

## GDPR and COVID-19: What Companies Need to Know About Data Privacy

***Effective measures to combat data risks resulting from COVID-19 include processing personal data, but companies must balance privacy rights and employee health.***

German data protection authorities have published initial guidance to companies that process personal data, outlining how they should protect their employees and their businesses from risks resulting from COVID-19. Under the EU General Data Protection Regulation (GDPR), health data or other information about virus infections is treated as sensitive data according to Art. 9(1) GDPR. Such sensitive data may only be processed if the controller meets strict requirements with regard to such processing. Such data processing may be lawful if the processing is necessary for carrying out the controller's obligations in the field of employment law. Obviously, employers have a fiduciary duty to protect their employees from exposure to COVID-19, however, the respective use cases and the potentially applicable provisions of the GDPR are complex and challenging. Moreover, employers in Germany need to observe additional requirements stipulated in the German Federal Data Protection Act (*Bundesdatenschutzgesetz – BDSG*). Companies should also observe respective guiding principles deriving from well-established German case law with regard to employee data privacy.

### Data protection authority guidance

The German Federal Data Protection Commissioner has presented an initial [statement](#) covering this complex topic, which summarises the general positions of the Federal authority. The State Commissioner of Baden-Wuerttemberg has published a more detailed [FAQ](#) in German language. Similarly, the State Commissioner of Rhineland-Plate has published detailed [guidance](#) on employee data protection in this context. The State Commissioner of Lower Saxony has published [information](#) for employers in the public and private sector. Other EU Member State data protection authorities have also published similar guidance covering their jurisdictions and their individual GDPR implementation and other data protection laws. A statement of the Chair of the European Data Protection Board on the processing of personal data in the context of the COVID-19 outbreak can be downloaded [here](#).

### Data protection Q&A table

Latham has analysed the guidance provided by authorities and formatted an easy-to-understand overview in a concise Q&A table. This overview reflects the typical questions companies may face when dealing with the challenges of COVID-19, and covers the use cases that regularly arise in the context of

aligning employees' occupational health with the privacy rights of their co-workers and business continuity needs. The Q&A table can be downloaded [here](#).

## **Determining which privacy requirements apply to individual cases**

Needless to say, when deciding how to proceed in individual cases, companies need to take into account all requirements under the applicable data protection laws. For instance, when determining what scope of data processing is necessary within the meaning of the GDPR, companies need to observe the data processing principles according to Art. 5 GDPR, in particular the principles of data minimisation and transparency.

Hence, use of the Q&A table does not substitute an individual analysis of personal data being processed to mitigate the impact of COVID-19. When implementing effective measures to prevent infections in the workplace, companies should take a practical approach. At the same time, companies must be aware that privacy is a fundamental right that is not suspended, even in the course of a far-reaching pandemic. Consequently, companies should transparently inform employees and customers of such COVID-19-related specific purposes, and by what means companies process this personal data. Moreover, companies should observe the general requirements of the GDPR and document precisely any data-processing activities and respective legal analyses.

## **Remote working and other typical data privacy considerations**

Many data privacy-related risks relate to IT security. For instance, cybersecurity criminals may use the current global situation to infiltrate company systems. While remote working may be an effective means to avoid further spread of COVID-19, companies should be aware of vulnerabilities resulting from remote work. For instance, IT security teams may need to be on-site in order to quickly and effectively counter penetration attempts.

Remote working creates additional challenges with regard to IT security and confidentiality. Criminals may also exploit the current situation in COVID-19-related phishing attempts. Moreover, working from home on a laptop requires different security measures than working in a typical workspace environment, therefore companies should inform and train their employees accordingly. The European Union Agency for Cybersecurity has published a helpful [overview](#) with top tips for cybersecurity when working remotely.

---

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

**Tim Wybitul**

tim.wybitul@lw.com  
+49.69.6062.6560  
Frankfurt

**Dr. Wolf-Tassilo Böhm**

wolf.boehm@lw.com  
+49.69.6062.6558  
Frankfurt

**You Might Also Be Interested In**

[General Meetings During the COVID-19 Crisis in Germany](#)

[COVID-19 in Germany: Immediate Measures to Gain State Aid Financing \(KfW Credit et al\)](#)

[How Germany Is Addressing Short-Time Work in the COVID19 Crisis](#)

---

*Client Alert* is published by Latham & Watkins as a news reporting service to clients and other friends. The information contained in this publication should not be construed as legal advice. Should further analysis or explanation of the subject matter be required, please contact the lawyer with whom you normally consult. The invitation to contact is not a solicitation for legal work under the laws of any jurisdiction in which Latham lawyers are not authorized to practice. A complete list of Latham's *Client Alerts* can be found at [www.lw.com](http://www.lw.com). If you wish to update your contact details or customize the information you receive from Latham & Watkins, visit <https://www.sites.lwcommunicate.com/5/178/forms-english/subscribe.asp> to subscribe to the firm's global client mailings program.