecciones) y garantizará que cumplan el propósito previsto de proteger la salud pública. Las políticas, requisitos y controles subyacentes deben ser alineados e implementados de manera coordinada por las autoridades sanitarias nacionales responsables.

3.2. Asegurarse de que el individuo mantenga el control

Un factor determinante para que las personas confíen en las aplicaciones es demostrar que mantienen el control de sus datos personales. Para garantizar esto, la Comisión considera que, en particular, deben cumplirse las siguientes condiciones:

- La instalación de la aplicación en su dispositivo debe ser voluntaria y sin consecuencias negativas para la persona que decide no descargar / usar la aplicación;
- No se deben agrupar diferentes funcionalidades de la aplicación (por ejemplo, información, verificador de síntomas, rastreo de contactos y funcionalidades de advertencia) para que el individuo pueda proporcionar su consentimiento específicamente para cada funcionalidad. Esto no debería impedir que el usuario combine diferentes funcionalidades de la aplicación si el proveedor lo ofrece como una opción;
- Si se utilizan datos de proximidad (datos generados por el intercambio de señales Bluetooth de baja energía (BLE) entre dispositivos dentro de una distancia epidemiológicamente relevante y durante un tiempo epidemiológicamente relevante), deben almacenarse en el dispositivo del individuo. Si esos datos se van a compartir con las autoridades sanitarias, se deben compartir solo después de la confirmación de que la persona afectada está infectada con el COVID-19 y con la condición de que él / ella decida hacerlo;

- Las autoridades sanitarias deben proporcionar a las personas toda la información necesaria relacionada con el procesamiento de sus datos personales (de conformidad con los artículos 12 y 13 del RGPD y el artículo 5 de la Directiva de privacidad electrónica);
- El individuo debe poder ejercer sus derechos bajo el RGPD (en particular, acceso, rectificación, eliminación). Cualquier restricción de los derechos bajo el GDPR y la Directiva de privacidad electrónica debe estar de acuerdo con estos actos y ser necesaria, proporcionada y prevista en la legislación;
- Las aplicaciones deben desactivarse a más tardar cuando se declara que la pandemia está bajo control; la desactivación no debe depender de la desinstalación por parte del usuario.

3.3. Base legal para el procesamiento

Instalación de las aplicaciones y almacenamiento de información en el dispositivo del usuario.

Como se señaló anteriormente, en virtud de la Directiva de privacidad electrónica (artículo 5), el almacenamiento de información en el dispositivo del usuario o el acceso a la información ya almacenada solo se permite si el usuario ha dado su consentimiento o el almacenamiento y / o acceso es estrictamente necesario para el servicio de la sociedad de la información (por ejemplo, la aplicación) solicitado explícitamente (es decir, instalado y activado) por el usuario.

El almacenamiento de información en el dispositivo del individuo y el acceso a la información ya almacenada en este dispositivo normalmente es necesaria para que las aplicaciones funcionen. Además, la funcionalidad de seguimiento y advertencia de contactos requiere que se almacene en el dispositivo del usuario otra información (como efímeras, que cambian periódicamente las identificaciones de usuario de alias de los usuarios de esta funcionalidad en las proximidades). Además, esta funcionalidad puede requerir que el usuario (infectado o probablemente infectado) cargue datos de proximidad. Tal carga no es necesaria para el funcionamiento de la aplicación como tal. Por lo tanto, no se cumplen los requisitos de la opción mencionados en el párrafo anterior. Eso deja el consentimiento (opción anterior) como el terreno más apropiado para las actividades relevantes. Este consentimiento debe ser "otorgado libremente", "específico", "Explícito" e "informado" en el sentido del GDPR. Debe expresarse a través de una clara acción afirmativa del individuo; esto excluye las formas tácitas de consentimiento (por ejemplo, silencio; inactividad).

Base jurídica para la tramitación por las autoridades sanitarias nacionales: legislación de la Unión o de los Estados miembros

Las autoridades sanitarias nacionales normalmente procesan datos personales cuando existe una obligación legal establecida en la legislación de la UE o de los Estados miembros que establece dicho procesamiento y cumple con las condiciones del artículo 6 y el artículo 9 del RGPD o cuando dicho procesamiento es necesario para el desempeño de una tarea realizada para promover el interés público reconocido por la legislación de la UE o de los Estados miembros.

Cualquier ley nacional debe proporcionar medidas específicas y adecuadas para salvaguardar los derechos y libertades de los interesados. Como regla general, cuanto más fuerte sea el impacto en las libertades de los individuos, las salvaguardas correspondientes más fuertes deberían estar previstas en la ley pertinente.

