

## **COVID-19 | La incidencia en la protección de datos de carácter personal**

### **Sumario:**

1. Principio general: el derecho fundamental a la protección de datos sigue siendo aplicable.
2. La incidencia en el tratamiento de datos en el ámbito laboral.
3. Protección de datos y teletrabajo.
4. Régimen de inversiones extranjeras relacionadas con el sector del tratamiento de datos.
5. Documentos de referencia sobre COVID-19 y protección de datos personales.

### **1. Principio general: el derecho fundamental a la protección de datos sigue siendo aplicable**

La situación actual de pandemia derivada del COVID-19 ha exigido tomar medidas excepcionales para intentar atajarla y mitigar el impacto económico y social que la misma puede tener. A tal fin responden el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19 y el Real Decreto-Ley 8/2020, de 17 de marzo, de medidas urgentes extraordinarias para hacer frente al impacto económico y social del COVID-19.

Tales medidas dan lugar a que se limite el derecho fundamental a la libertad de circulación, sin que quede suspendido, ni se haya suspendido ningún otro derecho fundamental.

Como ha indicado el Gabinete Jurídico de la Agencia Española de Protección de Datos (AEPD) en su Informe Jurídico 0017/2020, no “existe razón alguna que determine la suspensión de derechos fundamentales, ni dicha medida ha sido adoptada”. También, ha indicado en dicho informe que la protección de datos no debe 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”.

Al respecto, en el caso del derecho fundamental a la protección de datos personales, es necesario tener en cuenta que no es un derecho absoluto. En este sentido, el RGPD explica en su considerando 4 que “no es un derecho absoluto sino que debe considerarse

en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad.”

## **2. La incidencia en el tratamiento de datos en el ámbito laboral**

La anterior consideración implica como regla general que si una empresa trata datos personales de sus empleados relativos a si están contagiados por COVID-19, debe respetar los principios aplicables en materia de protección de datos personales.

### **Los datos de la persona afectada por COVID-19 son datos de salud**

La temperatura de la persona afectada por COVID-19, el hecho de que se haya contagiado o la información relativa a su evolución, son considerados por el Reglamento General de Protección de Datos (RGPD), aprobado por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, como una categoría especial de datos.

En concreto, los datos relativos a la salud son definidos en el RGPD como “datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud”.

El hecho de que sean categorías especiales implica que su tratamiento solo pueda llevarse a cabo cuando se dé alguna de las circunstancias previstas en el artículo 9.2 del RGPD, ya que son las únicas que pueden legitimar el tratamiento de los datos personales. En este sentido, la regla general es la prohibición de tratar datos personales relativos a la salud de una persona, salvo que concurra alguna de las circunstancias que se indican más adelante.

### **¿Cuáles son las claves que deben tenerse en cuenta cuando se tratan datos relativos a la salud en este caso?**

Todo tratamiento de datos personales, incluido en este caso el relativo al COVID-19, tiene que:

1. Tener una:
  - finalidad determinada, explícita y legítima;
  - base de legitimación del tratamiento;
2. Ser proporcional y necesario, no pudiendo utilizarse los datos personales para otras finalidades distintas;
3. Cumplir con los demás principios aplicables, tales como los de minimización del tratamiento, confidencialidad e integridad;
4. Cumplir con las obligaciones aplicables en materia de protección de datos.

En este sentido, ya que se trata de datos relativos a la salud, debe partirse de la existencia de un alto riesgo para el interesado, de manera que el responsable del tratamiento tiene que adoptar medidas adicionales para garantizar el derecho fundamental a la protección de datos.

Es decir, el tratamiento de los datos personales tiene que ser proporcional y cumplir con los requisitos aplicables para garantizar la licitud del tratamiento.

### **¿Es el derecho fundamental a la protección de datos el único a tener en cuenta por la empresa?**

No. El artículo 22.2 de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales (en adelante, LPRL) indica que “las medidas de vigilancia y control de la salud de los trabajadores se llevarán a cabo respetando siempre el derecho a la intimidad y a la dignidad de la persona del trabajador y la confidencialidad de toda la información relacionada con su estado de salud”.

Por tanto, cualesquiera medidas que puedan adoptarse en relación con el COVID-19 deberá tener también en cuenta el respeto del derecho a la intimidad y a la dignidad de los empleados.

