

VORLAGE · TOMORIS TOOLBOX

Smartphones und Tablets: Richtlinie für Firmen- und Privatgeräte

Mustertext mit Platzhaltern für Firmengeräte und BYOD, Mindestanforderungen nach BSI SYS.3.2.1 und NIST SP 800-124, Umsetzung mit Microsoft Intune

STAND

25.10.2026

UMFANG

PDF, 12 Seiten

ONLINE

tomoris.com/downloads/mobile-geraete-richtlinie-vorlage

AUF EINEN BLICK

A1

Richtlinie vor dem Einsatz:
BSI SYS.3.2.1.A1

2

Varianten: nur Firmengeräte oder auch BYOD

Nie

sieht Intune private Fotos,
Mails, Kontakte

30 Tage

offline, dann Firmendaten
löschen (Microsoft)

FÜR WEN

- IT-Leitung und Administration, die Firmen- und Privatgeräte für E-Mail, Chats und Dateien zulassen und absichern
- Personalabteilung, die Nutzung, Verlust und Austritt mit Arbeitsvertrag, Datenschutz und Betriebsrat abstimmt
- Geschäftsführung kleiner und mittlerer Unternehmen, die die Richtlinie freigibt und verantwortet

WORUM ES GEHT

Wer Smartphones oder Tablets für dienstliche Daten zulässt, braucht vorher eine Richtlinie; das BSI verlangt sie im IT-Grundschutz als Basis-Anforderung SYS.3.2.1.A1. Diese Vorlage enthält einen Mustertext mit Platzhaltern für Firmengeräte und, als Variante, für Privatgeräte (BYOD): Zulassung, Mindestanforderungen an Updates, Sperre und Verschlüsselung, Apps, Verlust und Diebstahl, Rückgabe beim Austritt. Sie zeigt, wie sich dienstliche und private Daten mit App-Schutzrichtlinien oder Arbeitsprofil trennen lassen, ohne das ganze Privatgerät zu verwalten, und was die IT dabei sieht und was nicht.

Diese Vorlage ist an Ihr Unternehmen, Ihre Geräte und Ihr MDM anzupassen und ersetzt keine Rechtsberatung, insbesondere nicht zu ArbVG, AVRAG und DSGVO; maßgeblich ist der Gesetzestext in der geltenden Fassung. IT-Grundschutz und NIST sind Empfehlungen, keine gesetzlichen Pflichten. Funktionen, Bezeichnungen, Menüs und Lizenzen von Microsoft können sich ändern.

Nutzung: Diese Vorlage dürfen Sie für den eigenen Gebrauch anpassen; weitergeben dürfen Sie sie nur in unveränderter Form.

INHALT

01	Wozu die Richtlinie dient	3
02	Firmengerät oder Privatgerät: die Varianten	3
03	Was die IT auf Privatgeräten sieht	4
04	Mindestanforderungen an jedes Gerät	5
05	Umsetzung mit Microsoft Intune und Entra ID	6
06	Verlust, Diebstahl und Austritt	7
07	Mustertext, Teil 1: Geltung, Zulassung und Mindestanforderungen	8
08	Mustertext, Teil 2: Privatgeräte, Verlust und Rückgabe	9
09	Checkliste: die Richtlinie einführen	11
10	Quellen	12

01

Wozu die Richtlinie dient

Was BSI und NIST von einer Richtlinie für Smartphones und Tablets verlangen und wie verbindlich das ist.

Smartphones und Tablets gehen leichter verloren als ein Bürorechner und werden an Orten genutzt, die das Unternehmen nicht kontrolliert (NIST SP 800-124 Rev. 2, 3.1.2). Das IT-Grundschutz-Kompendium des deutschen BSI (Edition 2023) verlangt als Basis-Anforderung: Bevor eine Institution Smartphones oder Tablets einsetzt, MUSS sie eine Richtlinie für Nutzung und Kontrolle der Geräte festlegen, auch dazu, wer damit auf welche Informationen zugreifen darf (SYS.3.2.1.A1). Der Baustein gilt für alle dienstlich eingesetzten Geräte; seine Gefährdungslage nennt ausdrücklich auch private Geräte (BYOD).