Las leyes de la UE y de los Estados miembros que preexisten al brote de COVID-19 y las que los Estados miembros están promulgando específicamente para combatir la propagación de epidemias pueden, en principio, utilizarse como base legal para el procesamiento de datos de individuos si proporcionan medidas permitiendo el monitoreo de epidemias y si esa ley cumple con los requisitos adicionales establecidos en el Artículo 6 GDPR.

Dada la naturaleza de los datos personales en cuestión (en particular los datos de salud como categorías especiales de datos personales), así como las circunstancias de la actual pandemia de COVID-19, confiar en la ley como base legal contribuiría a la seguridad jurídica, ya que prescribir en detalle el procesamiento de datos de salud específicos y especificar claramente los propósitos para el procesamiento; especifique claramente quién es el controlador, es decir, la entidad que procesa los datos y quién, además del controlador, puede tener acceso a dichos datos; excluir la posibilidad de procesar dichos datos para fines diferentes a los enumerados en la legislación y proporcionar garantías específicas.

El procesamiento por parte de las autoridades de salud sobre la base de la legislación no cambia el hecho de que las personas pueden instalar o no la aplicación y compartir sus datos con las autoridades de salud. Por lo tanto, no deben producirse consecuencias adversas para los usuarios cada vez que se desinstala la aplicación.

Las aplicaciones de seguimiento y advertencia de contactos proporcionan advertencias a las personas. Cuando la aplicación proporciona esta advertencia directamente, la Comisión llama la atención sobre la prohibición de someter a las personas a una decisión basada únicamente en el procesamiento automatizado que produce un efecto legal o que lo afecta de manera similar (artículo 22 del RGPD).

3.4. Minimización de datos

Los datos producidos a través de dispositivos y ya almacenados previamente en esos dispositivos están protegidos de la siguiente manera:

- Como "datos personales", es decir, cualquier información relacionada con una persona física identificada o identificable (Artículo 4 del GDPR), está protegida por el GDPR. Los datos de salud se benefician de una protección adicional (artículo 9 del GDPR).
- Como "datos de ubicación", es decir, datos procesados en una red de comunicaciones electrónicas o por un servicio de comunicaciones electrónicas, que indica la posición geográfica del equipo terminal del usuario, está protegido por la Directiva de privacidad electrónica (Art. 5),
- Cualquier información almacenada y a la que se acceda desde el equipo terminal del usuario está protegida por el Artículo 5 de la Directiva de privacidad electrónica.

Los datos no personales (como los datos anónimos irreversibles) no están protegidos por el GDPR.

La Comisión recuerda que el principio de minimización de datos requiere que solo se puedan procesar los datos personales que sean adecuados, relevantes y limitados a lo necesario en relación con el propósito. Una evaluación de la necesidad de procesar los datos personales y la relevancia de dichos datos personales debe llevarse a cabo a la luz de los propósitos perseguidos.

La Comisión señala, por ejemplo, que si el propósito de la funcionalidad es la verificación de síntomas o la telemedicina, estos propósitos no requieren acceso a la lista de contactos de la persona propietaria del dispositivo.

Generar y procesar menos datos limita los riesgos de seguridad. Por lo tanto, el cumplimiento de las medidas de minimización de datos también proporciona salvaguardas de seguridad.

- Funcionalidad de información:

Una aplicación con solo esta funcionalidad no necesitará procesar ningún dato de salud de las personas. Simplemente les proporcionará información. Para cumplir con este propósito, no se puede procesar ninguna información almacenada y a la que se acceda desde un equipo terminal que no sea la necesaria para proporcionar la información.

- Comprobador de síntomas y funcionalidades de telemedicina:

Si la aplicación incluye una o dos de estas funcionalidades, procesará datos personales de salud. Por lo tanto, una lista de datos que pueden procesarse debe especificarse en la legislación subyacente aplicable a las autoridades sanitarias.

Además, las autoridades sanitarias pueden necesitar los números de teléfono de las personas que utilizaron el verificador de síntomas y cargaron los resultados. La información almacenada y a la que se accede desde el equipo terminal solo se puede procesar en la medida en que sea necesaria para permitir que la aplicación cumpla su propósito y le permita funcionar.

