Recommendations and background: data protection in the time of Covid-19

Article by Dr Carlo Piltz and Moritz zur Weißen

The rapid spread of coronavirus (Covid-19) and the efforts to combat the spread of this epidemic make it necessary for both public agencies and private businesses to consider certain aspects of data protection law. For this reason, we have prepared a series of practical recommendations on this topic, as well as analyzing the background.

Our practical recommendations:

- Follow the recommendations of public health officials and the Robert Koch Institute. Only organized actions will have a significant impact on the spread of the virus.
- Take adequate measures to protect your employees. First assess the risk and then decide whether to have employees work from home, whether it makes sense to monitor your employees for fever or whether it is enough to provide general information about hygiene. Having employees work from home may be a sensible precaution, particularly for members of at-risk groups.
- If you find it necessary to circulate a questionnaire asking employees or visitors to your company whether they have been to at-risk areas or have had contact with infected persons, formulate the questions in the negative (e.g. Have you not been to any of the following at-risk areas in the past 14 days?).
- If temperature measurements are taken before anyone can be admitted to the company grounds, the measurement data should not be stored in order to avoid "processing" in terms of data protection law. If visitors refuse to have their temperature taken, entry may be denied based on the owner's right to control access to the property. If employees refuse to have their temperature taken, they may be sent to work from home after weighing the various risks.
- If employees inform you that they are infected, that they have been to at-risk areas or that they have had contact with infected persons, you should send them home in every case and advise them to contact the authorities. It is important for the affected person to report the case by phone; companies are not currently required to notify the authorities themselves.
Background: What is data concerning health?

Article 4 No. 15 of the GDPR defines "data concerning health" as personal data relating to the physical health or mental health of natural persons, including the provision of health care services, which reveals information about the status of their health. In accordance with Article 9(1) of the GDPR, data concerning health is a specific category of personal data which is subject to stricter processing restrictions than "normal" personal data. This data may only be processed if the exceptions cited in Article 9(2) of the GDPR apply.

Examples of data concerning health include records of temperature measurements or symptoms, information about medications taken and specific information about infections.

What is the legal basis for processing data concerning health?

For the most part, companies may only process data concerning health based on consent in accordance with Article 9(2)(a) of the GDPR, if processing is necessary for purposes of preventive or occupational medicine or to assess the employee's working capacity in accordance with Article 9(2)(h) of the GDPR or, and this is much more rare, if processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health (Article 9(2)(i) of the GDPR in conjunction with § 22(1) No. 1(c) of the Federal Data Protection Act).

Data concerning health may not be processed for performance of a contract (Article 6(1)(b) of the GDPR or based on a legitimate interest (Article 6(1)(f) of the GDPR), as no such exemptions are cited in Article 9(2) of the GDPR. As a result, companies are increasingly finding themselves torn between the need to take measures to contain the virus and the need to protect their employees and comply with data protection law.

However, health data arising from an employment relationship may be processed in accordance with § 26(3) of the Federal Data Protection Act if such processing is necessary for the exercise of rights or performance of duties in labor law or social security law or for social protection. This is only the case if there is no reason to assume that these considerations are outweighed by legitimate interests of the data subject in excluding processing. In other words, it is necessary to weigh the need for processing against the interests of the data subject, while respecting the employee's privacy.

Lower hurdles for classification as data concerning health

The systematic storage of data concerning possible virus symptoms may be sufficient for classification as data concerning health. In general, data concerning health may only be collected (and therefore processed), e.g. by
questionnaire, based on the consent of the data subject in terms of Article 9(2)(a) of the GDPR. It should be kept in mind that this consent must be provided expressly, voluntarily and in a clearly informed manner, and it may be revoked at any time. The requirement for voluntary consent raises problems, particularly in the context of an employment relationship. Consent is only voluntary if there is no pressure or compulsion and if the data subject suffers no negative consequences from refusing consent. If an employer asks an employee to provide information about a possible infection, the possibility typically cannot be dismissed that the employee will feel a certain amount of pressure to comply with the request. Accordingly, the processing of data concerning health based on consent is problematic, particularly within the context of an employment relationship.

