

Policy on data protection and confidentiality for "Mobile Working"

Working environment

For "Working Mobile", the working environment must be designed in such a way that operational data and information are adequately protected. This includes at least the following measures:

- The workplace is organized in a way that any visitors cannot look at the notebook or paper documents. If possible, this also applies to family members and roommates.
- As in the office, a clean-desk policy applies at the end of the working day so that nothing is left open.
- Confidential paper documents should be locked up in cupboards if possible or at least kept in document folders and thus withdrawn from the access of third parties.
- Windows in ground floor apartments are always closed when leaving the workplace.
- The notebook is always locked when leaving the workplace if other access (e.g. visitors, children, cat) cannot be excluded.
- Care is taken to ensure that telephone conversations are not heard by unauthorized persons (e. g. open window, other video conference in progress, Smart Home devices, etc.).

Handling paper documents

Even with us, not all work processes can yet be used completely digitally. When dealing with paper documents, risks arise that do not occur in the office environment. Therefore, the following measures must be observed:

- Paper documents are taken home in suitable folders (with the name of the company in case of loss) and should not be exposed to increased risk situations on the way (e. g. back seat while shopping, backpack in the restaurant, ...).
- Paper documents are not disposed of with household waste, but in the office (or - if available - at home by a shredder, if this corresponds to level 5 DIN 66399 recommended by the data protection authorities).
- Special care should be taken with important original documents so that they are not exposed to any risk of damage (e. g. children painting an original document).

Data protection

Mobile Working is like a virtual office - the security risks increase with the connection to the internet. Please implement the following with you:

- Use home Wi-Fi only with strong passwords.
- Access only to servers, file stores and applications required for Mobile Working through the VPN connection.
- Storage of data on network drives in the company accessible via the VPN connection.
- Use of Wi-Fi hotspots only if all communication is secured by VPN connection.

Validity of existing guidelines

All existing policies and guidelines for data protection and confidentiality continue to apply for Mobile Working. Please pay particular attention to the regulations for private use of business equipment, which are part of the IT Terms of Use.