

Directrices de la Comisión Europea para garantizar unas normas de plena protección de los datos en las aplicaciones para luchar contra la pandemia

Barcelona, 17 de abril de 2020

- La Comisión Europea (CE) ha publicado unas **directrices relativas al desarrollo de nuevas aplicaciones móviles** para contribuir a la lucha contra el coronavirus, con el objetivo de ofrecer el marco necesario para garantizar que los ciudadanos cuenten con la suficiente **protección de sus datos personales** y vean limitado el grado de injerencia cuando usen estas aplicaciones.
- Las normas de la UE, en particular el [Reglamento general de protección de datos](#) (RGPD) y la [Directiva sobre la privacidad y las comunicaciones electrónicas](#), ofrecen las mayores garantías de fiabilidad (es decir, su carácter voluntario, la minimización de los datos, la limitación temporal) para que se extienda el uso de estas aplicaciones y para garantizar la exactitud de las mismas.
- Las citadas directrices se centran en aplicaciones de uso voluntario con una o más de las siguientes funciones:
 - información precisa para los usuarios sobre la pandemia de coronavirus;
 - cuestionarios de autodiagnóstico y orientación individualizada (función de comprobación de síntomas);
 - alertas dirigidas a personas que han estado cerca de una persona infectada para que se hagan una prueba o se aislen (función de localización de contactos y de alerta); y
 - un foro de comunicación entre médicos y pacientes en aislamiento voluntario en el que se ofrece asesoramiento adicional en materia de diagnóstico y tratamiento (telemedicina).
- **Principales condiciones** para el desarrollo de aplicaciones móviles de lucha contra el coronavirus:
 - dada la alta sensibilidad de los datos y la finalidad última de las aplicaciones, la CE estima que la responsabilidad de rendir cuentas sobre el cumplimiento de las normas de protección de datos personales de la UE recae en las autoridades sanitarias nacionales, también encargadas de garantizar el cumplimiento del RGPD en su uso de los datos recogidos y de facilitar a las personas toda la información necesaria relacionada con el tratamiento de sus datos personales;

- la instalación de una aplicación en el aparato de un usuario debe ser voluntaria, los usuarios deben tener la posibilidad de dar su consentimiento para cada una de las funciones de la aplicación móvil (si se utilizan datos de proximidad, deben almacenarse en el dispositivo del usuario y compartirse únicamente con el consentimiento del usuario y los usuarios deben poder ejercer sus derechos conforme al RGPD);
- las aplicaciones deben respetar el principio de minimización de los datos, que requiere que solo puedan tratarse los datos personales pertinentes y limitados a los fines en cuestión (la CE considera que los datos de localización no son necesarios a efectos de rastreo del contacto y recomienda no utilizarlos en este contexto);
- los datos personales no deben conservarse más tiempo del necesario (los plazos deben fijarse en función de su pertinencia médica, así como de la duración realista de la adopción de las medidas administrativas necesarias);
- los datos deben almacenarse en el dispositivo del usuario y estar cifrados;
- con arreglo a las normas sobre protección de datos personales de la UE, los datos personales tratados por un tercero deben ser exactos (para garantizar la máxima exactitud, que también es fundamental para lograr la eficiencia de las aplicaciones de localización de los contactos, han de emplearse tecnologías como Bluetooth que proporcionen una evaluación más precisa de los contactos entre las personas); y
- las autoridades de protección de datos deben participar plenamente y ser consultadas en el desarrollo de las aplicaciones y deben encargarse de revisar el despliegue de las mismas.