PERSONAL DATA PROTECTION DURING REMOTE WORKING - GUIDEBOOK

In the view of the threat of COVID-19, one of the measures to control and prevent its spread is to limit contact with other people, including co-workers, as much as possible. Therefore, if the nature of the work permits, remote working is acceptable and advisable. When working remotely, however, we must remember to protect personal data. Below you will find some guidelines for how to ensure this is done.

Is it allowed to work on private devices?

Remote working should be carried out in accordance with the organisation's rules. However, it is recommended that you work on company equipment, if possible. If, according to the organisation's rules, an employee may use their private equipment or the employer has given permission to do so due to exceptional circumstances, the following rules should be followed.

1. If possible, contact the employer's IT specialists to determine how to appropriately prepare this equipment.
2. Computers should be scanned by an anti-virus program.
3. Computers should have software installed allowing them to connect to a virtual private network (VPN) and - if the nature of the work requires it - software allowing secure teleconferencing.
4. If a private computer is also used by other members of the household, a separate password – protected account must be set up for work purposes. When working remotely, members of the household are treated as outsiders, so they should not have access to work material.

Regardless of whether you use private or company equipment, remember these rules!

DEVICES

Follow the procedures adopted by your employer.

Do not install applications and software without express instructions from your employer or if not permitted by their proceudres.

Make sure that all system updates are done.

Remember the appropriate passwords protecting your devices. Change them frequently.

PERSONAL DATA PROTECTION DURING REMOTE WORKING - GUIDEBOOK

E-MAIL AND SOCIAL NETWORKING SITES

Use company email accounts and company communications systems. Don't communicate with business associates through private social media accounts.

Always check the recipements of outgoing e-mails.

Always check the senders of e-mails you receive. If you have any doubts about the sender or an attachement, immediately contact your company's IT specialists.

Do not e-mail encrypted information together with the password to it. The password should be sent separately. If the password is also sent by e-mail, persons with access to the e-mail will easily read the encrypted messages.

NETWORK ACCESS

Use only trusted networks and cloud access.

If you do not have access to the network and the cloud, remember to archive your data accordingly.

PROTECT CONFIDENTIAL INFORMATION

Even if you work from home, don't leave business information in sight of others.

When conducting business calls, limit the possibility of other people hearing them. Use headphones, and if possible go to a room where others are not present.

REMEMBER!

EVEN DURING AN EPIDEMIC, THE RULES ON THE PROTECTION OF PERSONAL DATA CONTINUE TO APPLY.

IF YOU FAIL TO COMPLY WITH THEM, YOU RISK FACING HEAVY PENALTIES. REMEMBER THE RULES ON INFORMATION SECURITY AND, IF IN DOUBT, CONTACT THE PERSON RESPONSIBLE FOR PERSONAL DATA PROTECTION IN YOUR COMPANY.