

CHECKLISTE · TOMORIS TOOLBOX

Sicher im Homeoffice: Checkliste für Mitarbeitende und Führungskräfte

Regeln für das Unternehmen, Gerät und Zugang, Heimnetz, Arbeitsplatz, Unterlagen und Gespräche, Verlust und Vorfall, nach BSI-Grundschutz und § 2h AVRAG

STAND

25.10.2026

UMFANG

PDF, 6 Seiten

ONLINE

tomoris.com/downloads/homeoffice-sicherheit-checkliste

AUF EINEN BLICK

4

Bereiche zum Abhaken für Mitarbeitende

20

Zeichen Mindestlänge des WLAN-Passworts (BSI)

schriftl.

Telearbeitsvereinbarung samt Orten (§ 2h AVRAG)

1.1.2025

Neufassung des § 2h AVRAG in Kraft

FÜR WEN

- Mitarbeitende, die regelmäßig oder gelegentlich von zu Hause arbeiten
- Führungskräfte und Personalabteilung, die Homeoffice vereinbaren
- IT-Leitung und IT-Dienstleister, die Homeoffice-Arbeitsplätze einrichten und betreuen
- Geschäftsführung kleiner und mittlerer Unternehmen

WORUM ES GEHT

Zu Hause fehlt vieles, was im Büro selbstverständlich ist: verschlossene Räume, ein gepflegtes Netzwerk, ein Aktenvernichter, jemand von der IT am Gang. Gleichzeitig sind Familie und Besuch im Raum. Diese Checkliste fasst zusammen, was das Unternehmen vor dem ersten Homeoffice-Tag regeln sollte, und was Mitarbeitende an Gerät, Heimnetz, Arbeitsplatz, Unterlagen und Gesprächen beachten. Grundlage sind die BSI-Bausteine Telearbeit und Häuslicher Arbeitsplatz, die BSI-Tipps für mobiles Arbeiten und die österreichische Regelung zur Telearbeit in § 2h AVRAG.

Diese Checkliste ist eine Empfehlung von TOMORIS und an Ihr Unternehmen anzupassen. Die Hinweise zum Arbeitsrecht geben einen Überblick und ersetzen keine Rechtsberatung; maßgeblich ist der Gesetzestext in der jeweils geltenden Fassung.

INHALT

01	Was zu Hause anders ist	2
02	Was das Unternehmen vorab regelt	3
03	Gerät und Zugang	4
04	Heimnetz und WLAN	4
05	Arbeitsplatz, Unterlagen und Gespräche	5
06	Verlust, Vorfall und Support	5
07	Quellen	6

01

Was zu Hause anders ist

Warum das Homeoffice eigene Regeln braucht und was das österreichische Arbeitsrecht dazu vorgibt.

Das BSI versteht unter Telearbeit jede auf Informations- und Kommunikationstechnik gestützte Tätigkeit, die ganz oder teilweise außerhalb der Geschäftsräume verrichtet wird (Baustein OPS.1.2.4). Am häuslichen Arbeitsplatz kann nicht die gleiche Sicherheit vorausgesetzt werden wie im Büro; er ist oft auch für Besuch oder Familienangehörige zugänglich. Deshalb verlangt das BSI, alle relevanten Aspekte der Telearbeit zu regeln und den Mitarbeitenden die Regeln oder ein Merkblatt auszuhändigen (OPS.1.2.4.A1).

Telearbeit nach § 2h AVRAG in der seit 1.1.2025 geltenden Fassung

Begriff

Telearbeit liegt vor, wenn regelmäßig Arbeitsleistungen, insbesondere mit Informations- und Kommunikationstechnologie, in der Wohnung oder an einem sonstigen nicht zum Unternehmen gehörenden Ort erbracht werden (Abs. 1).

Vereinbarung

Telearbeit samt den Orten der Arbeitsleistung ist aus Beweisgründen schriftlich zu vereinbaren (Abs. 2). Aus wichtigem Grund kann jede Seite sie mit einem Monat Frist zum Monatsletzten kündigen (Abs. 4).

Arbeitsmittel

Die Arbeitgeberseite stellt die erforderlichen digitalen Arbeitsmittel bereit; davon kann vereinbart abgewichen werden, wenn sie die angemessenen und erforderlichen Kosten für eigene Geräte der Beschäftigten trägt, auch pauschal (Abs. 3).