### **¿Es el COVID-19 un riesgo laboral?**

Sí. La LPRL define el término “riesgo laboral grave e inminente” como “aquel que resulte probable racionalmente que se materialice en un futuro inmediato y pueda suponer un daño grave para la salud de los trabajadores.

En el caso de exposición a agentes susceptibles de causar daños graves a la salud de los trabajadores, se considerará que existe un riesgo grave e inminente cuando sea probable racionalmente que se materialice en un futuro inmediato una exposición a dichos agentes de la que puedan derivarse daños graves para la salud, aun cuando éstos no se manifiesten de forma inmediata” (art. 4.4º).

### **¿Puede tratar la empresa datos relativos a la salud de sus empleados para identificar si están contagiados o han estado en riesgo de contagio?**

Sí. La empresa puede, e incluso tiene que, tratar los datos personales para finalidades tales como:

1. Vigilar la salud de los trabajadores y proteger la salud de la población en general.
2. Diseñar planes de contingencia que sean necesarios, o que hayan sido previstos por las autoridades sanitarias.

Todo tratamiento de datos personales tendrá que cumplir, en particular, con la normativa sobre protección de datos y también la relativa a la prevención de riesgos laborales.

### **¿Cuál es la base de legitimación del tratamiento de los datos personales relativos al COVID-19 en una empresa?**

Prestando atención al informe del Gabinete Jurídico de la AEPD, la base de legitimación del tratamiento sería el cumplimiento de obligaciones en el ámbito del Derecho laboral y de la seguridad y protección social (art. 9.2.b) del RGPD).

Sin perjuicio de lo anterior, podrían darse otras situaciones relativas al COVID-19 en las que también puedan tratarse los datos personales de los empleados. Una de estas situaciones es cuando el tratamiento es necesario para proteger intereses vitales del interesado o de otras personas y el interesado no esté capacitado para prestar su consentimiento. (art. 9.2.c) del RGPD) o el tratamiento sea necesario para la realización de un diagnóstico médico (art. 9.2.h) del RGPD), siempre que en este último caso su “tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes” (art. 9.3 del RGPD).

Por último, los supuestos relativos a la existencia de un interés público (art. 9.2.g) e i), que como explica el Gabinete Jurídico de la AEPD, “el primero de ellos calificado de “esencial” y el segundo de ellos que hace referencia a un interés público calificado “en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud”, todo ello 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”.

### **¿Es necesario el consentimiento del empleado para vigilar su salud?**

No. El artículo 22.1 de la LPRL indica que una excepción a la necesidad del consentimiento del trabajador para vigilar su salud es que esta tenga por finalidad “verificar si el estado de salud del trabajador puede constituir un peligro para el mismo, para los demás trabajadores o para otras personas relacionadas con la empresa o cuando así esté establecido en una disposición legal en relación con la protección de riesgos específicos y actividades de especial peligrosidad”.

### **¿Puede la empresa obligar a un empleado contagiado que comunique este dato incluso sin su consentimiento?**

En principio el empleado no está obligado a comunicar el motivo de su baja laboral, pero dado que la protección de datos no es un derecho fundamental absoluto, podría tener que hacerlo ya que prevalece el derecho a la protección de la salud de los demás empleados y de la población en general.

Además, el empleado tiene la obligación legal (art. 29.1 de la LPRL) de “velar, según sus posibilidades y mediante el cumplimiento de las medidas de prevención que en cada caso sean adoptadas, por su propia seguridad y salud en el trabajo y por la de aquellas otras personas a las que pueda afectar su actividad profesional, a causa de sus actos y omisiones en el trabajo, de conformidad con su formación y las instrucciones del empresario”.

**¿Puede la empresa comunicar a otros empleados que una persona tiene COVID-19?**

No, salvo que, como indica la AEPD en sus preguntas frecuentes, se dé alguna de las dos siguientes circunstancias (1) no pueda lograrse la finalidad de protección de la salud del personal sin divulgar la identidad de la persona contagiada o (2) lo ordenen las autoridades sanitarias. Se trata de proteger la privacidad o vida privada de la persona física.

**¿Puede una empresa que presta servicios a otra comunicarle a esta última que uno de sus empleados que tuvo contacto con los empleados de la primera que está contagiado?**

Si la empresa no puede comunicar a sus propios empleados la identidad de la persona contagiada cabe entender que tampoco podrá hacerlo en este caso, a menos que sea estrictamente necesario para lograr la finalidad ya indicada en la respuesta anterior o reciba un orden de las autoridades sanitarias. No obstante, lo que sí podrá hacer la empresa es comunicar dicha circunstancia, sin revelar la identidad del empleado.

