TOSEC Datenschutz / Consulting

Checkliste für die Wahrung des Datenschutzes im Home-Office

Bereich	Maßnahme	Inhalt
1. Organisation der Informationssicherheit	Erstellung einer Sicherheitsrichtlinie bzw. Regelungen für die mobile IT-Nutzung und Telearbeit	• Kommunikationsarten (E-Mail, Internet, Fax, Mobiltelefon) • Datenklassifizierung: Welche Daten dürfen wie das Unternehmen verlassen? • Sicherheitsanforderungen festlegen (z. B. Regelungen zu Datensicherung, Virenschutz, Firewall, Verschlüsselungsoption (in jedem Fall bei sensiblen Daten) • Wege der Datenübermittlung oder des Zugriffs: VPN, E-Mail, mobile Datenträger (USB), Ausdrucke • Vernichtung Papier und elektronische Datenträger • ggf. Regelungen zu Fernwartung • Aushändigung der Richtlinie an betroffene Mitarbeiter
	Erstellung eines Sicherheitskonzepts für Tele- bzw. Heimarbeit	• Benennung von Sicherheitszielen • Schutzbedarf der bearbeiteten Informationen und diesbezüglichen Risiken
2. Personalsicherheit	Einweisung der Tele- / Heimarbeiter	• Einweisung der Telearbeiter • Mitarbeiterschulungen, Sensibilisierungen z. B. zum Umgang mit ausgedruckten Dokumenten
3. Asset Management	Dokumentation der Ausgabe und Rücknahme von unternehmenseigener IT (z. B. Laptop, Drucker) an und von dem jeweiligen Mitarbeiter	
	Ggf. Vereinbarung eines Zutrittsrechts zum Heimarbeitsplatz zur Durchführung von Kontrollen und Zugriff auf Dokumente	

4. Zugriffskontrolle	Identifizierungs- und Authentisierungsmechanismus	
	Protokollierung	• Authentisierungen • Zugriffe • Veränderungen • Administratortätigkeiten • Fehler
	Administrationsrechte	• Regelungen und Kontrolle • Einschränkung der Benutzerumgebung für den Mitarbeiter
5. Kryptogramme	Verschlüsselung	• Mobile Endgeräte • Mobile Datenträger • E-Mails
6. Physische und Umgebungssicherheit	Arbeitsplatz-Sicherungsmaßnahmen	• Wer ist zutrittsberechtigt? • Welche Sicherungsmaßnahmen gibt es?
	Clean-Desk-Policy	• Gedruckte Dokumente vor Einsicht Unbefugter schützen
	Bildschirm	• Einstellung passwortgeschützter automatischer Bildschirmschoner
7. Betriebssicherheit	Updates	• Installiert und aktuell
	Virenschutz	• Installiert und aktuell
	Firewall	• Aktiviert
	Bootschutz	• Aktivierung empfehlenswert
	Datensicherung	• Regelungen und Kontrolle
8. Kommunikationssicherheit	Trennung von Daten	• Trennung privater Daten von unternehmenseigenen Daten
9. Compliance	Beauftragung von Freien Mitarbeitern	• Ggf. Abschluss eines Auftragsverarbeitungs-Vertrages