Eine verbindliche Richtlinie für Mitarbeitende SOLLTE Nutzung, Pflege, Aufbewahrung und Verlustmeldung regeln und verbieten, Verwaltungssoftware zu entfernen, das Gerät zu rooten oder Sicherheitseinstellungen zu ändern (SYS.3.2.1.A10). Wer ein Mobile Device Management (MDM) einsetzt, MUSS eine schriftliche Strategie festlegen, die auch das Betriebsmodell regelt: Privatgeräte, persönlich zugeordnete oder gemeinsam genutzte Firmengeräte (SYS.3.2.2.A1).

Pflicht oder Empfehlung? IT-Grundschutz und NIST sind in Österreich keine Gesetze, sondern anerkannte Standards. Das BSI teilt Anforderungen in Basis- (B), Standard- (S) und Anforderungen bei erhöhtem Schutzbedarf (H) ein; innerhalb jeder Anforderung ist MUSS unbedingt zu erfüllen, von SOLLTE darf nur nach sorgfältiger Abwägung und mit stichhaltiger Begründung abgewichen werden. Die Vorlage ist eine Empfehlung von TOMORIS. Gesetzlich zu beachten sind vor allem DSGVO, ArbVG und AVRAG (Abschnitt 03), für NIS2-Einrichtungen auch § 32 Abs. 4 lit. i NISG 2026 (Abschnitt 06).

02

Firmengerät oder Privatgerät: die Varianten

Welche Betriebsmodelle es gibt, wem Gerät und Daten gehören und wie sich Firmendaten auf Privatgeräten trennen lassen.

Betriebsmodelle nach NIST SP 800-124 Rev. 2 (5.1.3); Variante A der Vorlage erlaubt nur Firmengeräte, Variante B auch Privatgeräte

MODELL	EIGENTUM	TYPISCHE VERWALTUNG
Nur dienstlich genutztes Firmengerät	Gerät und alle Daten: Unternehmen	vollständig verwaltet, nur freigegebene Apps (Allowlist)
Firmengerät mit privater Nutzung (COPE)	Gerät und Daten: Unternehmen, auch bei privater Nutzung	verwaltet, offizielle App Stores, Sperrliste für Apps
Privatgerät (BYOD), auch aus einer Geräteliste des Unternehmens (CYOD)	Gerät: Mitarbeiterin oder Mitarbeiter; Firmendaten darauf: Unternehmen	nur Firmen-Apps und -Daten; App-Verwaltung (MAM) statt Geräteverwaltung kann Datenschutzbedenken entschärfen (4.2.2)

Drei Wege, Firmendaten auf Privatgeräten zu trennen (Beispiel Microsoft Intune)

App-Schutzrichtlinien ohne Registrierung (MAM)

Intune schützt Firmendaten in Apps wie Outlook, Word oder OneDrive ohne Registrierung des Geräts, nur wenn die App mit dem Firmenkonto genutzt wird; private Konten bleiben unberührt. Zertifikate, WLAN und VPN werden nicht verteilt; unter Android ist das Unternehmensportal nötig.

Android: persönliches Arbeitsprofil

Eine getrennte Partition auf Betriebssystemebene für Firmen-Apps und -Daten, die Intune verwaltet; Zertifikate, WLAN und VPN lassen sich verteilen. Microsoft empfiehlt das Arbeitsprofil, wenn Sie solche MDM-Funktionen brauchen, sonst MAM; beides lässt sich kombinieren.

iPhone und iPad: kontogesteuerte Benutzerregistrierung

Ab iOS/iPadOS 15 fügt die Person in den Einstellungen unter „VPN & Geräteverwaltung“ (VPN & Device Management) ihr Firmenkonto hinzu. Firmendaten liegen auf einem eigenen Volume und in verwalteten Apps, getrennt von privaten Daten; Intune hat nur eingeschränkte Funktionen, VPN etwa nur pro App.

