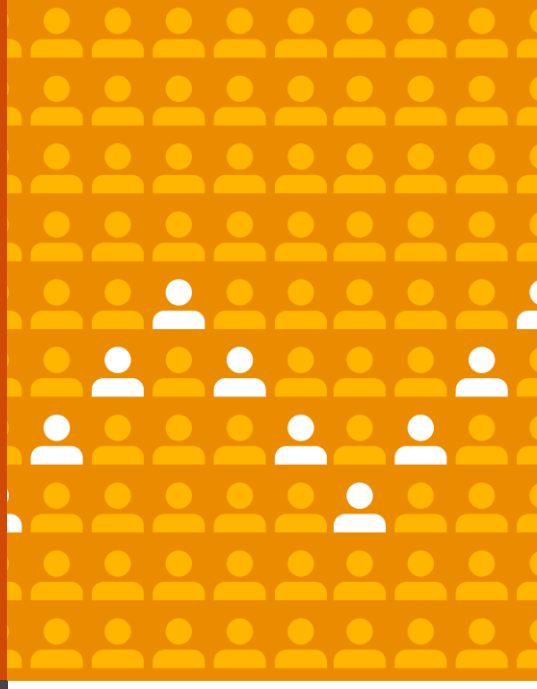
# Emergencia sanitaria: protección de datos, geolocalización y teletrabajo



**Analizamos el tratamiento de los datos personales de los trabajadores en la situación de emergencia de salud pública ocasionada por el COVID-19.**

Marzo, 2020


## Tu contacto en PwC Tax and Legal Services

**Assumpta Zorraquino**
Socia responsable de Regulación Digital
assumpta.zorraquino@pwc.com

**Alejandra Matas**
Directora en el área de Regulación Digital
alejandra.matas.brancos@pwc.com


El pasado 11 de marzo de 2020 la Organización Mundial de la Salud elevó a pandemia internacional la situación de emergencia de salud pública ocasionada por el COVID-19, requiriendo la adopción de medidas inmediatas y eficaces para hacer frente a los acontecimientos ante los que nos encontramos. Las circunstancias extraordinarias que concurren constituyen, sin lugar a duda, una crisis sanitaria sin precedentes y de enorme riesgo, tanto por el elevado número de ciudadanos afectados como por el inusual riesgo para nuestros derechos.

Esta situación de emergencia sanitaria, y la adopción del teletrabajo por parte de una parte significativa de los trabajadores, tienen implicaciones importantes en el ámbito de la Regulación Digital. En vista de lo anterior, para una mayor claridad y utilidad práctica, a continuación detallamos una serie de condicionantes y posibles escenarios, y analizamos la cuestión desde distintos prismas:

### 1. Protección de los datos personales

De acuerdo con lo indicado por la Agencia Española de Protección de Datos (en adelante, “AEPD”), en relación con el tratamiento de datos personales resultantes de la situación actual, en primer lugar y con carácter general, en situaciones en las que existe una emergencia sanitaria de alcance general, la protección de datos no debería utilizarse para obstaculizar o limitar las medidas que adopten las autoridades públicas, y en concreto las sanitarias, para luchar contra la pandemia en la que nos encontramos.
El Reglamento General de Protección de Datos (en adelante, “RGPD”) recoge en su Considerando 46 que debe entenderse lícito el tratamiento de datos personales cuando sea necesario para proteger un interés esencial, para la vida del interesado o de otra persona física. Ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado. Este último supuesto se da en aquellos casos en los que el tratamiento es necesario para fines humanitarios, incluyendo el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano.

En este sentido, habida cuenta de que el Gobierno Español ha declarado el estado de alarma por medio del Real Decreto 463/2020, de 14 de marzo con el fin de afrontar la situación de emergencia sanitaria ocasionada por el COVID-19, resulta razonable afirmar que nos encontramos ante la situación que recoge el Considerando 46 del RGPD.

