Infoblatt – Homeoffice ***zu beachtende Datenschutzregelungen (Überblick)***

Zusammenstellung der wichtigsten Punkte /Quelle - Datenschutzaufsichtsbehörden

1. Arbeitsumgebung

Die Arbeitsplatzumgebung zu Hause soll so ausgestalten sein, dass vom Grundsatz her 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/Papierunterlagen werfen können
- ✓ Es gilt eine Clean-Desk-Policy am Ende des Arbeitstages
- ✓ Papierunterlagen können in Dokumentenmappen oder Schränken verschlossen werden
- ✓ Sperrung des Notebooks bei Verlassen des Arbeitsplatzes, falls ein anderer Zugriff hat – egal ob gewollt oder ungewollt
- ✓ Es ist darauf zu achten, dass Telefongespräche nicht von unbefugten Personen mitgehört werden

2. Nutzung von Messenger-Diensten

Neben E-Mails werden zunehmend auch Messenger-Systeme für die Unternehmenskommunikation eingesetzt. Die verwendeten Dienste müssen für einen aus Datenschutzsicht beanstandungsfreien Einsatz bestimmte Anforderungen erfüllen.

- ✓ Kommunikation der Inhalte erfolgt Transport- und Ende-zu Ende verschlüsselt
- ✓ Keine Verwendung oder Weitergabe der Verkehrsdaten (wer wann mit wem kommuniziert) an den Anbieter für Zwecke wie Werbung oder Profiling
- ✓ Ende-zu-Ende-Verschlüsselung auch von Anhängen wie Bildern oder Textnachrichten
- ✓ Einsatz einer Mobile-Device-Management Lösung zur Steuerung von Kontakt-Uploads an Messenger-Anbieter

3. Genutzte Hardware

Es wird die Bereitstellung von dienstlichen Geräten empfohlen. Privatgeräte sollten nur in Ausnahmefällen eingesetzt werden.

- ✓ Dienstliche Notebooks werden gestellt
- ✓ Dienstliche Smartphones werden gestellt
- ✓ Bei Verwendung von Privatgeräten werden Remoteverbindungen auf Terminalserver verwendet
- ✓ Dienstlich gestellte Geräte werden auch zu Hause nicht für private Zwecke genutzt

4. Nutzung von Videokonferenzen

Bei der Auswahl von Videokonferenzlösungen, mit denen Präsenzbesprechungen teilweise oder vollständig ersetzt werden, müssen bestimmte Anforderungen beachtet werden.

- ✓ Vertrag zur Auftragsverarbeitung nach Art. 28 DS-GVO ist abgeschlossen
- ✓ Bei Anbietern in unsicheren Drittstaaten sind geeignete Garantien vorhanden; es werden hierbei insbesondere die aktuellen Entwicklungen und Veröffentlichungen zur PrivacyShield-Zertifizierung bei US-Anbietern verfolgt
- ✓ Verwendung einer Transportverschlüsselung (z. B. TLS) nach Stand der Technik
- ✓ Verwendung einer Ende-zu-Ende-Verschlüsselung, sofern Daten mit hohem Risiko besprochen bzw. übertragen werden
- ✓ Zugangsschutz zu Konferenzräumen über Passwörter oder individuelle Einladungslinks
- ✓ Keine Aufzeichnung der Inhalte durch den Anbieter zum Zweck der Qualitätsverbesserung oder sonstiger Auswertung
- ✓ Konfigurationsmöglichkeiten bei Erhebung von Telemetriedaten durch den Anbieter (Empfehlung: Deaktivierung)
- ✓ Keine Aufzeichnung der Videokonferenzen durch das Unternehmen
- ✓ Regelungen, wann und durch wen Screen Sharing verwendet wird, sind vorhanden
- ✓ Regelungen zum Zweck und der Speicherdauer (z. B. Löschung bei Beendigung der Konferenz) von ChatFunktionen sind vorhanden
- ✓ Verwendete Apps leiten keine unzulässigen Tracking-Informationen an die App-Anbieter

5. *Sicherheit*

Das eigene Homeoffice gilt als virtuelles Büro. Durch die Anbindung an das Internet erhöhen sich dabei die Sicherheitsrisiken enorm. Technische Lösungen helfen, diese Risiken zu minimieren

- ✓ Anbindung an das Firmennetz mit verschlüsselten VPN-Verbindungen nach Stand der Technik
- ✓ Einsatz von Verfahren zur Zwei-Faktor-Authentifizierung nebst PIN/Passwort (z. B. Hardwaretoken oder Software-Zertifikate) bei VPN-Verbindungen
- ✓ Nutzung vom heimischen WLAN mit starken Passwörtern
- ✓ Zugriff nur auf für das Homeoffice erforderliche Server, Dateiablagen und Anwendungen durch die VPN-Verbindung
- ✓ Speicherung von Daten auf über die VPN-Verbindung erreichbare Netzlaufwerke im Unternehmen
- ✓ Festplattenvollverschlüsselung bei Notebooks
- ✓ Vollverschlüsselung bei dienstlichen Smartphones - PIN-Sperre bei dienstlichen Smartphones
- ✓ Regelungen im Verlustfall bei mobilen Endgeräten (z. B.Remote Wipe bei Smartphones, Sperrung von Hardware-Token) wurden getroffen
- ✓ Täglich Updates der Virensignaturen auf den Homeoffice-Notebooks

6. *Allgemeine organisatorische Regelungen*

Die Anbindung von Mitarbeitern im Zu-Hause-Modus muss durchdacht und sicher ausgestaltet werden. Neben technischen Lösungen helfen organisatorische Regelungen, um Einfallstore für tiefgreifende Cyberangriffe zu verhindern.

- ✓ Überblick über die Mitarbeiter im Homeoffice
- ✓ Überblick über die Geräte der Mitarbeiter im Homeoffice
- ✓ Schulung/Informationen für Mitarbeiter über die Homeoffice-Regelungen
- ✓ Schriftliche Verpflichtung der Mitarbeiter, dass diese sich an die Regelungen halten – eine Vor-Ort-Kontrolle kann i. d. R. entfallen
- ✓ Keine Weiterleitung von dienstlichen E-Mails an private E-Mail-Konten