Supplementary Data Protection Notices and Security Rules for Working from Home

The employee commits to adhering to the relevant data protection and information security regulations, including the related company agreements, guidelines, and instructions of the COMPANY. Specifically, the employee commits to complying with the COMPANY's data protection policy. The confidentiality and data protection obligation signed upon employment commencement is expressly highlighted.

Additionally, the employee has special obligations for working from home, particularly regarding the handling of personal data. The principle applies: The more sensitive and therefore more deserving of protection personal data is, the more it must be protected, even in the home office. Especially sensitive data includes, for example, health data, personnel records, and social data.

The employee must always ensure in the home office that:

- The confidentiality of official information and personal data is guaranteed.
- Official devices and documents are protected from misuse.
- Private and official data are kept separate.

The following additional measures and procedures must be constantly applied in the home office:

- Both fixed devices (PC, thin client) and mobile devices such as laptops, official documents, and the smart card or the official data and information contained therein (e.g., paper documents with personal data) must be protected during transport and in the private premises of the employee so that they cannot be viewed, used, or stolen by unauthorized third parties (including household members).
- The employee may only take work documents necessary for work to the home office. Paper documents must not be exposed to increased risk situations during transport to/from home (e.g., back seat while shopping, backpack in a restaurant, etc.). If these documents are no longer needed in the home office and can be destroyed, they must either be disposed of within the COMPANY or destroyed in such a way that third parties cannot gain any content-related knowledge.
- The workplace must generally be in a lockable/separate room or a separated area not used by other household members during working hours. It must always be ensured that no unauthorized third parties (e.g., household members, neighbors, visitors) can gain insight into personal data during work.
- The workplace must be organized so that private and official data do not mix.

When leaving the workplace (regardless of the planned duration) and at the end of the workday, the employee must prevent access to all official stationary and mobile devices (e.g., laptop, phone). For short-term absences, the screen lock must be activated if access by third parties cannot be excluded. All official

documents must also be kept under lock and key (e.g., in a lockable cabinet or roll container).

- Fixed and mobile devices and official documents must not be left unattended unless they are appropriately secured or locked away.
- For official phone calls, care must be taken to ensure that neither third parties (e.g., household or family members) nor technical voice recording systems (e.g., digital voice assistants like Alexa or Cortana) can listen.
- If it is necessary to use private telephones (e.g., due to the failure of official devices), it must be ensured that official contact data is not permanently stored on the private phone. Since it is usually not necessary for private numbers to appear in calls, number suppression should be activated when using private phones.
- Access to electronic documents and data is exclusively via secure communication means provided by the COMPANY.
- Electronic documents and data must only be stored in the COMPANY's network or on the network drives (e.g., M:) and not locally on the mobile device.
- The employee commits to immediately reporting data protection and information security incidents, even in the home office, via the known channels.

Acknowledged and agreed:

(Name in block letters)

(Location, Date) (Signature of the employee)