**¿Puede la empresa tratar los datos de los visitantes a un centro de trabajo?**

Sí, porque se trata de una medida relacionada con la vigilancia de la salud de los trabajadores. Un visitante, aunque sea empleado de otra empresa del grupo, que estuviera contagiado, sería un riesgo para los empleados que puedan estar en contacto cuando visita el centro de trabajo correspondiente.

En este caso, la base de legitimación del tratamiento de los datos personales seguiría siendo el artículo 9.2.b) del RGPD, en los términos ya indicados.

**¿Puede utilizar la empresa cualquier tecnología que considere oportuna para identificar casos de COVID-19?**

No. Debe tenerse en cuenta que la empresa tiene obligación de optar por aquellos “reconocimientos o pruebas que causen las menores molestias al trabajador y que sean proporcionales al riesgo”.

No obstante, si la situación diera lugar a que fuera necesario utilizar una determinada tecnología más eficaz para identificar casos de COVID-19, se podría hacer, así como si se recibe una orden de las autoridades sanitarias.

**¿Puedo utilizar dispositivos de geolocalización para controlar que mis empleados no estén en lugares que puedan suponer un riesgo para ellos y para la empresa?**

No. La empresa está obligada a proteger a sus empleados de manera que no debería enviarles a lugares que puedan suponer un riesgo ni para ellos ni para la empresa y los dispositivos de geolocalización no pueden utilizarse fuera de las horas de trabajo, ya que supondría una intromisión ilícita en el derecho a la intimidad de aquéllos.

**¿Puede la empresa encomendar a un empleado o persona de seguridad que mida la temperatura de los empleados?**

Sería un riesgo que, además podría dar lugar a una infracción de la confidencialidad de los datos personales.

Que un empleado o las personas encargadas de la seguridad de una empresa mida la temperatura de otros empleados, es un riesgo para su salud derivado, entre otras cuestiones, del posible desconocimiento de cómo hacerlo sin correr riesgos de contagio en caso de que la persona a la que mide la temperatura esté contagiada o de que carezca de los medios necesarios para protegerse.

Por tanto, la medición de la temperatura, como recuerda la AEPD en sus preguntas frecuentes en la materia, ya que es parte de la vigilancia de la salud de los empleados, debería “ser realizada por personal sanitario”.

**¿Por qué debe ser personal sanitario el que trate los datos personales relativos a la salud?**

La LPRL ofrece tres razones fundamentales por las que los datos personales relativos a la salud de los empleados, en este caso sobre COVID-19, deben ser tratados únicamente por personal sanitario. En concreto, estas tres razones son que es personal con:

1. Competencia técnica;
2. Formación acreditada, y
3. Capacidad acreditada.

Además, es personal que se encontrará sujeto a una obligación de confidencialidad sobre la información a la que tengan acceso en el desempeño de sus funciones.

**Si los datos personales se tratan mal, ¿hay riesgos de sanciones?**

Sí. Dado que el derecho fundamental a la protección de datos sigue siendo aplicable, todo incumplimiento puede ser objeto de sanción, que en caso de ser una multa administrativa económica podría ser elevada ya que se trataría de una infracción considerada como muy grave.

**3. Protección de datos y teletrabajo**

Una de las medidas que se han adoptado para atajar la infección por COVID-19 es la generalización, cuando ello sea posible, del teletrabajo.

Esta circunstancia implica que pueden producirse tratamientos de datos personales fuera del ámbito normal de trabajo.

Ante esta circunstancia es necesario tener en cuenta:

