

CHECKLIST · TOMORIS TOOLBOX

Working Safely from Home: Checklist for Employees and Managers

Rules for the company, device and access, home network, workspace, documents and conversations, loss and incidents, based on BSI IT-Grundschutz and § 2h AVRAG

UPDATED

Oct 25, 2026

LENGTH

PDF, 6 pages

ONLINE

tomoris.com/en/downloads/homeoffice-sicherheit-checkliste

AT A GLANCE

4

Areas for employees to check off

20

Characters minimum length of the Wi-Fi password (BSI)

In writing

Telework agreement including locations (§ 2h AVRAG)

Jan 1, 2025

Revised § 2h AVRAG in force

WHO IT IS FOR

- Employees who work from home regularly or occasionally
- Managers and HR departments that agree on working from home
- IT management and IT service providers that set up and support home workplaces
- Executive management of small and medium-sized companies

WHAT THIS COVERS

At home, much of what is taken for granted in the office is missing: locked rooms, a maintained network, a paper shredder, someone from IT down the hall. At the same time, family members and visitors share the space. This checklist summarizes what the company should settle before the first day of working from home, and what employees should observe regarding their device, home network, workspace, documents, and conversations. It is based on the BSI modules Telework and Home Workplace, the BSI tips for mobile working, and the Austrian rules on telework in § 2h AVRAG (Arbeitsvertragsrechts-Anpassungsgesetz, Austrian Employment Contract Law Adaptation Act).

This checklist is a TOMORIS recommendation and must be adapted to your company. The notes on employment law provide an overview and do not replace legal advice; the statutory text in its current version is authoritative.

CONTENTS

01	What is different at home	2
02	What the company settles in advance	3
03	Device and access	4
04	Home network and Wi-Fi	4
05	Workspace, documents, and conversations	5
06	Loss, incidents, and support	5
07	Sources	6

01 —

What is different at home

Why working from home needs its own rules and what Austrian employment law requires.

The BSI defines telework as any activity supported by information and communication technology that is performed wholly or partly outside the business premises (module OPS.1.2.4). A home workplace cannot be assumed to offer the same security as the office; it is often accessible to visitors or family members as well. The BSI therefore requires that all relevant aspects of telework be regulated and that employees receive the rules or an information sheet (OPS.1.2.4.A1).

Telework under § 2h AVRAG as amended, in force since January 1, 2025

Definition

Telework exists when work is performed regularly, in particular using information and communication technology, in the employee's home or at another location that does not belong to the company (para. 1).

Agreement

Telework, including the locations where the work is performed, must be agreed in writing for evidentiary purposes (para. 2). For good cause, either party may terminate it with one month's notice to the end of a month (para. 4).

Work equipment

The employer provides the necessary digital work equipment; the parties may agree otherwise if the employer bears the reasonable and necessary costs of the employees' own devices, also as a lump sum (para. 3).

The modules come from the IT-Grundschutz Compendium, Edition 2023. The BSI is replacing the Compendium with Grundschutz++; according to the BSI milestone plan, the methodology is to be published on October 27, 2026. The requirements for working from home remain valid in substance.

02

What the company settles in advance

For executive management, managers, HR, and IT, before the first day of working from home.

- ☐ Written telework agreement, including the locations where work is permitted (§ 2h para. 2 AVRAG)
- ☐ Rules for telework or an information sheet with the security measures handed out and regularly updated (OPS.1.2.4.A1)
- ☐ Security requirements for home office devices defined; only authorized persons have access, use only for permitted purposes (OPS.1.2.4.A2)
- ☐ Digital work equipment provided or reimbursement for personal devices agreed (§ 2h para. 3 AVRAG); for private devices, risk assessed (BSI)
- ☐ Secure remote access set up, such as a cryptographically secured VPN, restricted to trusted devices and persons (BSI)
- ☐ Rules defined on which communication tools may be used for work and whether private use is allowed (OPS.1.2.4.A7)
- ☐ Rules defined on which documents and storage media may be taken home and how they are transported (INF.8.A2)
- ☐ Employees made aware of the risks and instructed in the measures, repeated regularly (OPS.1.2.4.A5)
- ☐ Contact person for hardware and software problems named, reporting channel for loss and incidents known (OPS.1.2.4.A9, BSI)
- ☐ Means for the secure disposal of confidential documents provided (INF.8.A5)

03 —

Device and access

For employees: what applies to the laptop and to accessing company data.

