Data protection and home office in times of the coronavirus

LEGAL AND PRACTICAL REQUIREMENTS AND PROPER IMPLEMENTATION

Overview of topics

- Protection of personal data in the home office
- Basic rules for home office set ups
- Requirements for the physical and digital workplace at home

Working in the home office is accompanied by great challenges. Quickly feasible solutions must be found and implemented for the company and IT to maintain stable and efficient business operations. At the same time, the additional costs for alternative solutions, especially in the IT department, should be kept as low as possible. Employers must now ensure to avoid "emergency solutions" which could have negative consequences in terms of data protection law.

Who is responsible for data protection in the home office?

The employer is responsible for ensuring that legal regulations are paid in (Art. 24 DSGVO) whether in the regular office or in the home office. Art. 4 No. 7 DSGVO designates the employer as the responsible controller. For data protection violations in the home office, the employer is therefore liable in the same way as if the violation happened in the company's own premises, even if members of the employee's household and thus persons from outside the company are often in the immediate vicinity. The employee himself often does not regard these as third parties, even if the legal assessment is very clear. Within the circle of employees, awareness of the higher demands for data protection in the home office must be raised. If non-authorized third parties in the home office become aware of protected personal data, this may entail a data breach. For this reasons, specific safeguarding measures to protect personally identifiable data need to be put in place. The employer must therefore also guarantee and monitor data protection in the home office.

Avoiding problems with labor law: Home office can only be agreed upon by mutual consent between employer and employee. Employers must, therefore, make sure that the agreements that are now being made with employees regarding the home office are explicitly limited to the current exceptional situation of the Corona pandemic. Otherwise, there is a risk that employees can successfully claim for home office even after the pandemic ended. The GSK update on the latest labor law issues can be downloaded here.

For which data do special requirements apply in the home office?

Personal data is processed in the home office on a regular basis as well. However, there is a higher risk that unauthorized third parties may gain knowledge of this data. Employees must, therefore, pay attention to how they behave responsibly when working in the home office. Although internal company information without personal reference is not subject to the statutory data protection regulations, it is nevertheless worthy of protection from the company's perspective. It is advisable for employers to draw up a special home office policy for all employees in which data protection and confidentiality are equally addressed and regulated. If such a home

office guideline does not yet exist in the company, the current situation may be an opportunity to make up for this with the involvement of the data protection officer and works council, where applicable.

Which basic rules are to be observed?

In particular, the basic rules for operational data and communication must be observed even in an exceptional situation such as the current pandemic. Personal data should never be stored in or processed with private e-mail accounts, apps of private messenger services or on private notebooks or PCs of employees. In addition to the general security concerns with these devices and applications, the employer has no way of verifying for what purpose the employees have granted further access rights to personal data to such applications. Many people use free e-mail providers or messengers that process data for advertising and other purposes to a considerable extent. These services often automatically transfer the e-mail addresses and telephone numbers of contact persons to the address book of the account. In the case the address book is linked to other services as well, the data is distributed widely. Often employees do not even know that they have shared their private communication in such a wide range. Employers must prevent such uncontrolled spread by prohibiting the use of private accounts for company-related work. This is also advisable because of the period following the current pandemic, as all data processed in violation of data protection regulations must be securely deleted. Monitoring this deletion is unlikely to succeed outside the company's systems. In the end, in addition to data protection concerns, there is always the risk that employees leaving a company will take sensitive company data such as customer contacts with them because such data has not been deleted before.

What applies to the physical workplace?

The greatest challenge in the home office is posed by the family and household members of the employees. Employees should be instructed to keep confidential matters confidential in the home office as well. At best, paper documents should not be taken from the regular workplace to the home office. Employees should also not print out documents containing personal data in the home office. Sometimes it is not possible to do without print outs at all. In this case, documents containing personal data should not be openly accessible to others within the household and should be stored securely and locked away at the end of the working day. Leaving the documents and information exposed at the kitchen table should not be an option. The computer screen should also be shielded from the view of third parties. Telephone calls should not be made in the presence of third parties within the same room. If an employee can't make phonecalls containing sensitive personal data in the absence of others, other employees with a suitable living situation should be identified that can take over the respective tasks in the meantime. Just as in the regular workplace, paper waste containing personal data may also be generated in the home office. Employees should collect this separately at home, keep it locked up and dispose all of it safely at their regular workplace later on. Simply tearing it into smaller pieces is usually not sufficient enough for safe disposal.

