Data protection and employment in times of the Corona pandemic

May employers collect private mobile numbers or other private contact details from employees in order to be able to warn or urge employees to stay at home at short notice in the event of plant closure or similar cases?

In the opinion of the State Commissioner for Data Protection and Freedom of Information of Baden-Wuerttemberg ("Data Protection Supervision BW"), this is ONLY permissible with the consent of the employee. Also in our opinion, no other permission norm is applicable.

May employers collect and process information on whether an employee was in a risk area or had direct contact with a sick person, etc.?

The Conference of the Independent German Data Protection Authorities of the Federal Government and the Federal States (German abbr.: "DSK") and the Data Protection Supervision BW affirm this by referring to the duty of care of the employer, as stipulated in the German Occupational Safety and Health Act (German abbr.: ArbSchG). This duty of care also applies to the personnel as a whole. The employer must respond appropriately for the purpose of medical precaution to protect the personnel. The employer can only guarantee this if he has sufficient information about potential risks of infection in his own company. In our opinion, too, the interests of the employee do not outweigh the risks for all employees. In practice, we recommend that when using survey forms, care should be taken to ensure that only those questions are listed in the questionnaire, which are directly related to the above-mentioned purposes (stay in the risk area or contact with sick persons).

Are employers allowed to inform employees that a certain employee has fallen ill with the virus, even mentioning the specific name, in order to exempt possible contact persons on this basis?

YES, BUT: In the opinion of the Data Protection Supervision BW, mentioning the name of the infected employee is ONLY permitted in an extreme emergency due to the stigmatizing effect this would have. Initially, the employer is only required to inform the department/team of the infected employee without mentioning the employee's name. If this procedure does not promise success, the employer must inform the public health department of the infection or the suspected infection and request instructions on how to proceed. If the public health department cannot be contacted (e.g. due to line overload) or if this procedure does not promise success, the employer can, as an ultima ratio, disclose the name of the infected employee to the other employees in the company.

This is not a practical approach. In case of an infection of an employee in the company, it is imperative to identify the possible contacts of the infected employee. For this purpose, it is usually necessary to disclose which employee had contact with the respective employee.

Furthermore, the question of data protection law regarding the permissibility of disclosing the name of the infected employee cannot be left to the health authorities.

May an employer whose employees work from home disclose the employee's home address to customers of the employer so that they can, for example, send forms to be recorded directly to the employees?

NO. The transmission of the private address of an employee to customers of the employer is normally not required for the execution of the employment relationship (Art. 26 (1) BDSG [Federal Data Protection Act]). The communication can easily be effected via the employer. This is also to be expected of the employer in view of the costs and the effort involved. Thus, the employer always has an alternative that encroaches less on the employee's personal rights.

Of course, the employer can ask for the employees' consent to a direct sending of the forms from the customers to the employees. Here, however, special attention must be paid to the voluntary nature of the consent.

Which special measures must an employer take in terms of data protection law if he allows employees to work remotely?

The employment relationship between the employer and the employee determines the data protection assessment of the remote work regulations. This does not change the data protection roles of those involved. The employer is the controller (Art. 4 No. 7 GDPR) and the employee is part of the controller. The physical separation does not eliminate the employee's involvement in the area of responsibilities of the controller. The controller must therefore understand the remote work "zone" as an extension of his or her own business in terms of premises and IT technology. Of particular importance in this context are the technical-organizational measures ("TOM"). According to Art. 25, 32 GDPR, the controller is obliged to implement these security measures to protect data.

First, the employer should determine basic rules for handling the operating resources (hardware and software). In particular, the private use of company resources (e.g. private Internet surfing, video streaming services) should be prohibited. At the same time, the employer should prohibit the processing of company data on private devices (e.g. laptops). Both measures should ensure that data remain within the company’s infrastructure. Furthermore, logging can also ensure that it is always possible to trace how data is processed in individual cases.

The actual use of operational resources should also be regulated. For example, passwords or data must not be disclosed to members of the employee's home community. Furthermore, provisions should also be made for the security precautions to be taken by the employee. In particular, the employee must ensure that unauthorized third parties do not have access to the company's resources and printouts and that any printouts are disposed of in accordance with data protection regulations.

The **MELCHERS DATA PROTECTION TEAM**- Dr. Dennis Voigt, Johannes Fischer and Albert Noll- will provide you with fast, effective and professional support in all questions concerning data protection.