- Funcionalidad de rastreo y advertencia de contactos:

La mayoría de las infecciones por COVID-19 ocurren a través de gotas que viajan solo a una distancia limitada. Identificar lo más rápido posible a las personas que han estado cerca de una persona infectada es un factor clave para interrumpir la cadena de infección. La proximidad determinante es una función de la distancia y la duración de un contacto y debe hacerse desde un punto de vista epidemiológico. La interrupción de la cadena de infección es particularmente relevante para evitar el resurgimiento de infecciones en la fase de salida de la crisis.

Los datos de proximidad podrían ser necesarios para esto. Para la medición de proximidad y contactos cercanos, las comunicaciones Bluetooth de baja energía (BLE) entre dispositivos parecen más precisas y, por lo tanto, más apropiadas, que el uso de datos de geolocalización (GNSS / GPS o datos de ubicación celular). BLE evita la posibilidad

de seguimiento (contrario a los datos de geolocalización). Por lo tanto, la Comisión recomienda el uso de datos de comunicaciones BLE (o datos generados por tecnología equivalente) para determinar la proximidad.

Los datos de ubicación no son necesarios para el propósito de las funciones de rastreo de contactos, ya que su objetivo no es seguir los movimientos de las personas ni hacer cumplir las prescripciones. Además, el procesamiento de datos de ubicación en el contexto del rastreo de contactos sería difícil de justificar a la luz del principio de minimización de datos y puede crear problemas de seguridad y privacidad. Por este motivo, la Comisión aconseja no utilizar datos de ubicación en este contexto.

Independientemente de los medios técnicos utilizados para determinar la proximidad, no parece necesario almacenar la hora exacta del contacto o el lugar (si está disponible). Sin embargo, podría ser útil almacenar el día del contacto para saber si el contacto ocurrió cuando la persona desarrolló los síntomas (o 48 horas antes) y para guiar el mensaje de seguimiento con consejos, por ejemplo, sobre cuánto tiempo se debe poner en cuarentena.

Los datos de proximidad solo deben generarse y procesarse si existe un riesgo real de infección (dependiendo de la cercanía y la duración del contacto).

Cabe señalar que la necesidad y la proporcionalidad de la recopilación de datos dependerán, por lo tanto, de factores como la medida en que las instalaciones de prueba están disponibles, en particular cuando ya se ordenaron medidas como el confinamiento. La advertencia de personas que han estado en contacto cercano con una persona infectada se puede hacer de dos maneras:

Según el primer enfoque, se envía automáticamente una alerta a través de la aplicación a los contactos cercanos cuando un usuario notifica a la aplicación, con la aprobación o confirmación de la autoridad de salud, por ejemplo, a través de un código QR o TAN, que él o ella dieron positivo. (Procesamiento descentralizado). El contenido del mensaje de alerta debe ser determinado preferentemente por la autoridad sanitaria. Según el segundo enfoque, los identificadores temporales arbitrarios se almacenan en un servidor de fondo mantenido por la autoridad sanitaria (solución de servidor de fondo). Los usuarios no pueden identificarse directamente a través de estos datos. A través de los identificadores, los usuarios que han estado en contacto cercano con un usuario probado positivamente, reciben una alerta en su dispositivo. Si las autoridades sanitarias desean contactar a los usuarios que han estado en contacto cercano con una persona infectada también por teléfono o SMS,

3.5. Limitar la divulgación / acceso de datos

- -Funcionalidad de información:

Ninguna información almacenada y a la que se acceda desde el equipo terminal puede compartirse con las autoridades sanitarias, salvo lo necesario para tener la funcionalidad de la información. Dado que esta funcionalidad solo proporciona los medios de comunicación, las autoridades sanitarias no tendrán acceso a ningún otro dato.

- Comprobador de síntomas y funcionalidades de telemedicina:

La funcionalidad del verificador de síntomas puede ser útil para que los Estados miembros guíen a los ciudadanos sobre si deben hacerse la prueba, proporcionar información sobre el aislamiento y cuándo y cómo acceder a la atención médica, en particular para los grupos de riesgo. Esta funcionalidad también puede complementar la vigilancia de atención primaria y ayudar a comprender cuáles son las tasas de infección de COVID-19 en la población. Por lo tanto, se puede decidir que las autoridades sanitarias responsables y las autoridades epidemiológicas nacionales deben tener acceso a la información proporcionada por el paciente. El ECDC podría recibir datos agregados de las autoridades nacionales para la vigilancia epidemiológica.

Si se elige permitir un contacto con los funcionarios de salud en lugar de hacerlo solo a través de la aplicación en sí, entonces también es necesario revelar a las autoridades nacionales de salud el número de teléfono de los usuarios de la aplicación.

