
# Declaración sobre el tratamiento de datos personales en el contexto del brote de COVID-19

## Adoptada el 19 de marzo de 2020

**El Comité Europeo de Protección de Datos (CEPD) ha adoptado la declaración siguiente:**

Los Gobiernos y los organismos públicos y privados de toda Europa están tomando medidas para contener y mitigar la COVID-19. Esas medidas pueden implicar el tratamiento de diferentes tipos de datos personales.

Las normas de protección de datos (como el Reglamento general de protección de datos o RGPD) no entorpecen las medidas adoptadas para luchar contra la pandemia del coronavirus. Combatir las enfermedades transmisibles es un objetivo estratégico común a todas las naciones, por lo que debe prestársele el mayor apoyo posible. Redunda en interés de la humanidad frenar la propagación de enfermedades y utilizar técnicas modernas para repeler las plagas que afectan a grandes zonas del mundo. Dicho esto, el CEPD desea subrayar que, incluso en estos momentos excepcionales, el responsable y el encargado del tratamiento de los datos deben garantizar la protección de los datos personales de los interesados. Por lo tanto, es preciso tener en cuenta una serie de consideraciones para garantizar el tratamiento lícito de los datos personales y recordar, en todos los casos, que cualquier medida adoptada en este contexto debe respetar los principios generales del derecho y no ser irreversible. La actual pandemia es una situación jurídica que puede legitimar ciertas restricciones de las libertades siempre que estas sean proporcionadas y su duración no se prolongue más allá de la propia duración de la epidemia

## 1. Licitud del tratamiento

El **RGPD es un instrumento legislativo de amplio alcance cuyas normas también se aplican al tratamiento de los datos personales en un contexto como el creado por la COVID-19**. **El RGPD permite a las autoridades sanitarias públicas competentes y a los empleadores tratar los datos personales en el contexto de una epidemia, de conformidad con el derecho nacional y con las condiciones en él establecidas.** Por ejemplo, cuando el tratamiento sea necesario por razones de interés público esencial en el ámbito de la salud pública. En estas circunstancias, no es necesario basar el tratamiento de los datos en el consentimiento de los afectados.

**1.1. Por lo que se refiere al tratamiento de datos personales, incluidas las categorías especiales de datos, por parte de las autoridades públicas competentes** (por ejemplo, las autoridades sanitarias públicas), el CEPD considera que dicho tratamiento está autorizado en virtud de los artículos 6 y 9 del

RGPD, en particular cuando recae bajo el mandato legal de la autoridad pública establecido por la legislación nacional y se ajusta a las condiciones establecidas en el RGPD.

**1.2. En el ámbito laboral**, el tratamiento de datos personales puede ser necesario para el cumplimiento de una obligación legal a la que el empleador esté sujeto, como las relativas a la seguridad y la salud en el trabajo, o por motivos de interés público, como el control de las enfermedades y otras amenazas para la salud. El RGPD contempla también excepciones a la prohibición del tratamiento de determinadas categorías especiales de datos personales, como los sanitarios, cuando lo exijan motivos de interés público esencial en el ámbito de la salud pública [artículo 9, apartado 2, letra i)], sobre la base del derecho de la Unión o de los Estados miembros, o cuando sea necesario proteger intereses vitales del interesado [artículo 9, apartado 2, letra c)], refiriéndose explícitamente el considerando 46 al control de epidemias.

**1.3. Por lo que se refiere al tratamiento de datos de telecomunicaciones**, **como los datos de localización**, debe también cumplirse el derecho nacional que da aplicación a la Directiva sobre la privacidad y las comunicaciones electrónicas. En principio, los datos de localización solo pueden ser utilizados por el operador si han sido anonimizados o si se cuenta con el consentimiento de los interesados. No obstante, el artículo 15 de la **Directiva sobre la privacidad y las comunicaciones electrónicas permite a los Estados miembros introducir medidas legales para proteger la seguridad pública**. Esa legislación de carácter excepcional solo puede adoptarse **si** constituye una medida **necesaria, apropiada y proporcionada en una sociedad democrática**. Debe ajustarse a la Carta de los Derechos Fundamentales y al Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Además, **queda sujeta al control judicial del Tribunal de Justicia de la Unión Europea y del Tribunal Europeo de Derechos Humanos**. Su duración debe limitarse estrictamente a la situación de emergencia que la provoque.

