Home Office - Labor Law, Data Protection and Cyber Security

The COVID-19 pandemic has been requiring many employees to move to home office. Given our current experiences with home office, it is further expected that even in the “Return to Work” phase, home office will remain a part of our work environment. Data protection authorities around the world have acknowledged the important public interests in fighting and handling the pandemic, however, the rules under data protection law are not suspended despite these unprecedented times. Addressing data protection and cyber security even in home office set-ups should still be at the radar of companies. Employers are also advised, if not even required, to put in place an individual home office agreement with the employees and, as the case may be, with the works council, to establish clear rules for working from home. A secure home office infrastructure and compliance with general data protection principles is the responsibility of both, the company as well as each employee. The following describes key aspects from a labor law, data protection and cyber security perspective for home office set-ups.

1. Individual Home Office Agreement

From a labor law perspective, the employer does not have a right to unilaterally order an employee to work from home unless the employment contract provides a right for the employer to do so. In most cases the employment contracts do not grant such a right to the employer. Thus, in principle the employee must work from a work station at the office and employer and employee will need to enter into an amendment agreement to the employment contract if the employer wants the employees to work from home during the current crisis or in similar situations.

Likewise, if an employee wants to work from home in the current crisis because of health reasons or child care challenges (closed schools or kinder garden), the employee requires the approval of the employer and cannot unilaterally decide to move to home office.

Thus, it is strongly recommended that employer and employee enter into an individual home office agreement, which among many other things stipulates whether home office is offered voluntarily to the employees, is mandatory, for how long home office is offered voluntarily or is mandatory, and whether the employer has a right to revoke the right to work from home. Other key aspects of such an individual home office agreement are summarized below.
2. Works Agreement

If a works council exists and if the employer wishes to ask not only one but a larger number of employees to work from home, consultation with the works council is required and is to be laid down in a respective works agreement.


When working from home, existing working time agreements, regulations on breaks and rest periods continue to apply. Thus, the individual home office agreement must require the employees to record and report their working times, breaks and rest periods either manually or via an IT tool.

For permanent home office set-ups (i.e., tele-working set-ups), the Federal Labor Court held that workplace health and safety regulations continue to apply with the consequences that the employer must provide - and pay for - appropriate furniture (e.g., office desk and chair), IT equipment (e.g., laptop, printer, monitor), sufficient space and light, Internet access, telephone service, electricity, partial rent, etc. Furthermore, the employer has the duty to check regularly whether the home office workplace complies with health and safety rules (and the employee must be required in the individual home office agreement to permit and tolerate such checks).

For temporary home office set-ups (i.e., as currently predominantly the case), it is unclear whether the workplace health and safety regulations continue to apply for the home office workplace. If the employer does not have the contractual right to enter an employee's private home, he cannot be held liable for compliance with health and safety regulations. If an employee works from home only occasionally or temporarily and if the employer provides an office workspace for the employee, there are strong arguments that the employer shall not be required to provide and pay for the furniture, equipment etc. for home office, as the employer does so already for the office workspace. Otherwise, the employer may not have an incentive to permit home office set-ups. For the current situation, it is, thus, strongly recommended that employers clarify in the individual home office agreement that employees are still free to use their designated office workspace which is fully equipped and that home office is offered only voluntarily and temporary without an obligation of the employer to equip the home office.

4. Restrictions for Home Office in Customer Contracts

To the extent, the company acts as a processor for its customers, the customer contracts, in particular the data processing agreements between the company as processor and the customer as controller may provide for home office restrictions. For example, the technical and organizational measures in a data processing agreement may restrict the location from which the customer's personal data can be processed to the company's office location. Those contractual restrictions must be assessed to determine whether an employee can perform his/her tasks remotely from home. Furthermore, any such customer contract may prescribe additional security measures and audit rights which must be flown down to the employees in the individual home office agreements when working from home. This can include a right of the employer to audit the home office set-up of the employee in order to verify
compliance with data protection and cyber security rules as imposed on the employee in the individual home office agreement. Such an audit right must be well-balanced against the employee's right of protection of the home.

5. Continued Application of Data Protection and Cyber Security Requirements

Requirements under data protection and cyber security continue to apply as well in a home office set-up. The German data protection authorities have issued several guidelines on key data protection and cyber security aspects that must be considered and complied with in a home office set-up (see references below). We have summarized below such home office-specific aspects as mentioned in those guidelines and those aspects should be applied in addition to common IT security requirements as typically described in an IT security policy or in a policy for technical and organizational security measures (such as internal security breach reporting obligations, employee commitments to data protection and data secrecy, access right concepts, contact details for data protection and security related questions, etc.).

