Best Practice im Homeoffice

Diese Checkliste soll einen Überblick über die wichtigsten Praxismaßnahmen im Homeoffice entsprechend den geltenden gesetzlichen Datenschutzvorgaben geben. Datenschutzverstöße im neuen Alltag können gezielt vermieden werden. Die vorgeschlagenen Best-Practices sensibilisieren das Thema und helfen bei der Umsetzung.

Die aufgeführten Best-Practices geben einen Überblick und sind nicht abschließend.

Selbst-Check: Datenschutzrechtliche Regelungen bei Homeoffice

Arbeitsumgebung

Bei der Arbeit zu Hause soll die Umgebung so ausgestaltet sein, dass die Vertraulichkeit und Verfügbarkeit der Daten wie im Büro sichergestellt ist.

- ☐ Der Arbeitsplatz ist so gewählt, dass Familienmitglieder oder Besucher keinen Blick auf das Notebook oder in die Papier-unterlagen werfen können.
- ☐ Es gilt eine Clean-Desk-Policy am Ende des Arbeitstages
- ☐ Es werden Sichtschutzfolien verwendet, wenn dies erforderlich ist (bspw. Schreibtisch am Fenster in Parterrewohnung)
- ☐ Fenster werden in Erdgeschosswohnungen bei Verlassen des Arbeitsplatzes immer geschlossen.
- ☐ Sperrung des Notebooks bei Verlassen des Arbeitsplatzes falls ein anderer Zugriff (z. B. Kinder, Katze) nicht ausgeschlossen ist

Umgang mit Papierdokumenten

Noch nicht alle Arbeitsabläufe sind komplett digital nutzbar. Beim Umgang mit Papierdokumenten ist daher auf besondere Gegebenheiten zu achten.

- ☐ Papierunterlagen werden in geeigneten Mappen (mit Namen des Unternehmens im Falle eines Verlusts) mit nach Hause genommen
- ☐ Papierunterlagen sollen beim Transport nach/von zu Hause nicht erhöhten Risikosituationen (z. B. Rücksitz beim Einkaufen, Rucksack im Restaurant, …) ausgesetzt werden
- ☐ Papierunterlagen sollen in Dokumentenmappen oder Schränken verschlossen werden
- ☐ Entsorgung von Papierunterlagen erfolgt nicht über den Hausmüll, sondern entweder im Büro oder zu Hause durch einen Aktenvernichter mit mind. Sicherheitsstufe 5 (nach DIN 66399)
- ☐ wichtigen Papierdokumenten sollten zum Schutz (z. B. Kinder bemalen ein Originaldokument) kopiert werden

☐ Es wird darauf geachtet, dass Telefongespräche nicht von unbefugten Personen mitgehört werden (z. B. offenes Fenster, laufende andere Videokonferenz, …)

Genutzte Hardware

Die Bereitstellung von dienstlichen Geräten sollte im Fokus stehen. Privatgeräte sollten nur in Ausnahmefällen eingesetzt werden.

☐ Dienstliche Notebooks werden gestellt

☐ Dienstliche Smartphones oder Softphones werden gestellt

☐ Bei Verwendung von Privatgeräten werden Remoteverbindungen auf Terminalserver verwendet

☐ Dienstlich zur Verfügung gestellte Geräte werden auch zu Hause nicht für private Zwecke genutzt

☐ Vollverschlüsselung bei dienstlichen Smartphones

☐ Pin-Sperre bei dienstlichen Smartphones

Sicherheit

Das Homeoffice ist das virtuelle Büro – die Sicherheitsrisiken erhöhen sich durch die Anbindung an das Internet.

☐ Anbindung an das Firmennetz mit verschlüsselten VPN-Verbindungen nach Stand der Technik

☐ Nutzung vom heimischen Wi-Fi mit starken Passwörtern

☐ Nutzung öffentlicher Wi-Fi-Hotspots nur bei durchgängiger Absicherung sämtlicher Kommunikation durch VPN-Anbindung

☐ Zugriff nur auf für das Homeoffice erforderliche Server, Dateiablagen und Anwendungen durch die VPN-Verbindung

☐ Speicherung von Daten möglichst nur auf über die VPN-Verbindung erreichbare Netzlaufwerke im Unternehmen

Allgemeine organisatorische Regelungen

Durch die Arbeit im eigenen Zuhause, entstehen völlig neue Sicherheitsprobleme, die als Tor für Cyberangriffe genutzt werden könnten.

☐ Keine Weiterleitung von dienstlichen E-Mails an private E-Mail-Konten