ECIJA | Torre de Cristal Pº de la Castellana, 259C
28046 Madrid · Tel: +34 917 816 160
www.ecija.com

Nota informativa

Madrid, 25 de marzo de 2020

Protección de Datos y COVID-19: recomendaciones para desarrolladores de aplicaciones

En el estado de alarma en el que nos encontramos, derivado de la pandemia del COVID-19, están surgiendo iniciativas tanto en el sector público como privado, cuyo objetivo principal es evitar o ayudar al posible colapso del sistema sanitario. Desde aplicaciones que persiguen realizar un autodiagnóstico de Covid-19, como prestar teleasistencia o ayuden a controlar el aislamiento y la trazabilidad del contagio a través de la geolocalización.

(I) SITUACIÓN ACTUAL

El pasado 16 de marzo de 2020, la **Agencia Española de Protección de Datos** (AEPD) lanzó un comunicado en relación a webs y apps que ofrecen autoevaluación y consejos sobre el Coronavirus, anunciando actuaciones de investigación para perseguir aquellas iniciativas que no fueran respetuosas con la normativa de protección de datos.

Cuatro días antes, la AEPD había publicado un informe en el que, distanciándose del criterio de otras autoridades de control europeas, venía a poner por encima de la protección de datos el interés general y la protección de la salud pública: "(…) *en consonancia con la normativa sectorial aplicable en el ámbito de la salud pública, las consideraciones relacionadas con la protección de datos -dentro de los límites previstos por las leyes- no deberían utilizarse para obstaculizar o limitar la efectividad de las medidas que adopten las autoridades, especialmente las sanitarias, en la lucha contra la epidemia, por cuanto ya la normativa de protección de datos personales contiene una regulación para dichos casos que compatibiliza y pondera los intereses y derechos en liza para el bien común (…).*

La realidad de la pandemia que vivimos y los datos que nos suministran a diario, impone que cualquier esfuerzo que ayude a superar esta crisis: apps de autodiagnóstico de Covid-19, de teleasistencia médica o cualquier otra, deba de ser inicialmente bienvenido sin perjuicio de los evidentes riesgos en materia de privacidad pudiera tener y que siempre deben tratar de minimizarse. Debemos ser conscientes que todas estas iniciativas luchan contrarreloj por sacar una aplicación que lamentablemente no tendrán la oportunidad de verificar y adecuar legalmente 100%. La realización de test y la identificación de contagiados resulta fundamental para frenar la epidemia.

El objetivo de esta nota no es otro que informar y ayudar a todas aquellas iniciativas que estén colaborando en este ámbito para que puedan minimizar sus riesgos de cumplimiento normativo.

(II) LA REGULACIÓN NORMATIVA Y LA POSICIÓN DE LAS AUTORIDADES

Debemos considerar que el tratamiento de datos personales debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado, la de otra persona física o el conjunto de la sociedad, en el contexto de epidemias, sin la necesidad de obtener el consentimiento del interesado, conforme se recoge en el considerando 46 del RGPD y que ha sido refrendado por el Comité Europeo de Protección de Datos (EDPD). Debe recordarse

que determinados tratamientos de datos podrían, incluso, encontrase legitimados en base al interés público esencial.

No obstante, lo anterior y si nos centramos en datos de localización y movimiento de los usuarios generados por los propios dispositivos de los usuarios, datos con los que cuentan los operadores de telecomunicaciones por su actividad, basándonos en razones de interés público, sí podrían facilitarse datos anonimizados y agregados que permitan determinar el movimiento de las personas durante este estado de excepcionalidad. Así, las autoridades públicas podrían realizar el procesamiento de los datos de ubicación de forma anónima / agregada, permitiendo generar informes sobre la concentración de dispositivos móviles en una determinada ubicación ("mapas de calor").