Das BSI warnt bei BYOD, dass eine Löschung über das MDM auch private Daten treffen kann und Firmendaten bei einer Reparatur unbefugt eingesehen werden oder beim Austritt ungeregelt auf dem Gerät bleiben können (SYS.3.2.1, Gefährdung 2.9). Empfehlung von TOMORIS: Für Privatgeräte genügen in vielen KMU App-Schutzrichtlinien; eine Registrierung lohnt sich, wenn Zertifikate, WLAN- oder VPN-Profile nötig sind. Sehr einschränkende oder überwachend wirkende Vorgaben können Mitarbeitende laut NIST dazu verleiten, auf Schatten-IT auszuweichen (3.1.13).

03

Was die IT auf Privatgeräten sieht

Welche Daten Intune laut Microsoft nie, immer oder nur unter Umständen sieht, und was HR und Betriebsrat klären müssen.

Bei App-Schutzrichtlinien und beim Android-Arbeitsprofil können Administratoren laut Microsoft Daten, die den Benutzern gehören oder von ihnen kontrolliert werden, weder lesen noch löschen. Die Tabelle zeigt, was die Organisation bei einem in Intune registrierten Gerät sieht; bei anderen MDM-Produkten prüfen Sie die Angaben des Herstellers.

Was die Organisation bei registrierten Geräten sieht (Microsoft Learn, Stand 20.8.2026)

ANGABE	FIRMENGERÄT	PRIVATGERÄT
Anrufe, Browserverlauf, E-Mails, SMS, Kontakte, Kalender, Kennwörter, Fotos, eigene Dokumente	nie	nie
Eigentümer, Geräte name, Modell, Hersteller, Betriebssystem und Version	ja	ja
Seriennummer und IMEI	ja	ja; bei Apple-Benutzerregistrierung nicht

Telefonnummer	vollständig; bei Android mit Arbeitsprofil die letzten vier Ziffern	die letzten vier Ziffern; bei Apple-Benutzerregistrierung nicht
Standort	nur bei Verlust; iPhone und iPad zeigen dann einen Hinweis auf dem Sperrbildschirm	nein
Installierte Apps	alle; bei Android mit Arbeitsprofil nur die im Arbeitsprofil	die verwalteten Apps, je nach Konfiguration mehr

Für HR: Kontrollmaßnahmen und technische Systeme zur Kontrolle der Arbeitnehmer, die die Menschenwürde berühren, bedürfen der Zustimmung des Betriebsrats (§ 96 Abs. 1 Z 3 ArbVG). Systeme, die Arbeitnehmerdaten über allgemeine Angaben zur Person und fachliche Voraussetzungen hinaus automationsunterstützt ermitteln, verarbeiten oder übermitteln, brauchen ebenfalls seine Zustimmung, soweit ihre Verwendung über Pflichten aus Gesetz, Normen der kollektiven Rechtsgestaltung oder Arbeitsvertrag hinausgeht; diese Zustimmung kann die Schlichtungsstelle ersetzen (§ 96a Abs. 1 Z 1 und Abs. 2 ArbVG). Ohne Betriebsrat sind Kontrollmaßnahmen, die die Menschenwürde berühren, nur mit Zustimmung der Arbeitnehmerin oder des Arbeitnehmers zulässig (§ 10 Abs. 1 AVRAG). Ob das auf Ihre Konfiguration zutrifft, ist im Einzelfall zu klären; dieser Hinweis ersetzt keine Rechtsberatung.

Informieren Sie vor der Registrierung über Zwecke und Rechtsgrundlage, Empfänger und Speicherdauer (Art. 13 Abs. 1 lit. c und e, Abs. 2 lit. a DSGVO), nennen Sie dabei die erhobenen Gerätedaten und erheben Sie nur, was nötig ist (Art. 5 Abs. 1 lit. c DSGVO). Standortdaten sollten laut NIST nur mit Zustimmung und klarer Beschreibung genutzt werden (3.1.11); Geofencing erzeugt Bewegungsprofile und kann zur unzulässigen Kontrolle missbraucht werden (BSI SYS.3.2.2, Gefährdung 2.4).

04

Mindestanforderungen an jedes Gerät

Updates, Bildschirmsperre, Verschlüsselung, Apps und Schnittstellen, mit der Fundstelle im IT-Grundschutz.