- Funcionalidad de rastreo y advertencia de contactos:
  - Datos de la persona infectada.

Las aplicaciones generan identificadores efímeros seudoaleatorios y que cambian periódicamente de los teléfonos que están en contacto con el usuario. Una opción es que los identificadores se almacenan en el dispositivo del usuario

(denominado procesamiento descentralizado). Otra opción puede proporcionar que estos identificadores arbitrarios se almacenen en el servidor al que tienen acceso las autoridades sanitarias (la denominada solución de servidor de fondo). La solución descentralizada está más en línea con el principio de minimización. Las autoridades sanitarias deben tener acceso solo a los datos de proximidad del dispositivo de una persona infectada para que puedan contactar a las personas en riesgo de infección.

Estos datos estarán disponibles para las autoridades de salud solo después de que la persona infectada (después de haber sido analizada) comparta estos datos de manera proactiva con ellos.

La persona infectada no debe ser informada sobre la identidad de las personas con las que ha estado en contacto epidemiológicamente relevante y a quienes se alertará.

- Datos de las personas que han estado en contacto (epidemiológico) con la persona infectada

La identidad de la persona infectada no debe divulgarse a las personas con las que ha estado en contacto epidemiológico. Es suficiente comunicarles el hecho de que han estado en contacto epidemiológico con una persona infectada durante los últimos 16 días. Como se señaló anteriormente, los datos sobre la hora y el lugar de dichos contactos no deben almacenarse. Por lo tanto, no es necesario ni posible comunicar esos datos.

Para rastrear los contactos epidemiológicos de un usuario de la aplicación electrónica que se encuentra infectado, las autoridades nacionales de salud solo deben ser informadas sobre el identificador de la persona con la que la persona infectada ha estado en contacto epidemiológico desde 48 horas antes del inicio de los síntomas hasta el 14 días después del inicio de los síntomas, según la proximidad y la duración del contacto.

El ECDC podría recibir datos agregados de rastreo de contactos de las autoridades nacionales para la vigilancia epidemiológica de los indicadores definidos en colaboración con los Estados miembros.

3.6. Proporcionar para fines precisos de procesamiento

La base jurídica (legislación de la Unión o del Estado miembro) debe prever el propósito del procesamiento. El propósito debe ser específico, para que no haya dudas sobre qué tipo de datos personales es necesario procesar para lograr el objetivo deseado y explícito. .

Los propósitos precisos dependerán de las funcionalidades de la aplicación. Puede haber varios propósitos para cada funcionalidad de una aplicación. Para proporcionar a las personas un control total de sus datos, la Comisión recomienda no agrupar diferentes funcionalidades. En cualquier caso, el individuo debe tener la posibilidad de elegir entre diferentes funcionalidades que persiguen cada una un propósito diferente.

La Comisión desaconseja el uso de los datos recopilados en las condiciones anteriores para otros fines que no sean la lucha contra COVID-19. En caso de que sean necesarios fines como la investigación científica y las estadísticas, deben incluirse en la lista original de propósitos y comunicarse claramente a los usuarios.

- Funcionalidad de información:

El objetivo de esta funcionalidad es proporcionar la información relevante desde el punto de vista de las autoridades sanitarias en el contexto de la crisis.

- Funcionalidades de verificación de síntomas y telemedicina:

La funcionalidad del verificador de síntomas puede proporcionar una indicación de qué proporción de las personas que informan síntomas compatibles con COVID-19 está realmente infectada (por ejemplo, frotando y probando a todas o una cantidad aleatoria de personas con tales síntomas, si hay capacidad para hacerlo). Esta identificación del propósito debe dejar en claro que los datos personales de salud se procesarán para proporcionar al individuo la posibilidad de autoevaluarse, sobre la base de un conjunto de preguntas formuladas, si él o ella ha desarrollado síntomas de COVID-19, o para obtener consejo médico si ha desarrollado los síntomas de COVID-19.

- Rastreo de contactos y funcionalidades de advertencia:

La mera indicación de un propósito "prevención de futuras infecciones por COVID-19" no es lo suficientemente específica. En este caso, la Comisión recomienda especificar con mayor precisión el (los) propósito (s) a lo largo de las

líneas de: “retener los contactos de las personas que usan la aplicación y que pueden haber estado expuestas a la infección por COVID-19 para advertir a esas personas quién podría haber sido potencialmente infectado ".

