

CHECKLISTE · TOMORIS TOOLBOX

IT-Onboarding: Checkliste für den Eintritt neuer Mitarbeitender

Konto, Rechte, Gerät, Erstanmeldung, Datengeheimnis und Schulung geordnet einrichten, nach BSI IT-Grundschutz und DSGVO, mit den Schritten für Microsoft 365

STAND

25.10.2026

UMFANG

PDF, 7 Seiten

ONLINE

tomoris.com/downloads/it-onboarding-checkliste

AUF EINEN BLICK

ORP.2

BSI: geregelte Einarbeitung neuer Mitarbeitender

§ 6

DSG: auf das Datengeheimnis verpflichten

1 h

gilt ein befristeter Zugriffspass standardmäßig

30 Tage

höchste einstellbare Gültigkeit des Zugriffspasses

FÜR WEN

- HR und Personalverantwortliche, die Eintritte vorbereiten
- IT-Leitung und Administration von Microsoft 365 und Microsoft Entra ID
- Führungskräfte, die Aufgaben, Rechte und Einarbeitung festlegen

WORUM ES GEHT

Beim Eintritt entscheidet sich, ob Konten sauber angelegt, Rechte auf das Nötige beschränkt und neue Kolleginnen und Kollegen von Anfang an sicher arbeiten. Diese Checkliste ordnet den Eintritt in drei Phasen: vor dem ersten Arbeitstag, am ersten Tag und in den ersten Wochen. Sie stützt sich auf die Bausteine ORP.2, ORP.3 und ORP.4 des BSI IT-Grundschutz-Kompendiums, auf das Datengeheimnis nach § 6 DSGVO und nennt für Microsoft 365 die Schritte von der Benutzeranlage über den befristeten Zugriffsspass bis zur Automatisierung. Sie ist das Gegenstück zur Checkliste IT-Offboarding.

Diese Checkliste ist eine Empfehlung von TOMORIS und ersetzt keine arbeits- oder datenschutzrechtliche Beratung. Passen Sie sie an Ihr Unternehmen an. Bezeichnungen, Standardwerte und Lizenzen in Microsoft 365 können sich ändern; maßgeblich sind die aktuelle Dokumentation von Microsoft sowie DSGVO und DSGVO in der geltenden Fassung.

INHALT

01	Was beim Eintritt geregelt sein muss	2
02	Der Ablauf auf einen Blick	3
03	Vor dem ersten Arbeitstag	3
04	Am ersten Arbeitstag	4
05	In den ersten Wochen	5
06	Schritte in Microsoft 365	5
07	Rollenwechsel und Fremdpersonal	6
08	Wer macht was	6
09	Quellen	7

01

Was beim Eintritt geregelt sein muss

Einarbeitung, Rechte nach Bedarf, Verpflichtung und Schulung

Personalabteilung und Vorgesetzte müssen dafür sorgen, dass neue Mitarbeitende eingearbeitet und über Regelungen, Handlungsanweisungen und Verfahrensweisen informiert werden; eine Checkliste und eine feste Ansprechperson sollen helfen (BSI ORP.2.A1). Benutzerkennungen und Berechtigungen dürfen nur nach tatsächlichem Bedarf vergeben werden (ORP.4.A2). Vier Bereiche gehören deshalb zu jedem Eintritt:

- Konto und Rechte: eindeutig einer Person zugeordnet, nur was die Aufgabe braucht, dokumentiert (ORP.4.A1 bis A3).

- Geräte und Zugang: Zutritts- und Zugangsmittel ausgeben und die Ausgabe dokumentieren (ORP.4.A5 bis A7); die Geräteausgabe ebenso festhalten (Empfehlung von TOMORIS).
- Verpflichtung: Datengeheimnis nach § 6 DSG, Einhaltung von Gesetzen und internen Regeln (ORP.2.A14), Verarbeitung personenbezogener Daten nur auf Anweisung (Art. 29 und 32 Abs. 4 DSGVO).
- Einweisung und Schulung: sicherer Umgang mit der IT und Schulung nach Aufgaben (ORP.3.A3, A6).