Technische Mindestanforderungen (B, S, H = Kategorie der Anforderung; SOLLTE-Teile in Basis-Anforderungen sind markiert)

BEREICH	ANFORDERUNG	GRUNDLAGE
Updates	Update-Zeitraum des Herstellers bei der Beschaffung prüfen, Geräte ohne Sicherheitsupdates aussondern, solche Apps nicht mehr einsetzen (SOLLTE); Updates rasch verteilen, etwa wöchentlich, zuerst an eine Pilotgruppe	SYS.3.2.1.A5 (B); NIST 4.3.6
Bildschirmsperre	angemessen komplexer Sperrcode, automatische Sperre nach kurzer Zeit, keine vertraulichen Inhalte auf dem Sperrbildschirm; nach mehreren Fehlversuchen zurücksetzen (SOLLTE); Biometrie nur, wenn sie mindestens so gut schützt	SYS.3.2.1.A4 (B), A18 (S)
Verschlüsselung	Gerätespeicher und SD-Karten mit schützenswerten Daten verschlüsseln	SYS.3.2.1.A11 (S)

Apps	erlaubte Quellen festlegen, andere technisch unterbinden; nur freigegebene Apps (SOLLTE)	SYS.3.2.1.A8 (B)
Manipulation	kein Rooten oder Jailbreak; manipulierte Geräte erkennen und sperren	SYS.3.2.1.A10 (S); SYS.3.2.2.A17 (H); Microsoft, Stufe 1
Berechtigungen und Schnittstellen	App-Zugriff auf Kamera, Mikrofon, Standort und Gesundheitsdaten restriktiv; nicht benötigte Funktionen und Schnittstellen abschalten (SOLLTE)	SYS.3.2.1.A3, A6 (B), A16 (S)
Cloud-Dienste	festlegen, welche Cloud-Dienste für Firmendaten erlaubt sind und ob bei privater Nutzung	SYS.3.2.1.A2 (B)

Konkrete Werte wie Sperrzeit oder Länge des Sperrcodes nennt das BSI nicht; der Mustertext enthält dafür Vorschläge von TOMORIS. Auf Privatgeräten ohne Registrierung prüfen App-Schutzrichtlinien beim Start der Firmen-App etwa die Mindestversion des Betriebssystems, Jailbreak oder Root und unter Android die Gerätesperre und sperren sonst den Zugriff (Microsoft, Datenschutzframework).

05

Umsetzung mit Microsoft Intune und Entra ID

Lizenzen, App-Schutzrichtlinie, bedingter Zugriff und Registrierung in vier Schritten.

1

Lizenzen und Rollen klären

App-Schutzrichtlinien: je Benutzer ein Microsoft-Entra-Konto mit zugewiesener Intune-Lizenz; für Outlook zusätzlich ein Exchange-Online-Postfach mit Microsoft-365-Lizenz, für Word, Excel und PowerPoint Microsoft 365 Apps for Business oder Enterprise. App-basierter bedingter Zugriff: Microsoft Entra ID P1 oder P2, auch für die erfassten Benutzer; einrichten können ihn Sicherheitsadministratoren und Administratoren für bedingten Zugriff.

2

App-Schutzrichtlinien anlegen

Im Microsoft Intune Admin Center je eine Richtlinie für iOS/iPadOS und Android. Microsoft empfiehlt für die meisten mobilen Benutzer Stufe 2 seines Datenschutzframeworks: Organisationsdaten verschlüsseln, PIN, Sicherungen blockieren, Kopien nur in OneDrive for Business, SharePoint und Fotobibliothek, Ausschneiden und Kopieren nur in verwaltete Apps (Einfügen in Firmen-Apps bleibt erlaubt), Mindestversion des Betriebssystems, Firmendaten nach 30 Tagen offline löschen, Geräte mit Jailbreak oder Root blockieren.

3

Bedingten Zugriff verlangen

Erst wenn die App-Schutzrichtlinien gelten: im Microsoft Entra Admin Center unter Entra ID › Conditional Access › Policies (Richtlinien) für alle Benutzer und Ressourcen auf Android und iOS die Gewährung „App-Schutzrichtlinie erforderlich“ verlangen, ein Notfallkonto ausnehmen, zuerst im Modus „Nur Bericht“ prüfen. „Genehmigte Client-App erforderlich“ ist seit 30.6.2026 schreibgeschützt: Richtlinien damit lassen sich nicht mehr anlegen oder bearbeiten, nur deaktivieren oder löschen; bestehende wirken weiter. Die Geräte registrieren sich über Microsoft Authenticator (iOS) oder das Unternehmensportal (Android) in Entra ID.