- ☐ For work, use only the device provided or approved by the company
- ☐ Lock the screen as soon as you leave your desk, even briefly; family members and visitors do not use the device
- ☐ Do not postpone updates and antivirus updates; the BSI counts current patches and signatures among the standard measures
- ☐ Laptop and portable storage media encrypted, as the BSI recommends for portable devices
- ☐ Access internal systems only through the designated secure access, such as the company VPN
- ☐ Do not store data permanently on the local device or on private storage; according to the BSI, important data should ideally not be stored locally at all

04 —

Home network and Wi-Fi

For employees: router and Wi-Fi following the BSI recommendations for private networks.

- ☐ Router administration protected with its own secure password, unless the device comes with an individual factory password
- ☐ Check the router firmware regularly for updates and install them
- ☐ Wi-Fi password with at least 20 random characters
- ☐ Default network name replaced so that it reveals nothing about the manufacturer or model
- ☐ Remote access to the router turned off if you do not need it
- ☐ Guest Wi-Fi for visitors and insecure devices, separate from home office applications
- ☐ Open the router configuration only via https; change firewall settings only with expert knowledge

Public Wi-Fi in a café, hotel, or train: Access internal systems only through a secure channel such as the company VPN (BSI).

05

Workspace, documents, and conversations

For employees: paper, room, disposal, and confidential conversations at home and on the go.

- ☐ Keep work documents and storage media in a lockable cabinet or mobile pedestal (INF.8.A1)
- ☐ Leave the workspace tidy, do not leave confidential information lying around (INF.8.A1)
- ☐ Close windows and lock doors when the workspace is unoccupied (INF.8.A3)
- ☐ If possible, a separate room or clearly separated area, set up ergonomically (INF.8.A4)
- ☐ Avoid printouts; do not put confidential paper in household waste, dispose of it according to company rules (INF.8.A5)
- ☐ On the go, use a privacy screen filter and consider which tasks should not be done in public places (BSI)
- ☐ Conduct confidential phone calls and video conferences so that housemates, visitors, or neighbors cannot overhear; check camera and screen sharing beforehand

The item on phone calls and video conferences is a TOMORIS recommendation; it follows from the BSI's observation that a home workplace is often accessible to visitors or family members as well.

06

Loss, incidents, and support

What you do when a device is missing, something looks suspicious, or the technology fails.

- 1 **Report loss immediately**
Device or storage medium lost or stolen: report it immediately through the known reporting channel so that the company can change passwords and block access (BSI).
- 2 **Report suspicions, do not resolve them yourself**
Report suspicious emails, unusual messages, or sign-in requests to the designated contact, write down your observations, and take action only when instructed.

3 Use support

For hardware or software problems, contact the designated person instead of opening devices yourself or installing software without approval (OPS.1.2.4.A9).

This checklist is a TOMORIS recommendation based on the BSI modules and recommendations cited. In Austria, the law requires in particular the written agreement and the work equipment under § 2h AVRAG; for personal data, Art. 32 GDPR also applies.

NEXT STEP

Check It Yourself or Put It into Practice Together

CHECK FOR FREE

Password generator (German)

tomoris.com/tools/passwort-generator

Wi-Fi QR code generator (German)

tomoris.com/tools/wlan-qr-generator

DISCUSS IMPLEMENTATION

Get in Touch

tomoris.com/en/contact

contact@tomoris.com

07

Sources

All statements are supported by sources. Legislation applies in its current version.

- 1 **BSI IT-Grundschutz Compendium, module OPS.1.2.4 Telework, Edition 2023**
Introduction, 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 Compendium, module INF.8 Home Workplace, Edition 2023**
Threat landscape 2.2, INF.8.A1 to A5
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...
- 3 **BSI cyber security recommendation: Tips for secure mobile working (April 14, 2021)**
Items 3 to 12
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Th...
- 4 **BSI: Security tips for private and public Wi-Fi**
Router password, firmware, Wi-Fi password, network name, remote access, guest network, https
www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Info...
- 5 **Arbeitsvertragsrechts-Anpassungsgesetz (AVRAG), current version in the RIS**
§ 2h as amended by BGBl. I No. 110/2024 and entry-into-force provision, version as of October 25, 2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...
- 6 **BSI: Grundschutz++, milestone plan (as of October 2026)**
Replacement of the Compendium, publication of the methodology on October 27, 2026
www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standa...
- 7 **Regulation (EU) 2016/679 (GDPR), Art. 32**
Security of processing
eur-lex.europa.eu/eli/reg/2016/679/oj/deu