Para una monitorización individualizada, debería hacerse el análisis de proporcionalidad exigido por la normativa aplicable, teniendo en este caso, un extraordinario peso la excepcionalidad de la situación epidémica y sanitaria, y el interés público derivado. Así, el art.15 de la Directiva sobre privacidad electrónica permite a los Estados miembros introducir medidas legislativas que persiguen la seguridad nacional y la seguridad pública (debe tenerse en cuenta que la protección de la salud pública puede estar incluida en la excepción de seguridad nacional o pública indicada). Esta legislación de emergencia es posible bajo la condición de que constituya una medida necesaria, apropiada y proporcionada dentro de una sociedad democrática. Si se introducen tales medidas, un Estado miembro está obligado a establecer garantías adecuadas, como otorgar a las personas el derecho a un recurso judicial.

El desarrollo de aplicaciones que faciliten la comunicación entre facultativos sanitarios y los propios pacientes, basadas en procesos de teleasistencia, no deben olvidar las exigencias derivadas de la normativa sanitaria en relación con la legitimación para el tratamiento, que podría derivarse de la relación previa entre médico y paciente, pero que debe completarse con cuestiones básicas como quién puede acceder a datos que podrían entenderse dentro de la historia clínica de los pacientes o que deben quedar guardados durante el plazo de 5 años, atendiendo a posibles reclamaciones. Otro de los aspectos clave hace referencia posibles comunicaciones de datos, por ejemplo, a la Autoridades sanitarias o la reutilización de la información, donde tendrán que valorarse otros posibles usos como la realización de estudios clínicos (donde deberá contemplarse lo establecido en la legislación específica)

Este estado de excepcionalidad, la normativa de protección de datos no puede entenderse como una traba o como un catálogo de cuestiones formales, sino como una regulación que busca aportar seguridad a los tratamientos sobre cuestiones claves como la transparencia. Una información ágil y entendible que informe a los usuarios sobre las finalidades para las que va a ser tratada la información o posibles finalidades derivadas. Nos encontramos ante un enfoque adaptado a garantías, tanto para afrontar el presente en el que nos encontramos como las necesarias en un futuro no lejano que hayamos conseguido vencer esta pandemia.

(III) NUESTRA POSICIÓN

Conforme se ha indicado anteriormente, debemos considerar que la normativa sobre protección de datos personales no debe resultar un obstáculo para el desarrollo y puesta a disposición de aplicaciones y sistemas que tengan por finalidad facilitar la detección y actuación ante la pandemia, tanto desde el ámbito privado como público.

La protección de la privacidad de las personas debe ser compatible con dichas finalidades mediante la implementación de sistemas de anonimización de los datos o la aplicación de principios tales como la minimización, mediante el que debemos tratar los datos estrictamente necesarios para la finalidad perseguida.

La seguridad debe ser un factor clave, que evite las fugas o filtraciones de datos, así como su pérdida o falta de disponibilidad o actualización cuestiones que podrían afectar a la efectividad de aplicación desarrollada.

El momento que vivimos ha puesto de manifiesto que, junto con el concepto individual de privacidad, debe entenderse éste atendiendo también a las circunstancias histórica, sociales y especiales, todo ello no implica el incumplimiento normativo, sino una actualización y el entendimiento desde una óptica ágil y dinámica. La situación de crisis sanitaria que vivimos requiere la adopción de soluciones ágiles, y su puesta a disposición de profesionales y autoridades.

Por todo ello, desde ECIJA queremos apoyar el desarrollo de soluciones, aplicaciones, y sistemas, que permitan, en estos días de incertidumbre, dar respuesta a las necesidades de profesionales, usuarios y autoridades, para que, entre todos, podamos, en un marco de seguridad, cumplimiento y confianza, poner nuestros máximos esfuerzos y recursos para hacer frente a la situación de excepcionalidad y crisis sanitaria que vivimos, y establecer unas sólidas bases para la superación de la misma.

