CHECKLISTE: DATENSCHUTZ UND DATENSICHERHEIT BEI MOBILEM ARBEITEN

Verwenden Sie diese Checkliste, um mobiles Arbeiten in Ihrem Unternehmen sicher zu gestalten und Datenschutzrisiken zuminimieren.

Organisatorisches

- Beziehen Sie Ihre Datenschutzbeauftragten ein, beispielsweise bei der Risikobewertung mobilen Arbeitens oder der Datenschutz-Folgenabschätzung nach Art. 35 der Datenschutzgrundverordnung.
- Erstellen Sie klare und schriftliche Regelungen zur mobilen Arbeit, die Rechte und Pflichten der mobil Arbeitenden sowie die Datenschutzanforderungen definieren.
- Sensibilisieren Sie die Beschäftigten regelmäßig zu Datenschutz und IT-Sicherheitsstandards. Dazu zählen zum Beispiel der Umgang mit vertraulichen Daten, Passwortschutz und Phishing-Prävention.
- Schließen Sie Vereinbarungen zur mobilen Arbeit ab, die beispielsweise bestimmte Arbeitssituationen (im Café, im Zug) ausschließen bzw. regeln (Hotel, Tagungseinrichtungen).

Technische Maßnahmen

- Stellen Sie Ihren Beschäftigten dienstliche Geräte zur Verfügung. Sind private Endgeräte zugelassen, zum Beispiel Smartphones, sorgen Sie für die Trennung von beruflichen und privaten Daten und Anwendungen.
- Verschlüsseln Sie alle mobilen Endgeräte wie Laptops und Smartphones sowie gespeicherte Daten, etwa durch Festplattenverschlüsselung.
- Ermöglichen Sie den Zugriff auf das Firmennetzwerk nur über ein Virtual Private Network (VPN) mit starker Verschlüsselung.
- Sorgen Sie für regelmäßige Software-Updates, Virenschutzprogramme und Firewalls auf allen Geräten.

Arbeitsplatzgestaltung

- Sicherer Arbeitsplatz: Stellen Sie sicher, dass der Arbeitsplatz zu Hause oder unterwegs datenschutzkonform gestaltet ist, etwa durch Blickschutzfilter und passwortgeschützte Bildschirmsperren.
- Umgang mit Papierdokumenten: Vermeiden Sie die Nutzung von Papierdokumenten oder sorgen Sie für sichere Entsorgung, zum Beispiel durch Schreddern.
- Lassen Sie unbenötigte oder defekte Geräte und Datenträger zurückbringen und durch das Unternehmen entsorgen.

Zugriffskontrolle

- Zwei-Faktor-Authentifizierung: Implementieren Sie hardwarebasierte Sicherheitslösungen wie Sicherheitskarten oder Token für den Zugriff auf sensible Daten.
- Einschränkung von Schnittstellen: Deaktivieren Sie USB-Anschlüsse und andere externe Schnittstellen auf mobilen Geräten, um unbefugten Zugriff zu verhindern.

Datensicherung

- Machen Sie klar, wo Daten gespeichert werden sollen und wo nicht (auf der lokalen Festplatte).
- Erstellen Sie eine Back-up-Strategie.
- Führen Sie regelmäßige Back-ups wichtiger Daten durch und speichern Sie diese sicher.

Kommunikation

- Nutzen Sie sichere Kommunikationskanäle wie verschlüsselte E-Mails oder Messenger-Dienste.
- Regeln Sie, mit welchen Anwendungen Videokonferenzen und Calls stattfinden sollen und mit welchen nicht.
- Versehen Sie entsprechende Anwendungen mit datenschutzkonformen Funktionen, wenn möglich, oder weichen Sie auf bessere Lösungen aus.