Die Bausteine stammen aus dem IT-Grundschutz-Kompendium, Edition 2023. Das BSI löst das Kompendium durch Grundschutz++ ab; die Methodik soll laut BSI-Meilensteinplan am 27.10.2026 veröffentlicht werden. Die Anforderungen an das Homeoffice bleiben inhaltlich gültig.

02

Was das Unternehmen vorab regelt

Für Geschäftsführung, Führungskräfte, Personal und IT, bevor der erste Homeoffice-Tag beginnt.

- ☐ Telearbeitsvereinbarung schriftlich, mit den Orten, an denen gearbeitet werden darf (§ 2h Abs. 2 AVRAG)
- ☐ Regeln für die Telearbeit oder ein Merkblatt mit den Sicherheitsmaßnahmen ausgehändigt und regelmäßig aktualisiert (OPS.1.2.4.A1)
- ☐ Sicherheitsanforderungen an Homeoffice-Geräte festgelegt; nur Berechtigte haben Zugang, Nutzung nur für erlaubte Zwecke (OPS.1.2.4.A2)
- ☐ Digitale Arbeitsmittel bereitgestellt oder Kostenersatz für eigene Geräte vereinbart (§ 2h Abs. 3 AVRAG); bei privaten Geräten Risiko abgewogen (BSI)
- ☐ Sicherer Fernzugang eingerichtet, etwa ein kryptografisch abgesichertes VPN, beschränkt auf vertrauenswürdige Geräte und Personen (BSI)
- ☐ Geregelt, welche Kommunikationsmittel dienstlich genutzt werden dürfen und ob private Nutzung erlaubt ist (OPS.1.2.4.A7)
- ☐ Geregelt, welche Unterlagen und Datenträger nach Hause dürfen und wie sie transportiert werden (INF.8.A2)
- ☐ Mitarbeitende für die Gefahren sensibilisiert und in die Maßnahmen eingewiesen, regelmäßig wiederholt (OPS.1.2.4.A5)
- ☐ Ansprechperson für Hard- und Softwareprobleme benannt, Meldeweg für Verlust und Vorfälle bekannt (OPS.1.2.4.A9, BSI)

- ☐ Möglichkeit zur sicheren Entsorgung vertraulicher Unterlagen geschaffen (INF.8.A5)

03 —

Gerät und Zugang

Für Mitarbeitende: was am Laptop und beim Zugriff auf Firmendaten gilt.

- ☐ Dienstlich nur das vom Unternehmen bereitgestellte oder freigegebene Gerät nutzen
- ☐ Bildschirm sperren, sobald Sie den Platz verlassen, auch für kurze Zeit; Familie und Besuch nutzen das Gerät nicht
- ☐ Updates und Virenschutz nicht aufschieben; das BSI zählt aktuelle Patches und Signaturen zu den Standardmaßnahmen
- ☐ Laptop und mobile Datenträger verschlüsselt, wie es das BSI für tragbare Geräte empfiehlt
- ☐ Auf interne Systeme nur über den vorgesehenen sicheren Zugang zugreifen, etwa das VPN des Unternehmens
- ☐ Daten nicht dauerhaft lokal oder auf privaten Speichern ablegen; laut BSI werden wichtige Daten idealerweise gar nicht lokal gespeichert

04 —

Heimnetz und WLAN

Für Mitarbeitende: Router und WLAN nach den Empfehlungen des BSI für private Netze.

- ☐ Router-Verwaltung mit eigenem, sicherem Passwort geschützt, sofern das Gerät kein individuelles Passwort ab Werk hat
- ☐ Router-Firmware regelmäßig auf Aktualisierungen prüfen und einspielen
- ☐ WLAN-Passwort mit mindestens 20 zusammenhanglosen Zeichen
- ☐ Standard-Netzwerknamen ersetzt, damit er nichts über Hersteller oder Modell verrät
- ☐ Fernzugriff auf den Router abgeschaltet, wenn Sie ihn nicht brauchen
- ☐ Gäste-WLAN für Besuch und unsichere Geräte, getrennt von Homeoffice-Anwendungen
- ☐ Router-Konfiguration nur über https aufrufen; Firewall-Einstellungen nur mit Fachkenntnis ändern

Öffentliche WLANs in Café, Hotel oder Zug: Auf interne Systeme nur über einen sicheren Kanal wie das VPN des Unternehmens zugreifen (BSI).

05

Arbeitsplatz, Unterlagen und Gespräche

Für Mitarbeitende: Papier, Raum, Entsorgung und vertrauliche Gespräche zu Hause und unterwegs.