Companies should consider such data protection and cyber security aspects either in the individual home office agreement or at least in a home office policy.

a) Home Office Desk and Paper Documents

In order to prevent unauthorized third parties, in particular other household members, from accessing and reviewing documents containing personal data, the employee should be required to have a dedicated home office workstation, ideally in a separate room. Documents and printouts containing personal data should be limited as much as possible and strictly separated from private documents. Documents containing sensitive data should not be in paper form at all. When leaving the home office desk, such documents must be retained in a secured container or locker to prevent access by other household members. Documents must not be disposed in the regular trash but securely shredded, e.g., bringing them to the office at some point for secure disposal.

When setting up the home office workstation, windows and other angles that may allow neighbors as well as other household members looking at the laptop screen must be considered. Appropriate screen protection should be applied. Work stations must be configured with appropriate screen savers whenever the employee leaves the work station, even for a short period of time, and access to work stations must be password protected. Passwords must not be stated on sticky notes at the work station. Employees must be instructed to lock the windows and doors when leaving the work station room.

b) Electronic Devices and Storage Media

Employees should use company devices instead of personal devices for home office requiring a strong password and having storage encryption. Personal flash drives or external hard drives should not be connected to the company device to prevent malware attacks and loss of data. To the extent possible, personal data processed by the employee for work-related purposes should not be stored on any personal
devices, and sensitive data must not be stored on any such personal devices. Processing of personal data should be carried out exclusively via secure VPN on the company’s servers.

In case the usage of personal devices is necessary, private data and work-related data must be separated through dedicated accounts (typically available for smartphones and tablets). Usage of personal devices for work-related activities may trigger the application of the telecommunication secrecy and similar protection for the employees against access by the employer that should be addressed in advance in a policy or agreement.

c) Secure VPN and other security aspects

The private WiFi / Internet access used to access the company’s IT systems must be password protected (ideally with WPA3). The company’s router must support access to the company’s IT system via secure VPN (Virtual Private Network). Ideally, a 2-factor authorization is required to access the company’s IT systems. The private router of the employee should have appropriate firewalls in place to prevent unauthorized access via the employee's router to the company's IT systems. Security measures, such as fully updated anti-virus protection and firewalls, must also apply for remote access. Employees must be made aware of the risks associated with phishing and other malware emails. Regular security updates must be made available to employees working from home and any remote access to the company's IT systems must be logged.

d) Communication Technology

If employees are required to use private phones, the call history must be deleted regularly. Business contact details should not be stored in private phones, unless a separate account for business use is set up. Messenger services providing end-to-end encryption can be used provided the messenger operator does not analyze the usage of the services (including content of the communication) for own purposes. The guidelines further state that messenger services shall not be used to share sensitive data.

End-to-end encryption may not always be available for multi-party video calls. In order to reduce the risks, video call providers that are located in the EU/EEA and that store the data in the EU/EEA should be preferred. The video call provider must be required not to analyze the usage of the video call system (in particular communication content and users of the system) for its own purposes. Audio and video calls must not be recorded unless all participants explicitly consent to the recording after having received a detailed notice about the purposes and further processing of the recording. Calls must be done in a private environment preventing other household members from listening to the conversation.

Employees must only use the corporate email account. Use of any private email accounts via commercial email providers must be prohibited, including forwarding of business emails to private email accounts.
6. Conclusion

Even in these unprecedented times, working from home should be governed in individual agreements with each affected employee which should address not only labor law requirements, but also data protection and cyber security aspects.

Further resources:

Below please find links to various statements and guidance issued by German data protection authorities relating to home office:

https://www.lda.bayern.de/de/corona_datenschutz.html
https://www.lda.brandenburg.de/media_fast/4055/Heimarbeit_200323.pdf
https://www.bfdi.bund.de/SharedDocs/Publikationen/Faltblaetter/Telearbeit.html

For further information, please contact:

Julia Kaufmann LL.M.
julia.kaufmann@bakermckenzie.com
Prof. Dr. Michael Schmidl LL.M
michael.schmidl@bakermckenzie.com
Dr. Bernhard Tannehl
bernhard.trappehl@bakermckenzie.com
Dr. Holger Lutz, LL.M.
holger.lutz@bakermckenzie.com
Dr. Michaela Nebel
michaela.nebel@bakermckenzie.com
Florian Tannen
florian.tannen@bakermckenzie.com
This client newsletter is prepared for information purposes only. The information contained therein should not be relied on as legal advice and should, therefore, not be regarded as a substitute for detailed legal advice in the individual case. The advice of a qualified lawyer should always be sought in such cases. In the publishing of this Newsletter, we do not accept any liability in individual cases.

Baker & McKenzie - Partnerschaft von Rechtsanwälten und Steuerberatern mbB is a professional partnership under German law with its registered office in Frankfurt/Main, registered with the Local Court of Frankfurt/Main at PR No. 1602. It is associated with Baker & McKenzie International, a Verein organized under the laws of Switzerland. Members of Baker & McKenzie International are Baker McKenzie law firms around the world. In common with terminology used in professional service organizations, reference to a “partner” means a professional who is a partner, or equivalent, in such a law firm. Similarly, reference to an “office” means an office of any such law firm.

© Baker McKenzie