4

Geräte registrieren

Firmengeräte vor der Ausgabe im Werkzustand ins MDM aufnehmen (SYS.3.2.2.A4), etwa über die automatisierte Geräteregistrierung von Apple oder Zero-Touch von Android (NIST 5.3.4.2). Privatgeräte über das Android-Arbeitsprofil, die Apple-Benutzerregistrierung oder nur mit App-Schutzrichtlinien.

Abweichung bewusst entscheiden: Das BSI empfiehlt, Smartphones und Tablets per MDM zu verwalten (SOLLTE, SYS.3.2.1.A32); der Baustein SYS.3.2.2 behandelt BYOD nicht. Wer Privatgeräte nur mit App-Schutzrichtlinien absichert, begründet das nachvollziehbar und dokumentiert es, etwa im Sicherheitskonzept. Damit App-Schutzrichtlinien erzwungen werden, rät Microsoft zum bedingten Zugriff. Menüs und Bezeichnungen: Microsoft Learn, Oktober 2026.

06

Verlust, Diebstahl und Austritt

Was sofort zu tun ist, welche Löschaktion zu welchem Gerät passt und was beim Austritt geschieht.

Ablauf bei Verlust oder Diebstahl



Sofort

Melden

Die Person meldet den Verlust oder unberechtigte Änderungen an Gerät und Software sofort an die zuständige Stelle (SYS.3.2.1.A7).



Dann

Sperren und löschen

Die IT sperrt den Zugriff auf Firmendaten und löscht aus der Ferne: Firmengeräte vollständig, Privatgeräte nur die Firmendaten (NIST 4.3.3, 4.3.11).



Binnen 72 h

Datenschutz prüfen

Waren personenbezogene Daten betroffen, ist die Verletzung unverzüglich und möglichst binnen 72 Stunden ab Kenntnis der Aufsichtsbehörde zu melden, außer sie führt voraussichtlich nicht zu einem Risiko (Art. 33 Abs. 1 DSGVO); dokumentiert wird jede Verletzung (Abs. 5).

Löschaktionen in Microsoft Intune

AKTION	WAS SIE ENTFERNT	PASSEND FÜR
Zurücksetzen (Wipe)	das ganze Gerät auf Werkseinstellungen, alle Benutzerdaten und Einstellungen	registrierte Firmengeräte

Zurückziehen (Retire)	verwaltete Apps, Einstellungen und Profile, beim Android-Arbeitsprofil dessen gesamten Inhalt; persönliche Daten bleiben	registrierte Privatgeräte
Selektives Zurücksetzen	nur die Firmendaten in Apps mit App-Schutzrichtlinie, sobald die App läuft	Privatgeräte ohne Registrierung

Fernlöschung allein schützt nicht: Mit den Bordmitteln von iOS und Android wirkt sie nur bei eingeschaltetem, verbundenem Gerät, und Angreifer können Daten vorher auslesen (NIST 4.3.3). Sperrcode und Verschlüsselung sind die erste Schutzschicht. Löschen Sie Privatgeräte nie ohne Zustimmung vollständig; das Löschen von Daten, die nicht dem Unternehmen gehören, kann laut NIST rechtliche Probleme verursachen (4.3.12).

Beim Austritt setzt die IT zurückgegebene Firmengeräte vor der Weitergabe auf Werkseinstellungen zurück. SIM- und SD-Karten löscht das nicht: SD-Karten entnehmen und löschen, SIM-Karten nach der Regelung zur Rufnummer behandeln; bei der Entsorgung empfiehlt NIST, beide zu entnehmen und zu vernichten (5.5). Nach der Außerbetriebnahme sollen keine schutzbedürftigen Daten auf Gerät oder Speichermedien bleiben (SYS.3.2.2.A22).