Die Checkliste ist eine Empfehlung von TOMORIS. Der BSI IT-Grundschutz ist in Österreich keine Rechtspflicht, sondern ein Standard, an dem sie sich orientiert; § 6 DSG und die DSGVO gelten unmittelbar. Den Austritt behandelt die Checkliste IT-Offboarding.

02

Der Ablauf auf einen Blick

Drei Phasen bis zum Ende der Einarbeitung und der Fall eines Rollenwechsels

Phasen des IT-Onboardings (Empfehlung von TOMORIS)



Vor Tag 1

Vorbereiten

Rolle und Rechte festlegen, Konto und Lizenz anlegen, Gerät und Zugangsmittel vorbereiten, Ansprechperson benennen.



Tag 1

Starten

Einweisung, Verpflichtung auf das Datengeheimnis, sichere Erstanmeldung und Einrichtung der Multi-Faktor-Authentifizierung.



Monat 1

Einarbeiten

Schulung nach Aufgaben, Rechte prüfen, vorübergehende Rechte wieder entziehen.



Bei Wechsel

Anpassen

Bei neuer Rolle nicht mehr benötigte Rechte entfernen und neue nach Bedarf vergeben.

03

Vor dem ersten Arbeitstag

Konto, Rechte, Gerät und Ansprechperson vorbereiten

- ☐ Personalabteilung meldet Eintritt, Funktion und Beginn rechtzeitig an IT und Vorgesetzte.
- ☐ Benötigte Rechte aus der Funktion abgeleitet; Rechte über den Standard hinaus nur nach zusätzlicher Begründung und Prüfung (ORP.4.A2).
- ☐ Konto angelegt, das eindeutig einer Person zugeordnet ist; Anlage nur über eine separate administrative Rolle (ORP.4.A1, A2).
- ☐ Konto, Gruppen und Rechteprofil dokumentiert (ORP.4.A3).

- ☐ Zutritt und Zugang festgelegt; Ausgabe von Schlüsseln, Chipkarten oder Token wird dokumentiert (ORP.4.A5 bis A7).
- ☐ Gerät vorbereitet und inventarisiert; in Microsoft 365 Lizenz zugewiesen.
- ☐ Für die Stelle nötige Qualifikation geklärt (ORP.2.A15); bei Bedarf Angaben zur Vertrauenswürdigkeit geprüft, etwa den Lebenslauf (ORP.2.A7).
- ☐ Ansprechperson oder Pate bzw. Patin für die Einarbeitung benannt (ORP.2.A1).
- ☐ Bei Fremdpersonal: schriftliche Vertraulichkeitsvereinbarung, bevor Zugang zu vertraulichen Informationen besteht (ORP.2.A5).

04 —

Am ersten Arbeitstag

Einweisen, verpflichten, sicher anmelden

1

Einweisen

Über geltende Regelungen, Handlungsanweisungen und Verfahrensweisen informieren (ORP.2.A1); in den sicheren Umgang mit den IT-Komponenten einweisen, verbindliche und verständliche Richtlinien bereitstellen (ORP.3.A3).

2

Verpflichten und belehren

Soweit nicht schon kraft Gesetzes verpflichtet, vertraglich verpflichten, personenbezogene Daten nur auf Anordnung zu übermitteln und das Datengeheimnis auch nach Ende des Dienstverhältnisses zu wahren; über Übermittlungsanordnungen und die Folgen einer Verletzung belehren (§ 6 Abs. 2 und 3 DSGVO). Auf die Einhaltung von Gesetzen und internen Regeln verpflichten (ORP.2.A14).

3

Sicher erstmals anmelden

Für die erste Anmeldung einen befristeten Zugriffspass ausstellen, mit dem die Person ihre Anmeldeverfahren selbst einrichtet. TOMORIS empfiehlt, keine Passwörter per E-Mail zu verschicken und den Zugriffspass persönlich oder über einen getrennten Weg zu übergeben.