Partiendo de esta base, de conformidad con lo dispuesto en el RGPD se podrán tratar los datos personales sin el consentimiento de los interesados, pues a pesar de que los datos de salud están catalogados en el RGPD como categorías especiales de datos, su tratamiento puede ampararse en las excepciones recogidas en el artículo 9.2 del RGPD.

> en situaciones en las que existe una emergencia sanitaria de alcance general, la protección de datos no debería utilizarse para obstaculizar o limitar las medidas que adopten las autoridades públicas.

En particular, dichas excepciones consisten en que se podrán tratar datos personales de los interesados sin recabar su consentimiento:

- Para cumplir con las obligaciones en el ámbito del Derecho laboral y de la seguridad y protección social. Los empleadores deberán cumplir con las obligaciones de prevención de riesgos laborales, por lo que el trabajador deberá informar al empleador en caso de sospecha de contacto con el virus con el fin de salvaguardar su propia salud y la de los demás (art.9.2.b).
- Para proteger el interés vital del interesado o de otra persona (art.9.2.c).
- Por razones de un interés público esencial (art.9.2.g).
- Para realizar diagnósticos médicos (art.9.2.h).
- Por razones de interés público en el ámbito de la salud pública (art.9.2.i).

Llegados a este punto, conviene apuntar que los tratamientos de datos personales, aún en esta situación de emergencia sanitaria como a la que nos referimos en esta nota, deben seguir realizándose en plena observancia de la normativa en esta materia, así como aplicando los principios que se recogen en el RGPD de licitud, lealtad, transparencia, limitación de la finalidad, exactitud, y minimización de datos. Sobre todo, este último principio merece especial atención, puesto que los datos tratados deberán limitarse a los exclusivamente necesarios para la finalidad pretendida sin que se pueda extender a otros datos personales no necesarios.

En suma, la normativa de protección de datos permite que el responsable del tratamiento adopte las decisiones que sean necesarias para salvaguardar los intereses vitales de las personas físicas.

## 2. Geolocalización de los ciudadanos por el Estado.

La Ley Orgánica 3/1986 de Medidas Especiales en Materia de Salud Pública (modificada mediante Real Decreto-ley 6/2020, de 10 de marzo) señala que "con el fin de controlar las enfermedades transmisibles, la autoridad sanitaria, […], podrá adoptar las medidas oportunas para el control de los enfermos, de las personas que estén o hayan estado en contacto con los mismos y del medio ambiente inmediato, así como las que se consideren necesarias en caso de riesgo de carácter transmisible".

Ello nos lleva, necesariamente, a plantearnos si el Estado Español estaría legitimado para geolocalizar a los ciudadanos durante el período de estado de alarma para prevenir la propagación del COVID-19. A pesar de que la legislación europea impide aplicar estas medidas de vigilancia de la población, el estado de alarma decretado en algunos países podría empujar a los gobiernos a emplear la tecnología de 'Big Data' para evitar la propagación. El mecanismo utilizado podría consistir en una aplicación móvil que los ciudadanos instalarían en sus smartphones a través de la cual el Estado podría geolocalizar a aquellas personas infectadas o con riesgo de ser infectadas.

A través de estas apps, a la vez que el usuario, aportando sus datos personales (domicilio, edad, sexo, teléfono o correo electrónico) y realizando el autodiagnóstico oportuno podría tener acceso a información general sobre la enfermedad, el Estado podría observar la distribución de los infectados en el mapa, mejorar la gestión de las acciones sanitarias, optimizar los recursos asistenciales o incluso, en última instancia, advertir a las autoridades si un usuario ha abandonado su domicilio infringiendo las normas gubernamentales limitativas de la libertad deambulatoria. .

> Las iniciativas de teletrabajo, deben adoptarse con las debidas garantías para asegurar la confidencialidad y la seguridad de los sistemas.

