microlab
protección de datos

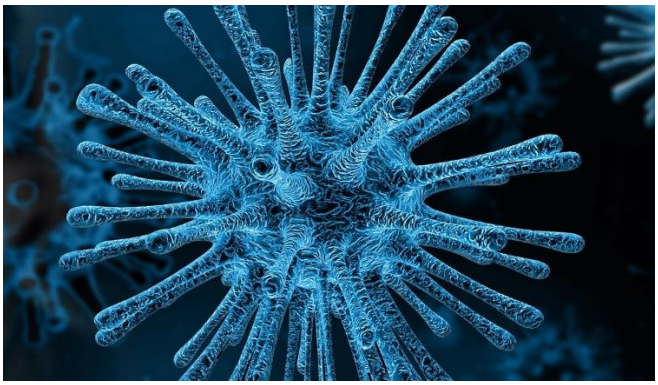
Newsletter. Julio de 2020

Prevención del COVID-19: ¿Qué puede hacer el empresario?

La pandemia del Coronavirus ha castigado a las empresas, que no solamente han visto paralizada su actividad sino que, además, deben cambiar su forma de trabajo para adecuarse a las recomendaciones sanitarias.

Estos cambios en la organización conllevan necesariamente el tratamiento de datos personales en el seno de la empresa, en especial de datos relativos a la salud de los trabajadores.

A continuación, detallaremos qué datos puede tratar el empresario para prevenir el contagio del Covid-19 en su negocio.



¿Puede el empresario solicitar información relativa a la salud a sus trabajadores?

Sí, el empresario puede preguntar a los trabajadores si están o han estado infectados por el coronavirus para evitar la propagación de la enfermedad. Además, para realizar este tratamiento **no es necesario el consentimiento de los trabajadores**, pues la base legal es la protección de intereses vitales del resto de los trabajadores.

No obstante, es preciso recalcar que las preguntas deberían limitarse exclusivamente a indagar sobre la existencia de síntomas, o si la persona trabajadora ha sido diagnosticada como contagiada, o a estado sujeta a cuarentena.

¿Puede la empresa informar al resto de trabajadores si un compañero se ha infectado?

Esto, conllevaría la cesión de categorías especiales de datos, por lo que la empresa debe actuar de forma prudente.

En primer lugar, se debería facilitar esta información al resto de la plantilla sin identificar al interesado.

Si no pudiera garantizarse la salud del resto de trabajadores sin identificar al interesado, podría proporcionarse la información identificativa, siempre en última instancia.

¿Puede tomarse la temperatura a trabajadores y clientes?

La fiebre o la febrícula no es un síntoma exclusivo del coronavirus, pudiendo estar causada por múltiples enfermedades. Por otro lado, muchos pacientes no desarrollan fiebre durante el proceso vírico. En definitiva, la fiebre no determina que una persona esté infectada por coronavirus, por lo que puede suponer un tratamiento excesivo y poco determinante para la finalidad perseguida, que es evitar el contagio.

Si bien **la empresa puede tomar la temperatura de sus trabajadores**, en base a las funciones de vigilancia de la salud que le otorga la normativa laboral, la Agencia Española de Protección de Datos se ha mostrado cauta y ha recomendado que las empresas estén a las instrucciones dictadas por el Ministerio de Salud antes de tomar la temperatura a **clientes y visitas**.

Teletrabajo: cinco claves para no comprometer la seguridad de la empresa

Esta crisis sanitaria ha obligado a miles de trabajadores a cambiar sus hábitos de trabajo y realizar su actividad laboral desde su domicilio, a veces incluso con sus dispositivos personales.

Para alcanzar el mismo nivel de seguridad conseguido en los locales de la empresa, es necesario seguir determinados protocolos que suplan las deficiencias en materia de seguridad que por su naturaleza tiene el teletrabajo.

1. **Revisión de los dispositivos utilizados para el teletrabajo**

Los dispositivos corporativos utilizados durante el teletrabajo deberán estar actualizados a nivel de aplicación, sistema operativo y software antivirus. El personal deberá tener los privilegios mínimos necesarios para el desempeño de sus funciones, no debiendo tener acceso a más información de la estrictamente necesaria.

Igualmente, será altamente recomendable incorporar mecanismos de cifrado de la información y deshabilitar las funciones y comunicaciones que no sean necesarias (lector de CD, Wifi, puertos USB…).

2. **Acceso a la red corporativa desde el exterior**

Para garantizar la seguridad es necesario monitorizar los accesos a la red corporativa con el ánimo de identificar patrones anormales de comportamiento, para evitar la propagación de malware o el acceso no autorizado.

3. **No utilizar los dispositivos corporativos para el ocio**

El personal no deberá descargar ningún software que no haya sido previamente autorizado por la organización, pues este tipo de conductas pueden ocasionar graves riesgos en la seguridad de la información.