## 2. Principios esenciales aplicables al tratamiento de datos personales

Los datos personales necesarios para alcanzar los objetivos perseguidos deben ser tratados con fines específicos y explícitos.

Además, los interesados deben recibir información transparente sobre las actividades de tratamiento que se estén llevando a cabo y sus características principales, incluido el período de conservación de los datos recogidos y los fines de su tratamiento. La información facilitada deberá ser fácilmente accesible y estar redactada en un lenguaje claro y sencillo.

Es importante adoptar medidas de seguridad adecuadas y políticas de confidencialidad que garanticen que los datos personales no se comuniquen a terceros no autorizados. Las medidas aplicadas para gestionar la situación de emergencia actual y el proceso de toma de decisiones subyacente deben documentarse adecuadamente.

## 3. Uso de datos de localización móvil

- **¿Pueden los Gobiernos de los Estados miembros utilizar los datos personales asociados a los teléfonos móviles de los particulares en sus esfuerzos por vigilar, contener o mitigar la propagación de la COVID-19?**

Los Gobiernos de algunos Estados miembros se plantean utilizar los datos de localización móvil como posible forma de vigilar, contener o mitigar la propagación de la COVID-19, lo que implicaría, por ejemplo, la posibilidad de geolocalizar a determinadas personas o enviar mensajes sobre salud pública por teléfono o SMS a grupos de personas en una zona específica. **Las autoridades públicas deben procurar, en primer lugar, tratar los datos de localización de forma anónima (esto es, tratar datos**

**agregados de manera que las personas no puedan ser reidentificadas), con lo que se podría obtener informes sobre la concentración de dispositivos móviles en un lugar determinado («cartografía»).**

Las normas sobre protección de datos personales no se aplican a los datos que hayan sido debidamente anonimizados.

**Cuando no es posible tratar únicamente datos anónimos**, la Directiva sobre privacidad y comunicaciones electrónicas permite a los Estados miembros introducir medidas legales para proteger la seguridad pública (artículo 15).

Si se introducen medidas que permitan el tratamiento de datos de localización sin anonimizar, los Estados miembros están obligados a establecer **garantías adecuadas**, como reconocer a los particulares que utilicen servicios de comunicaciones electrónicas el **derecho a ejercer acciones judiciales**.

**Es aplicable, asimismo, el principio de proporcionalidad. Deben preferirse siempre las soluciones menos invasivas, teniendo en cuenta el objetivo específico que se pretende alcanzar.** Ciertas medidas invasivas, como el «rastreo» de personas (es decir, el tratamiento de datos históricos de localización no anonimizados), podrían considerarse proporcionadas en circunstancias excepcionales y dependiendo de las modalidades concretas del tratamiento. No obstante, habrían de estar sujetas a unas salvaguardias y unos controles reforzados que garantizasen el respeto de los principios de la protección de datos (proporcionalidad de la medida en cuanto a su duración y a su alcance, limitación del período de conservación de datos y limitación de la finalidad).

## 4. Ámbito laboral

- **¿Puede un empleador exigir a los visitantes o a sus empleados que proporcionen información sanitaria específica en el contexto de la COVID-19?**

Resulta especialmente pertinente a este respecto la aplicación del principio de proporcionalidad y de minimización de los datos. El empleador solo debe exigir información sanitaria en la medida en que lo permita el derecho nacional.

- **¿Puede un empleador someter a revisiones médicas a sus empleados?**

La respuesta debe buscarse en las normativas nacionales en materia de empleo o de seguridad y salud. Los empleadores solo deben tener acceso a los datos sanitarios y tratarlos si sus propias obligaciones legales así lo exigen.

- **¿Puede un empleador revelar que uno de sus empleados está infectado por el coronavirus a sus compañeros de trabajo o al personal externo?**

Los empleadores deben informar a su personal acerca de los casos de COVID-19 y tomar medidas de protección, pero no deben divulgar más información de la necesaria. Cuando sea necesario revelar el nombre del empleado o los empleados que hayan contraído el virus (por ejemplo, con fines preventivos) y el derecho nacional lo permita, se informará de ello previamente a los empleados afectados, cuya dignidad e integridad se protegerá.

- **¿Qué información tratada en el contexto de la COVID-19 pueden obtener los empleadores?**

Los empleadores podrán obtener la información personal que requiera el desempeño de su cometido y la organización del trabajo de acuerdo con la legislación nacional.

Por el Comité Europeo de Protección de Datos

La presidenta

(Andrea Jelinek)