NIS2-Einrichtungen: § 32 Abs. 4 lit. i NISG 2026 verlangt Maßnahmen zu Sicherheit des Personals, Zugriffskontrolle und Management von Anlagen. Konkretisiert wird das in Anhang Nr. 12 der Durchführungsverordnung (EU) 2024/2690, den § 2 NISV 2026 für alle wesentlichen und wichtigen Einrichtungen anwendbar macht: Nach Nr. 12.5 sind Abgabe, Rückgabe oder Löschung von Anlagen und Werten wie Geräten bei Ende des Beschäftigungsverhältnisses zu regeln und zu dokumentieren; sonst dürfen sie nicht mehr auf die Systeme zugreifen können.

07

Mustertext, Teil 1: Geltung, Zulassung und Mindestanforderungen

Paragrafen 1 bis 5. Ersetzen Sie alles in eckigen Klammern und wählen Sie Variante A oder B.

Ersetzen Sie die Platzhalter in eckigen Klammern, wählen Sie bei | eine Möglichkeit und streichen Sie, was nicht zutrifft; in Variante A (nur Firmengeräte) entfällt § 6. Zahlen wie [5] Minuten sind Vorschläge von TOMORIS ([30] Tage offline ist Microsofts Wert aus Stufe 2), Regeln ohne Fundstelle organisatorische Ergänzungen von TOMORIS. Stimmen Sie den Text mit Datenschutz, Personalabteilung und, falls vorhanden, Betriebsrat ab.

Richtlinie für Smartphones und Tablets der [Unternehmen], Fassung [Version] vom [Datum]

§ 1 Zweck und Geltungsbereich

Diese Richtlinie regelt die dienstliche Nutzung von Smartphones und Tablets bei [Unternehmen]. Sie gilt für alle Beschäftigten und [externe Personen, z. B. überlassene Arbeitskräfte], für Firmengeräte und für jedes Gerät, mit dem auf dienstliche E-Mails, Dateien, Chats oder Anwendungen zugegriffen wird. Verantwortlich ist [Name, Funktion]; Ansprechstelle ist [IT-Stelle, Kontakt] (SYS.3.2.1.A1).

§ 2 Zugelassene Geräte

Variante A: Dienstliche Daten dürfen nur auf Firmengeräten verarbeitet werden, die [Unternehmen] beschafft und in [MDM, z. B. Microsoft Intune] aufgenommen hat. Variante B: Zusätzlich sind Privatgeräte zugelassen, wenn sie § 3 erfüllen und nach § 6 eingebunden sind; [Regelung zu Kosten und Tarif]. Zugelassen sind [Betriebssysteme und Mindestversionen] (SYS.3.2.2.A2).

§ 3 Mindestanforderungen

Jedes Gerät mit dienstlichen Daten erhält noch Sicherheitsupdates des Herstellers; angebotene Updates installieren Sie binnen [7] Tagen. Ein Sperrcode aus mindestens [6] Ziffern schützt das Gerät, es sperrt sich nach höchstens [5] Minuten und zeigt keine Vorschau vertraulicher Nachrichten auf dem Sperrbildschirm. Biometrie nur nach Freigabe durch [IT-Stelle]. Der Speicher ist verschlüsselt; Rooten oder Jailbreak sind verboten. Geräte, die das nicht erfüllen, erhalten keinen Zugriff (SYS.3.2.1.A4, A5, A10, A11, A18).

§ 4 Apps und Cloud-Dienste

Auf Firmengeräten installieren Sie Apps nur aus [den App Stores von Apple und Google | dem Unternehmensportal]. Dienstliche Daten bearbeiten Sie nur in den Apps aus Anlage 1 mit Ihrem Firmenkonto und speichern sie nur in [OneDrive for Business, SharePoint]; private Cloud-Speicher, Messenger und E-Mail-Konten sind dafür nicht erlaubt. Apps erhalten nur die nötigen Berechtigungen, etwa für Kamera, Mikrofon oder Standort (SYS.3.2.1.A2, A6, A8).

§ 5 Private Nutzung von Firmengeräten

[Firmengeräte dienen nur dienstlichen Zwecken. | Private Nutzung ist in geringem Umfang erlaubt, private Apps nur aus den offiziellen App Stores.] Gerät und Firmendaten bleiben Eigentum von [Unternehmen]. Private Daten sichern Sie selbst; bei Verlust und Rückgabe wird das Gerät vollständig gelöscht. Verwaltungssoftware und Sicherheitseinstellungen ändern Sie nicht (SYS.3.2.1.A10).