3.7. Establecer límites estrictos para el almacenamiento de datos

El principio de limitación de almacenamiento requiere que los datos personales no se conserven por más tiempo del necesario. Los plazos deben basarse en la relevancia médica (según el propósito de la aplicación: el período de incubación, etc.), así como las duraciones realistas de los pasos administrativos que pueden ser necesarios.

- Funcionalidad de información:

Si se recopilan datos al instalar esta funcionalidad, se deben eliminar de inmediato. No hay justificación para mantener dichos datos.

- Comprobador de síntomas y funcionalidades de telemedicina:

Dichas datos deben ser eliminadas por las autoridades sanitarias después de un máximo de un mes (período de incubación más margen) o después de que la persona fue analizada y el resultado es negativo. Las autoridades sanitarias pueden retener datos durante períodos más largos para informes de vigilancia e investigación, siempre que estén en forma anónima.

- Rastreo de contactos y funcionalidades de advertencia:

Los datos de proximidad deben eliminarse tan pronto como ya no sean necesarios para alertar a las personas. Este debería ser el caso después de un máximo de un mes (período de incubación más margen) o después de que la persona fue evaluada y el resultado es negativo. Las autoridades de salud pueden retener los datos de proximidad durante períodos más largos para informes de vigilancia e investigación, siempre que estén en forma anónima.

Los datos deben almacenarse en el dispositivo del usuario y solo los datos que han sido comunicados por los usuarios y que son necesarios para cumplir con el propósito deben cargarse en el servidor disponible para las autoridades sanitarias donde se elige esta opción (es decir, solo cargar los datos en el servidor de "contactos cercanos" de una persona que dio positivo de infección de COVID-19).

3.8. Garantizar la seguridad de los datos.

La Comisión recomienda que los datos se almacenen en el dispositivo terminal del individuo en forma encriptada utilizando técnicas criptográficas de última generación. En el caso de que los datos se almacenen en un servidor central, el acceso, incluido el acceso administrativo, debe registrarse.

Los datos de proximidad solo deben generarse y almacenarse en el dispositivo terminal del individuo en formato cifrado y seudónimo. Para garantizar que el seguimiento por parte de terceros, se excluye, la activación de Bluetooth debería ser posible sin tener que activar otros servicios de ubicación.

Durante la recopilación de datos de proximidad a través de BLE, es preferible crear y almacenar ID de usuario temporales que cambian regularmente en lugar de almacenar la ID real del dispositivo. Esta medida proporciona protección adicional contra el espionaje y el rastreo por parte de piratas informáticos y, por lo tanto, dificulta la identificación de personas.

La Comisión recomienda que el código fuente de la aplicación se haga público y esté disponible para su revisión.

Se pueden prever medidas adicionales para proteger los datos procesados, en particular mediante la eliminación automática o el anonimato de los datos después de un cierto punto en el tiempo. En general, el grado de seguridad debe coincidir con la cantidad y la sensibilidad de los datos personales procesados.

Todas las transmisiones del dispositivo personal a las autoridades sanitarias nacionales deben estar encriptadas.

Cuando la legalización nacional establece que los datos personales recopilados también pueden procesarse con fines de investigación científica, en principio se debe utilizar la seudonimización.

3.9. Garantizar la precisión de los datos.

Garantizar la precisión de los datos personales procesados no solo es un requisito previo para la eficiencia de la aplicación, sino que también es un requisito según la legislación de protección de datos personales.

En este contexto, es esencial garantizar la precisión de la información sobre si se ha producido un contacto con una persona infectada (distancia epidemiológica y duración) para minimizar el riesgo de tener falsos positivos. Esto debería abordar escenarios cuando dos usuarios de la aplicación están en contacto en la calle, en el transporte público o en un edificio. Es poco probable que el uso de datos de ubicación basados en redes de telefonía móvil sea lo suficientemente preciso para esto.

Por lo tanto, es aconsejable confiar en tecnologías que permitan una evaluación más precisa del contacto (como Bluetooth).

3.10. Autoridades de protección de datos involucradas

Las Autoridades de Protección de Datos deben participar y consultar por completo en el contexto del desarrollo de la aplicación y deben mantener su implementación bajo revisión. Dado que el procesamiento de datos en el contexto de la aplicación calificará como un procesamiento a gran escala de categorías especiales de datos (datos de salud), la Comisión llama la atención sobre el Artículo 35 GDPR sobre evaluación de impacto de protección de datos.

- FUENTE: La Oficina de Publicaciones de la Unión Europea https://op.europa.eu/en/web/about-us/who-we-are

EUR-Lex
Acceso al derecho de la Unión Europea