1. Todas las empresas deberían tener un plan de contingencias para garantizar el derecho a la protección de datos cuando puedan llevarse a cabo tratamientos de datos fuera del entorno físico laboral.
2. En particular deben aplicar medidas técnicas y organizativas que garanticen la seguridad de la información en el tratamiento de datos.
3. Debe garantizarse que todos los dispositivos, como ordenadores, móviles o *tablets*, que vayan a manejar los empleados cumplen con medidas de seguridad.
4. Las redes de internet que vayan a utilizar los trabajadores en sus comunicaciones con la empresa o con clientes o terceros han de ser seguras.
5. Debe garantizarse que todo el personal que trate datos personales lo haga aplicando medidas de seguridad adecuadas.
6. Debe concienciarse a todo el personal acerca de la importancia de ser cautelosos con el tratamiento de datos personales. En particular, evitar que otras personas puedan acceder a los datos personales, ya que se podría estar vulnerando la confidencialidad, o se podrían borrar de manera no autorizada, vulnerando la integridad y disponibilidad de los datos.
7. Debe advertirse que en ningún caso pueden deshacerse de documentos que contengan datos personales si no es de modo seguro (nunca en las papeleras o “cubos de la basura” sino mediante destructores de papel).
8. Debe advertirse a todo el personal de la empresa que deben notificar de inmediato cualquier incidencia que pueda producirse en el tratamiento de datos personales.

En definitiva, el teletrabajo implica que la empresa tenga que haber adoptado medidas técnicas y organizativas para garantizar el tratamiento lícito de los datos de carácter personal que lleven a cabo sus trabajadores en cualquier lugar. Estos tratamientos tienen que cumplir con los requisitos aplicables en materia de protección de datos y seguridad de la información. Desde el uso de redes privadas virtuales (*Virtual Private Networks*, VPR por sus siglas en inglés), para proteger las comunicaciones entre el equipo portátil y la red de la empresa, hasta contemplar la aplicación de medidas de seguridad en dispositivos del propio usuario (*Bring Your Own Device*, BYOD por sus siglas en inglés) que pueda utilizar para trabajar.

#### **4. Régimen de inversiones extranjeras relacionadas con el sector del tratamiento de datos**

La Disposición final cuarta del Real Decreto-ley 8/2020, modifica la Ley 19/2003, de 4 de julio, sobre régimen jurídico de los movimientos de capitales y de las transacciones económicas con el exterior. En particular añade un artículo 7.bis por el que se regula la suspensión del régimen de liberalización de determinadas inversiones extranjeras directas en España.

Señala que a efectos de lo establecido en dicho artículo se consideran inversiones extranjeras directas en España todas aquellas inversiones realizadas por residentes de países fuera de la Unión Europea y de la Asociación Europea de Libre Comercio cuando el inversor pase a ostentar una participación igual o superior al 10 por 100 del capital social de la sociedad española, o cuando como consecuencia de la operación societaria, acto o negocio jurídico se participe de forma efectiva en la gestión o el control de dicha sociedad.

A continuación, dispone que queda suspendido el régimen de liberalización de las inversiones extranjeras directas en España, que se realicen en diversos sectores que afectan al orden público, la seguridad pública y a la salud pública.

Entre tales sectores:

1. (a) Las Infraestructuras críticas, ya sean físicas o virtuales, incluidas, entre otras, las **infraestructuras de tratamiento o almacenamiento de datos**, así como terrenos y bienes inmuebles que sean claves para el uso de dichas infraestructuras, entendiéndose por tales, las contempladas en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
2. (d) **Sectores con acceso a información sensible, en particular a datos personales, o con capacidad de control de dicha información**, de acuerdo con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Por otra parte, el apartado 5 del citado artículo 7 bis dispone que la suspensión del régimen de liberalización determinará el sometimiento de las referidas operaciones de inversión a la obtención de autorización y que las operaciones de inversión llevadas a cabo sin la preceptiva autorización previa carecerán de validez y efectos jurídicos, en tanto no se produzca su legalización.

En fin, el apartado 6 del mismo artículo dispone que la suspensión prevista en el mismo regirá hasta que se dicte Acuerdo de Consejo de Ministros por el que se determine su levantamiento.

## **5. Documentos de referencia sobre COVID-19 y protección de datos personales**

Los siguientes documentos, publicados por las autoridades de protección de datos, pueden utilizarse como referencias en materia de tratamiento de datos personales y COVID-19:

1. Informe 0017/2020 del Gabinete Jurídico de la AEPD sobre el tratamiento de datos personales en relación con la situación derivada de la extensión del COVID-19.
2. *Report 0017/2020 from the State Legal Service Department (the Spanish DPA) on processing activities relating to the obligation for controllers from private companies and Public Administrations to report on workers suffering from COVID-19.*
3. Preguntas frecuentes (FAQs) de la AEPD sobre el COVI-19.
4. Nota de la Agencia Catalana de Protección de Datos en relación con los tratamientos de datos personales relacionados con las medidas para hacer frente al COVID-19.
5. *Statement of the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak.*