COVID 19: CRISIS MANAGEMENT

IT security & data protection in times of Corona (CoVid19)

DEKRA

In most companies, the current Covid 19 crisis is leading to a rapid increase of people working from home. Obviously, home office has a lot of advantages such as ensuring the continued operation of administrative business processes. At the same time, working from home creates new challenges in the area of IT security and data protection for those organizations and their employees.

For your convenience, we have compiled some recommendations for business owners, entrepreneurs and employees.

1. DATA PROTECTION AND CORONA (COVID19) A QUICK GUIDE FOR SMES.

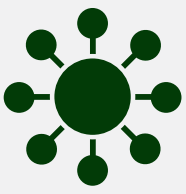
Validity of GDPR (General Data Protection Regulation)

In principle, all requirements of GDPR are still valid. As a reminder, GDPR gives a legal framework for processing personal data by private and public data processors and, therefore, ensures the protection of personal data and the free movement of data within the European Union and organizations doing business in the EU. Non-compliance can result in fines of up to 20 million euros or up to four percent of annual worldwide group revenue.

In the current Covid 19 crisis, health data of employees may need to be gathered in order to combat the pandemic effectively and further processed to authorities. This has to happen in compliance with the data protection regulation which is listed below.

Possibility of collecting private contact details of employees by the employer

Current private contact details of employees (mobile phone numbers, email addresses, etc.) may be requested by employers and can be temporarily stored provided the intent, such as faster communication during the pandemic, is clearly defined and the employees' consent has been obtained.
The employer is obliged to delete this information as soon as the pandemic has ended. Employees need to be informed accordingly, especially regarding to the duration of storage. The state-of-art deletion periods should therefore be limited to 8 weeks since the incubation period is currently considered to be 2 weeks and a safety period of 6 weeks should be enough. Consequently, after 8 weeks the purpose for retaining the information is expired, unless data has been requested by public authorities for processing in between.

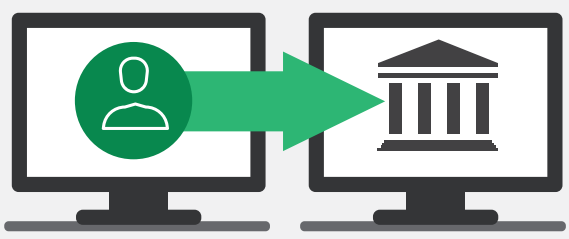


Further processing of personal information by employers in case an employee visited a defined risk area or had direct contact with someone that tested positive for the virus

The employer may ask for personal information if it is collected to protect the workforce from infection. Examples include where the employees spent their vacations or if they had contact with people that tested positive for the virus.

Handling of and passing on information in the event an employee has been infected

1. In the workforce
It is absolutely not recommended to mention infected employees by name in front of your workforce. Other employees who have been in touch with the infected person though, should be released from work and, if possible, sent to home office immediately. If those measures cannot be successfully (and expediently) implemented, the name of an infected person can be given in order to identify the source of infection. This can only happen in absolutely exceptional cases and only after consultation with local health authorities.



2. Transmission of information to authorities
If authorities request specific information, e.g. about infected employees, the employer is obligated to comply and provide the requested information.

(due to protection of personal data - defined by GDPR)

On request by health authorities, to provide visitor data from recent visitor logs or system in cases where infected personnel and locations have been identified.

As soon as an official order or decree is issued, the organization should comply and pass on the requested personal data from visitor logs/systems. However, the purpose has to be clearly defined as necessary to reduce exposure to individuals or the public. If there is no order or decree, but the organization has the consent of the visitors, they are free to share this information with the authorities or not.

Data collection and transfer from service providers (e.g. hospitals, doctors) to health authorities

Health care providers are required to pass on the following information, if available, to the public health department:

- Name and first name,
- Sex,
- Date of birth,
- Address of the principal residence
- Further contact details,
- Diagnosis or suspected diagnosis,
- Day of the illness, the date of the disease, the date of diagnosis and, where appropriate, the date of death, and time or period of infection.
- Source of infection (Country, District, City)