4

Mehr-Faktor-Anmeldung einrichten

Authenticator-App oder Passkey registrieren lassen. Details zur Einführung und zu den Methoden enthält die Checkliste MFA in Microsoft 365.

5

Gerät und Zugangsmittel übergeben

Schlüssel, Chipkarten und Token übergeben und die Ausgabe dokumentieren (ORP.4.A5 bis A7), das Gerät ebenso (Empfehlung von TOMORIS). Die Person zur Geheimhaltung von Passwörtern anhalten (ORP.4.A8).

6

Meldeweg erklären

Zeigen, wie verdächtige E-Mails und Sicherheitsvorfälle gemeldet werden und wer Ansprechperson ist (Empfehlung von TOMORIS).

05

In den ersten Wochen

Schulen, Rechte prüfen, Einarbeitung abschließen

- ☐ Nach Aufgaben und Verantwortlichkeiten zu Informationssicherheit geschult (ORP.3.A6).
- ☐ Darauf hingewiesen, dass Informationen aus der Arbeit nur für den internen Gebrauch bestimmt sind und Informationssicherheit auch außerhalb der Arbeitszeit gilt (ORP.2.A14).
- ☐ Aufgaben und Zuständigkeiten dokumentiert (ORP.2.A14).
- ☐ Rechte mit den tatsächlichen Aufgaben abgeglichen; Dokumentation und Rechtevergabe stimmen überein (ORP.4.A3).
- ☐ Vorübergehend vergebene Rechte, etwa für die Einarbeitung, wieder entzogen (abgeleitet aus ORP.4.A2).
- ☐ Vertretung für die Aufgaben der neuen Person geregelt (ORP.2.A3).
- ☐ Einarbeitung mit Vorgesetzten und Ansprechperson abgeschlossen und Rückmeldung zur Checkliste eingeholt (Empfehlung von TOMORIS).

06

Schritte in Microsoft 365

Benutzer, befristeter Zugriffspass, Geräte und Automatisierung

Benutzer anlegen

Im Microsoft 365 Admin Center Benutzer anlegen und Lizenz zuweisen. Microsoft empfiehlt Rollen mit den geringsten Berechtigungen; Globaler Administrator soll auf Notfallszenarien beschränkt bleiben.

Befristeter Zugriffspass (TAP)

Zeitlich begrenzte Kennung für eine oder mehrere Anmeldungen, mit der Benutzende kennwortlose Methoden einrichten. Vorher in der Richtlinie für Authentifizierungsmethoden aktivieren und Benutzer oder Gruppen auswählen. Ab Werk 1 bis 8 Stunden gültig, Standard 1 Stunde; in der Richtlinie von 10 Minuten bis 30 Tage einstellbar; einmalige Verwendung kann erzwungen werden.

Windows Autopilot

Richtet neue Windows-Geräte ein und konfiguriert sie vor, damit sie bereit für den Einsatz sind; auch zum Zurücksetzen und Wiederherstellen. Die automatische Registrierung in Intune setzt Entra ID P1 oder P2 voraus.

Lebenszyklus-Workflows

Automatisieren Aufgaben für Eintritt, Wechsel und Austritt, etwa eine E-Mail an Vorgesetzte sieben Tage vor dem Eintrittsdatum oder das Erstellen temporärer Kennwörter. Erfordern Lizenzen für Microsoft Entra ID Governance oder Microsoft Entra Suite.

Bezeichnungen, Standardwerte und Lizenzbedingungen in Microsoft 365 können sich ändern; maßgeblich ist die aktuelle Dokumentation von Microsoft. Kennwortrichtlinien legen Sie am besten in einer eigenen Passwortrichtlinie fest.