(IV) RECOMENDACIONES

- Adopta desde el inicio del diseño de la plataforma un enfoque "*privacy friendly*", estableciendo estrategias que incorporen la protección de la privacidad de los usuarios a lo largo de todas las etapas de desarrollo de la plataforma App, hasta su retirada.
- Dado que, inevitablemente, surgirán iniciativas que pretendan aprovechar la situación y obtener datos de forma ilícita. Diferénciate y trata de informar siempre de forma transparente y lo más clara posible. En el supuesto de que los datos personales recabados sean utilizados para fines estadísticos y de archivo de interés público, deberás informar sobre ello a los usuarios.
- Así, con carácter previo a la captación de los datos personales del usuario, deberá ponerse a disposición de éstos, la política de protección de datos personales de la App, que permita a los usuarios comprender el alcance del tratamiento de sus datos, los riesgos a los que pueden verse expuestos, así como el modo de hacer valer sus derechos en materia de protección de datos.
- La base jurídica del tratamiento podrá ser el interés público en el ámbito de la salud pública, así como la protección de intereses vitales de los usuarios, o incluso el cumplimiento normativo atendiendo a diferentes finalidades.
- En el supuesto de que la aplicación mediante notificación *push* solicite en los dispositivos móviles la autorización para conocer la ubicación de los usuarios, la base jurídica de dicho tratamiento será el consentimiento del usuario, que tendrá la posibilidad en todo momento, habilitar o deshabilitar dicha opción de geolocalización, tanto desde la app, como desde la configuración de su propio terminal.
- No solicites a los usuarios a través de la App más datos de los estrictamente necesarios para la protección de los intereses vitales de los usuarios y terceros.
- No trates los datos para finalidades distintas a la principal vinculada a facilitar el diagnóstico o seguimiento por un profesional sanitario, la protección pública derivada de la situación de excepcionalidad por la que se desarrolla la aplicación.
- No utilices fotografías de terceras personas salvo que tengas autorización para ello.
- Una aplicación que trata datos de salud o de especial sensibilidad necesita hacer una evaluación de proporcionalidad e impacto con la finalidad de poder detectar, evaluar y tratar los riesgos asociados al tratamiento de datos relativos al estado de salud de los usuarios. (enlace)
- En el supuesto de llevarse a cabo elaboraciones de perfiles con los datos personales recabados, deberá informarse sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el usuario. Ten en cuenta que, si

este perfilado se va a completar con datos de otras fuentes, este requisito debe ser mayor, llegando a solicitar el consentimiento de los usuarios.

- Adopta las medidas de seguridad adecuadas dirigidas a proteger la confidencialidad, integridad y disponibilidad de los datos personales, así como una descripción de las medidas de seguridad técnicas y organizativas implementadas, la adopción de procesos de verificación, evaluación y revisión periódica de la eficacia de las medidas implantadas. Para ello, cuentas ya con herramientas y proveedores en el mercado que garantizan el cumplimiento de las medidas de seguridad establecidas para el tratamiento de datos.
- Elige bien tus proveedores de servicios, asegúrate que cumplen con la normativa en sus condiciones de uso y que aportan seguridad a los datos que vas a tratar, ellos actuarán como encargados tuyos y es importante blindar la responsabilidad de cada uno.
- No trates cookies en la plataforma que requieran informar y obtener el consentimiento del usuario. No las necesitas inicialmente para el objeto perseguido.
- Elimina los datos cuando dejen de ser necesarios para la finalidad para la que fueron recogidos.
- Si vas a compartir información por redes sociales, no compartas datos personales, sino datos estadísticos, que no permitan identificar a las personas, respeta su derecho a la intimidad.
- Recuerda que si sufres una brecha de seguridad, como una fuga de datos, deberás notificarlo a la Agencia Española de Protección de Datos y en determinados supuestos a los propios usuarios (enlace)

Quedamos a su disposición para cualquier cuestión que pudieran necesitar.

Área Privacidad y Protección de Datos
+ 34 91 781 61 60
info@ecija.com