La consultora Evolvers explica la seguridad y la protección de datos personales en tiempos del COVID-19

El Comité Europeo de Protección de Datos ha realizado una declaración sobre el tratamiento de los datos personales, en la que destaca que la normativa sobre protección de datos no impide tomar medidas en la lucha contra el COVID-19

Tres días después de que la Organización Mundial de la Salud determinara que la situación del COVID-19 era una pandemia internacional, se decretó en España el Estado de Alarma para la gestión de la situación de crisis sanitaria internacional ocasionada por el coronavirus.

En esta desconcertante situación, en la que se ha restringido y limitado la plena efectividad de algunos derechos y libertades de los ciudadanos, el Derecho a la protección de datos personales no ha sufrido ninguna alteración. Evolvers, consultora legal y de negocio especializado en esta materia, aclara las principales cuestiones, de la mano de su experta Ainhoa Juárez Carreño.

Sin embargo, en el marco de esta crisis sanitaria, el Comité Europeo de Protección de Datos ha realizado una declaración sobre el tratamiento de los datos personales, en la que destaca que la normativa sobre protección de datos no impide tomar medidas en la lucha contra el COVID-19, sin olvidar que aquellos que traten información personal en estas circunstancias, deberán asegurar la disponibilidad, integridad y confidencialidad de la información.

Asimismo, la Agencia Española de Protección de Datos publicó el pasado 12 de marzo de 2020, un informe dando respuesta a preguntas frecuentes sobre protección de datos en el ámbito laboral, como consecuencia del COVID-19.

El informe coincide con lo establecido por el Comité Europeo y establece que la normativa de protección de datos personales es aplicable en su integridad en la situación actual ya que este derecho fundamental no se ha visto suspendido ni limitado por la situación del Estado de Alarma.

Las líneas de actuación que ha determinado la Agencia Española de Protección de Datos, con respecto al tratamiento de los datos de salud de los trabajadores, son las siguientes:

- El empleador tendrá derecho a conocer si algún trabajador está infectado o no por el COVID-19, atendiendo al principio de minimización de datos, para diseñar a través de su servicio de prevención de riesgos laborales los planes de contingencia que sean necesarios, o que hayan sido previstos por las autoridades sanitarias.

- Con la misma finalidad de prevención, la empresa podrá comunicar al resto de sus trabajadores la información relativa a posibles contagiados, no pudiendo identificar a la persona afectada.

- Asimismo, la empresa podrá solicitar información a sus trabajadores, teniendo en cuenta, en todo caso, el principio de proporcionalidad y limitándose a conocer, exclusivamente, las visitas que algún trabajador pudiera haber realizado a países en los que existe un alto riesgo de contagio del COVID-19, o con relación a si se manifiesta alguno de los síntomas de la enfermedad. No podrá, en virtud del principio de minimización de datos, preguntar a los trabajadores sobre otras cuestiones que no estén relacionadas con el COVID-19.

- Además, la Agencia Española de Protección de Datos establece la obligación de los trabajadores de comunicar a la empresa si han tenido contacto con un caso de coronavirus para que puedan aplicarse los protocolos establecidos por las autoridades sanitarias.

- Por otro lado, se permite también que el personal de seguridad pueda tomar la temperatura a los trabajadores con el fin de detectar posibles casos de coronavirus y verificar si el estado de salud de las personas trabajadoras puede constituir un peligro para ellas mismas y para el resto del personal.

Como se puede observar, el Derecho a la protección a la salud y el Derecho a la protección de los datos personales, ambos derechos fundamentales, conviven en armonía por el momento, si bien dese Evolvers -explica la experta -"no queremos olvidar que actualmente existen empresas que no pueden garantizar la seguridad de la información".

"Nuestro departamento de nuevas tecnologías y de protección de datos –explican desde el despacho jurídico- ha enviado a sus clientes una encuesta para poder realizar un análisis de riesgos, siendo el resultado el siguiente":

- El 80% de los clientes se ha acogido a la modalidad de teletrabajo

- El 70% de dichas empresas ha facilitado un ordenador personal al trabajador y el otro 30% teletrabaja utilizando su ordenador doméstico.

- Del 30% del uso de ordenadores domésticos, la mitad comparten el ordenador con el resto de su familia.

- El 100% se conecta al correo electrónico de la empresa y a la red corporativa con las redes domésticas Wifi.

- Respecto a los dispositivos móviles, el 95% son de uso personal y también se utilizan para trabajar.

Por ello, desde Evolvers, quieren lanzar las siguientes recomendaciones para que las empresas puedan minimizar los riesgos y garantizar la seguridad de la información, porque la Agencia Española de Protección de Datos no ha contemplado por el momento qué ocurre con aquellas empresas que han optado por instaurar el teletrabajo de forma extraordinaria.

No hay que olvidar que, el Comité Europeo de Protección de Datos aboga por garantizar la disponibilidad, confidencialidad e integridad de la información por parte de aquellas empresas u organizaciones que estén realizando un tratamiento de datos.

Es necesario que las compañías, ante esta situación extraordinaria, revisen si han establecido contraseñas seguras, si han actualizado el sistema operativo y las aplicaciones informáticas; si han bloqueado o cerrado correctamente las sesiones tras un tiempo de actividad determinado; que se realicen copias de seguridad diariamente; que sus trabajadores se conecten a través de redes que estén protegidas con contraseña; que accedan a sitios web con protocolo seguro y que procedan a la eliminación de información temporal, prestando especial atención a la carpeta de descargas y a la papelera de reciclaje; que las memorias USB, CD, DVD, sean desconectadas correctamente tras su uso; que se proceda al borrado del histórico de navegación, así como de las cookies y que se mantengan actualizados los teléfonos móviles, en los que únicamente deben instalarse las aplicaciones que tengan su origen en tiendas oficiales, más aún si el mismo teléfono es utilizado para trabajar y con fines domésticos.

Datos de contacto:

Agencia de comunicación MAD&COR
www.madandcor.com
675943952

Nota de prensa publicada en: [Madrid](#)

Categorías: [Nacional](#) [Derecho](#) [Hardware](#) [E-Commerce](#) [Ciberseguridad](#) [Dispositivos móviles](#)

NotasdePrensa

<https://www.notasdeprensa.es>