TaylorWessing

Home Office – FAQ

IT and data protection regulations

In order to contain the spread of the COVID-19 virus (coronavirus), it is recommended to avoid social contacts. Where possible, work should be done from home. In the following you will find answers to the most frequently asked questions, especially with regard to European IT and data protection regulations that must be adhered to when employees do home office.

Q: How can the employer protect confidential data from third party access if it allows its employees to work from home?

A: Employee access to the employer's systems should be provided via a secure access point (e.g. VPN access) with robust access verification. In addition to encryption 'in transit' of communication with the company network, the operational end devices should have reasonable protection mechanisms (password protection, encryption etc.). Further, the employer should consider restricting access to systems and data on a need-to-know-basis. This particularly applies to sensitive data (e.g. HR data).

Q: What can the employee do to protect confidential data from access by third parties?

A: If third parties (e.g. family members, flatmates) have access to the employee's home work station, the employee should ensure that the risks of unauthorized access to data by third parties are minimized (e.g. locking the computer when leaving the workplace, locking the workroom when absent, making confidential telephone calls only when listening in is impossible). Physical personal and confidential data should be protected and be stored in a lockable cabinet. Finally, the employee should ensure that he/she destroys documents that are no longer required in a manner that complies with data protection regulations (for example, by shredding the document into small pieces).

Q: Do I need a home office policy?

A: There is no legal obligation to create a home office policy. However, it is very useful and advisable to define the general conditions and obligations when working from home in a uniform guideline. A respective guideline could also provide information on how to obtain IT support when working remotely (e.g. respective contact details, access to virtual solutions etc.).

Q: Are employees allowed to use their private Wi-Fi connection when working from home?

A: Generally yes. However, the employer should inform its employees to ensure that the Wi-Fi connection is adequately secured.

Q: Are employees allowed to take physical data (files, printouts, etc.) to their home office or to print out data from home?

A: When working from home, they should preferably not rely on physical documents since, in the absence of appropriate technical measures, there is only a limited possibility of minimising the risk of loss or damage. Extensive use should therefore be made of scans, electronic files etc. If the employee is nevertheless dependent on physical documents, these should only be transported in sealed containers. Furthermore, the documents must not be left unattended.

Q: Who is responsible within for ensuring appropriate technical and organisational measures (Art. 32 GDPR) when employees work from home?

A: The employer remains responsible for compliance with the provisions of the GDPR.

Q: Are employees allowed to connect their own devices (e.g. printers, monitors etc.) to the company devices at home?

A: In principle, the use of equipment that is not provided by the employer should be prohibited. This is the only way to avoid safety impairments for the company's hardware and software. In individual cases, however, pragmatic solutions can certainly be found together with the employer.

Q: Is the employee allowed to use the company hardware also for private purposes when working from home?

A: The private use of the employer's hardware will be prohibited in many cases, which often makes sense from a legal perspective. If private use is permitted, the employee must be specifically informed of his or her obligations and the restrictions on private use. Furthermore, it must be ensured that data for private and business use are separated in the best possible way.

Q: Can the employee use his own computer for home office work?

A: If possible, the use of private hardware for home office work should be avoided. If the use of private devices is unavoidable, the employer should ensure the technical requirements for the use of private devices (installation and implementation of appropriate IT security systems, separation of private and business data (e.g. within a container solution), mobile device management). Ideally, activities from private devices should only take place in the "cloud", i.e. the company network of the employer, so that a data separation takes place. The employer should set out the framework conditions for the use of private devices in a directive, which the employee must adhere to.

Q: Can employees use software/applications that are installed on their private device (e.g. MS Office)?

A: Generally not, as there may be problems regarding the necessary licenses. The employee has often concluded a license agreement, according to which the business use is expressly prohibited.

Q: Can the employer or the employee forward company e-mails to the private e-mail account of the employee?

A: As a general rule, this should be avoided. In case of such forwarding, the employer can no longer adequately fulfil its obligations under data protection law (e.g. ensuring proper storage and compliance with appropriate technical and organisational measures).

Q: What does the employer have to do to handle cybersecurity incidents when employees work remotely?

A: Cybersecurity is of upmost importance, particularly with regard to home office. Therefore. the employer should have in place (or develop at short notice) standard procedures employees have to follow in case of a cybersecurity incident. The procedure should particularly outline the communication chain and the relevant contact details.

Q: Does the employer have to inform the employee separately about the data processing in connection with home office work?

A: The duty to inform under data protection law is comprehensive. If the existing data protection notices for employees do not contain information on data processing regarding home office, separate information is required.

Q: What does the employer have to observe from an employment law perspective?

A: We have prepared an employment law FAQ (German law) on the employment law implications of the Corona pandemic in general as well as home office options.

Authors

Paul Voigt, Lic. en Derecho, CIPP/E
Partner
p.voigt@taylorwessing.com

Wiebke Reuter, LL.M. (London)
Associate
w.reuter@taylorwessing.com

Rita Danz
Associate
r.danz@taylorwessing.com