**Duties of the employer as the basis for necessary data processing**

In accordance with the provisions of § 618(1) of the Civil Code, employers are required to ensure that their employees are adequately protected from infection by other employees. This protective duty for the employer extends not only to the employee's co-workers, but also to possible infection by third parties with whom employees come into contact while adhering to regulations. If there is a concrete possibility of inflection, the employer is required to take appropriate countermeasures, particularly in the health care sector. Such measures may include e.g. educating employees about existing risks and ways to prevent the realization of those risks.

For measures to be taken, a concrete risk must exist in light of the specific working environment. The public health authorities refer to the criteria used by the Robert Koch Institute (RKI) for the purpose of risk assessment. The RKI has defined criteria for at-risk areas with regard to coronavirus, under which the employer is required to take preventive measures if an employee has been to an at-risk area or had contact with infected persons. Otherwise, the employee cannot be compelled to provide information.

**What are appropriate measures for companies?**

Accordingly, companies are required to take appropriate measures to protect employees (and third parties) from possible inflection. Requiring all employees to provide other employees with information about travel times and destinations or health status, or even requiring them to report any flu symptoms, is impermissible in the absence of a legal basis in data protection law.

However, companies are free to define stricter rules e.g. for controlling entry into the building or checking employees' temperature. As long as the associated data is not stored, this activity is likely not subject to data protection law. In any case, taking someone’s temperature likely does not qualify as data processing as long as
the measurement results are not recorded. The mere act of taking someone's temperature likely does not qualify as data processing and therefore would not be subject to the requirements of data protection law. Only if the measurement data is stored for an extended period of time would a legal basis be required for the processing of systematically collected data.

In the case of entry control, processing of "normal" personal data like the visitor's name can be justified based on legitimate interest in accordance with Article 6(1)(f) of the GDPR. If visitors must also have their temperature taken before being admitted, the above statements apply here as well. If the measurement results are not stored, there is no need for a specific authorizing statute. If the data is to be stored, it is necessary to obtain the express consent of the data subject in accordance with Article 9(1)(a) of the GDPR or an official order in accordance with Article 9(2)(i) of the GDPR in conjunction with § 22(1) No. 1(c) of the Federal Data Protection Act.

Collection of risk data using an Excel spreadsheet, i.e. asking people whether they have been to an at-risk area or had contact with an infected person in the last 2 weeks (the maximum incubation period) may be based on a legitimate interest in accordance with Article 6(1)(f) of the GDPR with regard to "normal" personal data such as names. Ideally, questions about risk criteria should be formulated in the negative (e.g. I have not been to any of the at-risk areas in the past two weeks) and should entail a binary response, either "yes" or "no." In this way, all indications are that the information provided would not be regarded as data concerning health, so that an additional exemption in accordance with Article 9(2) of the GDPR would not be required. Asking about risk criteria is also deemed permissible by the Irish supervisory authority.

Based on the risk of possible infection for those meeting the personal and geographical risk criteria, processing of employee health data by the employer is likely justified based on § 26(3) of the Federal Data Protection Act (in order to carry out statutory duties arising from the employment relationship). However, it is necessary to weigh the need for processing against the employee's right to privacy.
Additional information:

- [Telemedicus: Covid-19 und Datenschutz: Welch Maßnahmen dürfen Arbeitgeber treffen?](#)
- [Statement by the Irish supervisory authority](#)
- [Statement by the supervisory authority in Luxembourg](#)
- [Statement by the French supervisory authority](#)

About us:

Reuschlaw Legal Consultants advise companies active on a national and international scale in more than 30 countries in the areas of product liability, product safety law, recall management, insurance law, cybersecurity and data protection, compliance management and contract law.

**Company contact:** Melanie Schaumann | Head of Marketing & Communications | T: +49 30 / 2332895 0 | E: melanie.schaumann@reuschlaw.de