Hace años, la Agencia Española de Protección de Datos sancionó a una clínica porque uno de los empleados se descargó Emule (programa de compartición de archivos) con la intención de descargarse una película y, sin darse cuenta, compartió los historiales clínicos de cientos de personas. Este, es un claro ejemplo de la importancia de utilizar los dispositivos corporativos únicamente con fines profesionales.

4. **Proteger la información frente a terceros**

Los dispositivos corporativos deben de estar fuera de la vista de terceros y el personal deberá bloquear la sesión cada vez que se desatiendan.

La misma protección merece la documentación en soporte papel. Esta no deberá estar al alcance de terceros cuando no se esté manejando, y no se deberá tirar a la basura sin previamente destruir las hojas de tal manera que la información sea irrecuperable.

5. **No conservar la información en local para evitar las brechas de seguridad**

Para prevenir la perdida de información es crucial evitar el almacenaje de información en local, debiendo utilizar siempre que sea posible los recursos de almacenamiento en red facilitados por la organización.

Es importante destacar que los empleados no deben utilizar servicios de nube no autorizados por la organización, como el correo particular o cuentas personales de Google Drive o Dropbox.

Sancionan a Glovo por no designar un delegado de protección de datos

La empresa española, que se dedica al reparto a domicilio de todo tipo de productos, **ha recibido una sanción de 25.000 €** por incumplir la obligación de designar un delegado de protección de datos (DPD).

La AEPD ha afirmado en su resolución que Glovo debería contar con esta figura, al realizar un tratamiento de datos personales a gran escala. Esta empresa cuenta con más de un millón de clientes en España, siendo una de las aplicaciones favoritas de los usuarios españoles para pedir comida a domicilio.

Si bien **el concepto de gran escala no está definido en la normativa** (causando cierta inseguridad jurídica), el Comité Europeo recomienda tener en cuenta distintos factores para determinar si el tratamiento se realiza a

gran escala, como el número de interesados afectados, el volumen de datos, el alcance geográfico o la duración del tratamiento.

Por su parte, Glovo ha alegado que, si bien no ha designado un DPD, cuenta en su organización con un **Comité de Protección de Datos que lleva a cabo las funciones propias de esta figura**, por lo que piensa agotar todas las instancias judiciales, al considerar que no ha incurrido en el incumplimiento de la normativa de protección de datos.

Esta resolución sancionatoria surge tras dos reclamaciones interpuestas por clientes de la plataforma, que consideraron que no se cumplían todas las garantías de cumplimiento.

El Ministerio de Trabajo publica el anteproyecto de Ley de trabajo a distancia

Este texto legal pretende regular el trabajo a distancia y el teletrabajo, centrando su redacción en los derechos de los trabajadores y fijando aspectos relacionados con la intimidad del trabador y el derecho a la protección de datos personales.

Para cumplir correctamente con la normativa de protección de datos, detallaremos los aspectos más relevantes de este anteproyecto en materia de privacidad:

- El control de los trabajadores mediante dispositivos automáticos y el uso de medios telemáticos deberá garantizar el derecho a la intimidad y a la protección de datos de los trabajadores, debiendo asegurarse la **idoneidad, necesidad y proporcionalidad** de los medios de control utilizados.
- La empresa no podrá exigir la instalación de programas o aplicaciones en dispositivos propiedad del trabajador, ni la utilización de estos dispositivos en el desarrollo del trabajo a distancia.
- Las personas trabajadoras podrán hacer un uso personal de los equipos informáticos puestos a su disposición por parte de la empresa, teniendo en cuenta los usos sociales y las particularidades del trabajo a distancia. No obstante, los términos de del uso personal deberá especificarse a través de la negociación colectiva o los acuerdos de empresa.
- **Derecho a la desconexión digital.** La empresa debe garantizar la desconexión y limitación absoluta de los medios tecnológicos de comunicación empresarial y de trabajo durante los periodos de descanso, así como el respeto a la duración máxima de la jornada. los medios y medidas adecuadas para garantizar el ejercicio efectivo del derecho a la desconexión en el trabajo a distancia deberán fijarse mediante negociación colectiva o acuerdo de empresa.

Abogada sancionada por reutilizar documentos con datos personales en el reverso

La Agencia Española de Protección de Datos ha impuesto una sanción de 2.000 € a una abogada por reutilizar papel con información de otros clientes en el reverso, que incluía datos personales.

Si bien el reverso de los documentos contenía datos personales de clientes anteriores, la abogada reutilizó estos documentos con la intención de abaratar costes, lo que constituyó el incumplimiento del **principio de integridad y confidencialidad** consagrado en el Reglamento General de Protección de Datos, que obliga a los responsables a garantizar "*una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.*"

De esta resolución se destaca la importancia de la seguridad de la información, a veces relevada en las organizaciones por desconocimiento o falta de medios.

Editado por Microlab Hard

Madrid. C/ Cronos 8, 1º, Madrid

Barcelona. C/ Santiago Rusiñol 8, Molins de Rei