Tal y como hemos visto en el punto anterior, el artículo 9.2 del RGPD permite tratar los datos personales cuando, o bien el ciudadano presta su consentimiento, o bien cuando los sistemas de prevención médica o sanitaria lo determinen. En ese caso se cumple la legalidad y además es posible que los ciudadanos cedan sus datos a dichas aplicaciones, no solo para obtener un diagnóstico sobre su situación médica sino también para intentar eliminar el riesgo que conlleva esta "crisis sanitaria" para la sociedad.

Sin embargo, y tal como remarcábamos en el punto anterior, es esencial que se sigan respetando los principios recogidos en el RGPD, garantizando que los datos personales:

- Se utilizarán exclusivamente para este objetivo médico;
- Se emplearán para estos fines y no se venderán a terceros;
- Se limitarán los datos solicitados a los mínimos necesarios; y
- Se restringirá el tiempo de disponibilidad, almacenándolos durante el tiempo necesario para controlar la pandemia y una vez finalizada ésta, permanecerán debidamente bloqueados mientras pueda derivarse responsabilidades administrativas o jurisdiccionales.

Por todo ello, le corresponde a la administración cumplir con el principio de información, seguridad y transparencia para que de esta manera los ciudadanos puedan sentir que sus derechos van a mantenerse intactos. El estado de alarma decretado en España permite al Gobierno limitar ciertos derechos y libertades de los ciudadanos. La limitación de nuestra libertad de movimiento consistente en no permitir a los ciudadanos, salvo en casos excepcionales, salir de su casa, durará de momento 15 días, mientras que la utilización de los datos de los ciudadanos limita la privacidad, que se puede ver afectada durante mucho más tiempo.

### 3. Derecho a la intimidad y uso de dispositivos personales en el ámbito laboral

Por otra parte, las iniciativas de teletrabajo que se están promoviendo, y que en gran medida han de contribuir a dar continuidad al negocio, deben adoptarse con las debidas garantías para asegurar la confidencialidad y la seguridad de los sistemas y, a nivel organizativo, articular los correspondientes protocolos que prevean un adecuado control y monitorización, y se adapten las fórmulas de medición del desempeño y de cumplimiento de la jornada laboral.

Asimismo, es necesario establecer unas pautas de actuación cuando se utilicen no solo las herramientas corporativas, sino en particular cuando se contemple la posibilidad de trabajar desde dispositivos personales (BYOD), previendo eventuales incidencias, y situaciones de mayor exposición de la información confidencial de la compañía.

Todo ello, de acuerdo con lo establecido, entre otros, en los arts. 87.2 de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales y 32 del RGPD, esto es, que el acceso por parte de la compañía a los contenidos de los medios digitales facilitados deberá limitarse al control del cumplimiento de las obligaciones laborales o estatutarias, así como que éste deberá aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado garantizando la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas.

La situación de alerta generada a nivel mundial abre la puerta a ataques de phishing a través de servicios de mensajería instantánea, correos electrónicos y otros medios.

**4. Ciberseguridad en el teletrabajo**

Conviene tener en cuenta que la situación de alerta generada a nivel mundial abre la puerta a multitud de ataques de phishing a través de servicios de mensajería instantánea, correos electrónicos y otros medios. Los ciberdelincuentes aprovechan situaciones de miedo y alarma colectiva para sacar provecho, y nada indica que esta vaya a ser una excepción.

Los ciberdelincuentes tratarán de suplantar organizaciones legítimas con información relevante sobre el COVID-19 simulando prestar ayuda, acompañamiento y consejo: en la mayoría de los casos se solicitará que se abra un archivo o que se acceda a un enlace de internet para obtener información del usuario. Por ello es muy importante seguir las recomendaciones facilitadas por la AEPD, que reproducimos a continuación:

- Mantenerse informado mediante fuentes oficiales y confiables, acudiendo directamente a las webs de las instituciones.
- Verificar la dirección de correo electrónico remitente del mensaje.
- Evitar facilitar datos personales a través de webs a las que se ha accedido siguiendo un enlace contenido en un mensaje o correo electrónico.
- Desconfiar de mensajes con faltas ortográficas, errores gramaticales, saludos genéricos o solicitudes con urgencias injustificadas.