contrast

HR • APRIL 2020

Antivirus measures in the workplace.

What you need to know.

The outbreak of Covid-19 requires you as an employer to take measures to prevent a possible spread of the virus in the workplace.

In this context, you may now be processing additional personal data about your employees (e.g. about recent trips, their medical background, possible symptoms of illness).

However, the European Data Protection Board points out that this still has to be done in compliance with the data protection rules. For example, you must have a *legitimate ground* for this processing (for more information see GDPR toolkit – legitimate grounds). In Belgium, according to the Belgian Data Protection Authority, there is currently no reason for a broader or systematic application of the ground contained in Article 6.1 d) GDPR (*« necessity of processing in order to protect the vital interests of the data subject or of another natural person »*). In addition, for data concerning health, the Authority refers to the ban on processing of Article 9 GDPR, which requires the explicit consent of the data subject. The Authority points out that the exception to this rule on grounds of public health only applies if you are acting *« in implementation of explicit guidelines imposed by the competent authorities ».* In other countries you may have more options based on national law/national measures. Furthermore, even in these circumstances, the *principle of data minimization* requires that you not process more data than necessary, while the *principle of transparency* requires that you inform data subjects, in particular about the purpose of the processing and the retention period for the data (for more information see GDPR toolkit - transparency).

In addition, you are probably trying to have your employees telework as much as possible. Teleworking is recommended in the fight against the Covid-19 virus, but in turn it increases the risk of digital viruses. Employees use personal laptops with less effective antivirus software and connect to the company via a less secure internet connection. In Belgium, the Centre for Cybersecurity also warns against the many phishing messages that exploit the interest in news about the Covid-19 virus. Additional measures are therefore required to meet your security obligation and prevent data breaches.

contrast

What you need to do.

In general, one should minimize the processing of (sensitive) personal data as much as possible. For example, according to the Authority, the data protection rules do *not* prevent you from e.g. checking the body temperature of your employees (so long as this check is not accompanied by a recording of this data). In the same vein, it should also be permissible to have your employees complete a medical questionnaire, so long as the anonymity of the answers can be ensured.

Any processing of personal data in the fight against the Covid-19 virus requires the (explicit) consent of the employee. You can therefore *ask* employees to report any information that may be relevant in that context, but not oblige them to do so. Furthermore, it is advisable to appoint a single central contact person who receives the information concerned and not to distribute the information more widely than necessary within the company (e.g. only to employees who have worked closely with the data subject). In most cases, it will not be necessary to disclose the identity of the data subject. In any case, keep the information to a minimum and do not retain it for any longer than is required for fighting this pandemic. Inform your employees about the processing via a specific message on the intranet or by e-mail.

Furthermore, make sure that you organize the telework in a safe way. Let employees work as much as possible with secured company laptops and encrypted USB sticks. Provide an optimally protected VPN connection and multi-factor authentication. Ask your employees to verify that the (antivirus) software is always up to date, to make regular backups and to be especially careful when opening attachments to e-mails and hyperlinks. In view of the accountability of your company, it is advisable to include these rules regarding teleworking in your security policy.