What rules apply to the digital workplace?

For the digital workplace, encryption of data media and password protection is as important in the home as well as at the regular office. All devices with stored data on them, which are moved outside the regular workplace, can get lost and thus possibly become a reportable data breach. If employees also access the companies system from home, this should be done via a secure VPN connection to establish data security and to avoid the creation of data copies on private notebooks. Unauthorized access to data must be prevented in the home office as well. One of the measures to ensure this, is a locking of the the notebook, even if the workplace is only left behind for a short time. Employees should be made aware once again, that even under the current situation, family members must not have access to the company notebook. The company's own IT equipment should be strictly limited to company-related work to minimize risks. For example, if children use a company notebook for homework or games, there is a greater risk that they will unknowingly install malware. Children often lack the

awareness of risks online. It is also to be expected that hackers will abuse the current situation to exploit protection gaps or do phishing.

What should be considered when using private devices?

In principle, it should be avoided that data is stored on devices that are not owned by the company. Private USB sticks should also not be used. They are often used unencrypted and there is a high risk of losing them.
The usage of private USB sticks is often forgotten later on and therefore there is a high-risk data is not deleted or deleted in a restorable manner that can be recovered by third parties later on. If employees use private smartphones to make phone calls, personal data such as contacts should not be stored in the address book of the phone, as these are often linked to other applications such as messaging apps, which read and transfer the address book to the servers of their respective providers. On private printers, the internal memory should be regularly deleted. In the case employees still use a private PC to access applications via WebAccess, which should be avoided, it should be ensured that there are no plug-ins installed in browsers of the private PC since these often read the entire input and process the data on external servers.

How can additional software be used to facilitate the work?

With all software solutions that are introduced in the context of the current situation, such as online meeting and messenger applications, care must be taken.
It must be ensured that even under time pressure the verification and documentation process required by the General Data Protection Regulation ("GDPR") is adhered to. In particular, questions regarding ordered data processing acc. to Art. 28 GDPR and data transfers in the case of applications offered by providers from countries that do not belong to the European Economic Area must be clarified and the necessary measures to safeguard the level of data protection required inside the European Union taken in this respect. The special features to be observed when using external software will be examined in more detail in one of our next GSK updates.

Dr. Katy Ritzmann
Lawyer, Partner
Berlin site
katy.ritzmann@gsk.de

Dr Jörg Kahler
Lawyer, Partner
Berlin site
joerg.kahler@gsk.de

Ira Mießler, LL.M.
Lawyer, Associate
Berlin site
ira.miessler@gsk.de

Anne Bettina Nonnaß
Lawyer, Associate
Berlin site
anne. nonnass@gsk.de

Jörg Wünschel
Lawyer, Associate
Berlin site
joerg.wuenschel@gsk.de

GSK
STOCKMANN

Disclaimer
This client briefing exclusively contains general information which is not suitable to be used in the specific circumstances of a certain situation. It is not the purpose of the client briefing to serve as the basis of a commercial or other decision of whatever nature. The client briefing does not qualify as advice or a binding offer to provide advice or information and it is not suitable as a substitute for personal advice. Any decision taken on the basis of the content of this client briefing or of parts thereof is at the exclusive risk of the user.

GSK Stockmann as well as the partners and employees mentioned in this client briefing do not give any guarantee nor do GSK Stockmann or any of its partners or employees assume any liability for whatever reason regarding the content of this client briefing. For that reason we recommend you to request personal advice.

www.gsk.de

GSK Stockmann

BERLIN
Mohrenstrasse 42
10117 Berlin
T +49 30 203907-0
F +49 30 203907-44
berlin@gsk.de

HEIDELBERG
Mittermaierstrasse 31
69115 Heidelberg
T +49 6221 4566-0
F +49 6221 4566-44
heidelberg@gsk.de

FRANKFURT / M.
Taunusanlage 21
60325 Frankfurt am Main
T +49 69 710003-0
F +49 69 710003-144
frankfurt@gsk.de

MUNICH
Karl-Scharnagl-Ring 8
80539 Munich
T +49 89 288174-0
F +49 89 288174-44
muenchen@gsk.de

HAMBURG
Neuer Wall 69
20354 Hamburg
T +49 40 369703-0
F +49 40 369703-44
hamburg@gsk.de

LUXEMBOURG
GSK Stockmann SA
44, Avenue John F. Kennedy
L-1855 Luxembourg
T +352 271802-00
F +352 271802-11
luxembourg@gsk-lux.com