- ☐ Dienstliche Unterlagen und Datenträger in einem verschließbaren Schrank oder Rollcontainer aufbewahren (INF.8.A1)
- ☐ Arbeitsplatz aufgeräumt verlassen, keine vertraulichen Informationen offen liegen lassen (INF.8.A1)
- ☐ Fenster schließen und Türen absperren, wenn der Arbeitsplatz nicht besetzt ist (INF.8.A3)
- ☐ Wenn möglich, eigener Raum oder klar abgetrennter Bereich, ergonomisch eingerichtet (INF.8.A4)
- ☐ Ausdrücke vermeiden; vertrauliches Papier nicht in den Hausmüll, sondern nach Regel des Unternehmens entsorgen (INF.8.A5)
- ☐ Unterwegs Sichtschutzfolie nutzen und abwägen, welche Tätigkeiten an öffentlichen Orten nicht stattfinden (BSI)
- ☐ Vertrauliche Telefonate und Videokonferenzen so führen, dass Mitbewohner, Besuch oder Nachbarn nicht mithören; Kamera- und Bildschirmfreigabe vorher prüfen

Der Punkt zu Telefonaten und Videokonferenzen ist eine Empfehlung von TOMORIS; er folgt aus dem Hinweis des BSI, dass der häusliche Arbeitsplatz oft auch für Besuch oder Familienangehörige zugänglich ist.

06

Verlust, Vorfall und Support

Was Sie tun, wenn ein Gerät weg ist, etwas verdächtig wirkt oder die Technik streikt.

1

Verlust sofort melden

Gerät oder Datenträger verloren oder gestohlen: sofort über den bekannten Meldeweg melden, damit das Unternehmen Passwörter ändern und Zugänge sperren kann (BSI).

2 Verdacht melden, nicht selbst lösen

Verdächtige E-Mails, ungewöhnliche Meldungen oder Anmeldeanfragen an die benannte Stelle melden, Beobachtungen notieren und Maßnahmen nur nach Anweisung setzen.

3 Support nutzen

Bei Hard- oder Softwareproblemen die benannte Ansprechperson kontaktieren, statt Geräte selbst zu öffnen oder Software ohne Freigabe zu installieren (OPS.1.2.4.A9).

Die Checkliste ist eine Empfehlung von TOMORIS auf Grundlage der genannten BSI-Bausteine und -Empfehlungen. Gesetzlich vorgegeben sind in Österreich insbesondere die schriftliche Vereinbarung und die Arbeitsmittel nach § 2h AVRAG; für personenbezogene Daten gilt zusätzlich Art. 32 DSGVO.

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

KOSTENLOS PRÜFEN

Passwort-Generator

tomoris.com/tools/passwort-generator

WLAN-QR-Code-Generator

tomoris.com/tools/wlan-qr-generator

UMSETZUNG BESPRECHEN

Kontakt aufnehmen

tomoris.com/contact

contact@tomoris.com

07

Quellen

Alle Aussagen sind belegt. Gesetzestexte gelten in der jeweils geltenden Fassung.

- 1 BSI IT-Grundschutz-Kompendium, Baustein OPS.1.2.4 Telearbeit, Edition 2023
Einleitung, OPS.1.2.4.A1, A2, A5, A7, A9
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...
- 2 BSI IT-Grundschutz-Kompendium, Baustein INF.8 Häuslicher Arbeitsplatz, Edition 2023
Gefährdungslage 2.2, INF.8.A1 bis A5
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...
- 3 BSI-Empfehlung zur Cyber-Sicherheit: Tipps für sicheres mobiles Arbeiten (14.4.2021)
Punkte 3 bis 12
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Th...
- 4 BSI: Sicherheitstipps für privates und öffentliches WLAN
Router-Passwort, Firmware, WLAN-Passwort, Netzwerkname, Fernzugriff, Gast-Netz, https
www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Info...
- 5 Arbeitsvertragsrechts-Anpassungsgesetz (AVRAG), geltende Fassung im RIS
§ 2h idF BGBl. I Nr. 110/2024 und Inkrafttretensbestimmung, Fassung vom 25.10.2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...
- 6 BSI: Grundschutz++, Meilensteinplan (Stand Oktober 2026)
Ablösung des Kompendiums, Veröffentlichung der Methodik am 27.10.2026
www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standa...
- 7 Verordnung (EU) 2016/679 (DSGVO), Art. 32
Sicherheit der Verarbeitung
eur-lex.europa.eu/eli/reg/2016/679/oj/deu