07

Rollenwechsel und Fremdpersonal

Wenn sich Aufgaben ändern oder Externe mitarbeiten

- ☐ Bei personellen Veränderungen nicht mehr benötigte Kennungen und Berechtigungen entfernen (ORP.4.A2), statt neue Rechte nur hinzuzufügen.
- ☐ Externes Personal wie eigene Mitarbeitende auf Gesetze, Vorschriften und interne Regeln verpflichten (ORP.2.A4).
- ☐ Kurzfristig eingesetztes Fremdpersonal in sicherheitsrelevanten Bereichen beaufsichtigen, längerfristiges wie eigenes Personal einweisen (ORP.2.A4).
- ☐ Konten von Fremdpersonal mit Ablaufdatum anlegen und bei Ende der Tätigkeit Zugangsberechtigungen zurücknehmen (ORP.2.A4; Ablaufdatum als Empfehlung von TOMORIS).

08

Wer macht was

Zuständigkeiten im Onboarding

Zuständigkeiten (Aufteilung angelehnt an BSI ORP.2 und ORP.4)

ROLLE	AUFGABE IM ONBOARDING
Personalabteilung	Meldet den Eintritt, sorgt mit den Vorgesetzten für die Einarbeitung, holt die Verpflichtung auf das Datengeheimnis ein.
Vorgesetzte	Legen Aufgaben, benötigte Rechte und Vertretung fest, benennen die Ansprechperson, geben Sonderrechte frei.

IT-Betrieb	Legt Konto, Gruppen und Rechte an, dokumentiert sie, bereitet Gerät und Zugangsmittel vor, stellt den Zugriffspass aus.
Datenschutz	Stellt Text und Belehrung zum Datengeheimnis bereit.
Neue Mitarbeitende	Richten ihre Anmeldemethoden ein, halten Passwörter geheim, nehmen an Einweisung und Schulung teil.

Die genaue Aufteilung ist eine Empfehlung; entscheidend ist, dass jede Aufgabe eine zuständige Person hat. Führen Sie die Checkliste je Eintritt und legen Sie sie zur Personalakte oder zur IT-Dokumentation.

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

UMSETZUNG BESPRECHEN

Kontakt aufnehmen

tomoris.com/contact

contact@tomoris.com

09

Quellen

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

- BSI IT-Grundschutz-Kompodium, Baustein ORP.2 Personal (Edition 2023)**
ORP.2.A1, A3, A4, A5, A7, A14, A15, gelesen am 25.10.2026
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...
- BSI IT-Grundschutz-Kompodium, Baustein ORP.3 Sensibilisierung und Schulung (Edition 2023)**
ORP.3.A3, A6, gelesen am 25.10.2026
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...
- BSI IT-Grundschutz-Kompodium, Baustein ORP.4 Identitäts- und Berechtigungsmanagement (Edition 2023)**
ORP.4.A1 bis A3, A5 bis A8, gelesen am 25.10.2026
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...
- Datenschutzgesetz (DSG), geltende Fassung im RIS**
§ 6 Datengeheimnis, gelesen am 25.10.2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...
- Verordnung (EU) 2016/679 (DSGVO), deutsche Fassung auf EUR-Lex**
Art. 29 und Art. 32 Abs. 4, gelesen am 25.10.2026
eur-lex.europa.eu/eli/reg/2016/679/oj/deu
- Microsoft Learn: Benutzer hinzufügen und Lizenzen zuweisen**
Rollen mit geringsten Berechtigungen, Lizenzzuweisung, gelesen am 25.10.2026
learn.microsoft.com/de-de/microsoft-365/admin/add-users/add-use...
- Microsoft Learn: Was sind Lebenszyklus-Workflows?**
Phasen, Beispiel, Lizenzanforderungen, gelesen am 25.10.2026
learn.microsoft.com/de-de/entra/id-governance/what-are-lifecycl...
- Microsoft Learn: Befristeten Zugriffspass in Microsoft Entra ID konfigurieren**
Zweck, Richtlinie, Lebensdauer, einmalige Verwendung, gelesen am 25.10.2026
learn.microsoft.com/de-de/entra/identity/authentication/howto-a...
- Microsoft Learn: Übersicht über Windows Autopilot**
Zweck; Entra ID P1 oder P2 für die Intune-Registrierung, gelesen am 25.10.2026
learn.microsoft.com/de-de/autopilot/overview