08 —

Mustertext, Teil 2: Privatgeräte, Verlust und Rückgabe

Paragrafen 6 bis 10, Anlage 1 zu den freigegebenen Apps und die Kenntnisnahme zum Unterschreiben.

§ 6 Privatgeräte (nur Variante B)

Auf Privatgeräten schützt [Unternehmen] nur Firmen-Apps und Firmendaten mit [App-Schutzrichtlinien | Android-Arbeitsprofil | Apple-Benutzerregistrierung]; private Apps und Daten bleiben unverwaltet. Firmendaten bleiben in diesen Apps; Kopieren in private Apps und private Sicherungen sind gesperrt. Die Firmen-Apps verlangen [eine PIN]; nach [30] Tagen offline werden ihre Firmendaten gelöscht. Vor einer Reparatur lassen Sie die Firmendaten von [IT-Stelle] entfernen.

§ 7 Datenschutz

Auf Privatgeräten sieht [Unternehmen] nur [Angaben aus der Tabelle in Abschnitt 03 je nach Verfahren, bei Registrierung etwa Eigentümer, Geräte-Name, Modell, Betriebssystem, Seriennummer, IMEI, letzte vier Ziffern der Telefonnummer, verwaltete Apps], nicht aber Anruf- und Browserverlauf, E-Mails, SMS, Kontakte, Kalender, Kennwörter, Fotos, private Dokumente und den Standort. Den Standort eines Firmengeräts ruft [IT-Stelle] nur bei Verlust ab. [Eine Leistungs- oder Verhaltenskontrolle findet nicht statt.] Näheres: [Datenschutzinformation, Betriebsvereinbarung].

§ 8 Verlust, Diebstahl, Verdacht

Verlust, Diebstahl oder den Verdacht einer Manipulation melden Sie sofort an [IT-Stelle, Telefon, auch außerhalb der Arbeitszeit] (SYS.3.2.1.A7). [IT-Stelle] sperrt dann den Zugriff und löscht aus der Ferne: Firmengeräte vollständig, Privatgeräte nur die Firmendaten. Einen Diebstahl zeigen Sie zusätzlich bei der Polizei an. Lassen Sie Geräte nicht unbeaufsichtigt, etwa sichtbar im Auto (Aufbewahrung, SYS.3.2.1.A10).

§ 9 Rückgabe und Austritt

Firmengeräte geben Sie samt Zubehör spätestens am [letzten Arbeitstag] an [Stelle] zurück; private Daten sichern Sie vorher, danach wird das Gerät auf Werkseinstellungen zurückgesetzt. [Regelung zur Rufnummer]. Auf Privatgeräten entfernt [IT-Stelle] Firmendaten und Verwaltung; private Daten bleiben erhalten. Rückgabe und Löschung werden dokumentiert (SYS.3.2.2.A6, A22; NIS2: Anhang Nr. 12.5 DVO (EU) 2024/2690).

§ 10 Ausnahmen, Verstöße, Überprüfung

Ausnahmen genehmigt [Name, Funktion] schriftlich und befristet. Bei Verstößen kann [IT-Stelle] den Zugriff des Geräts auf Firmendaten sperren; [weitere Folgen, abgestimmt mit HR und Betriebsrat]. [Stelle] prüft Richtlinie und Einstellungen mindestens [jährlich] und vor neuen Betriebssystemversionen (SYS.3.2.2.A20). Gültig ab [Datum], freigegeben durch [Name, Funktion].

Anlage 1: Freigegebene Apps und Ablageorte (Beispielzeile in eckigen Klammern)

APP ODER DIENST	ZWECK	FIRMENGERÄT	PRIVATGERÄT
[z. B. Outlook]	[E-Mail, Kalender]	[ja]	[ja, mit App-Schutz]
_____	_____	_____	_____
_____	_____	_____	_____

Kenntnisnahme je Person und Gerät (ersetzt keine Betriebsvereinbarung und keine Zustimmung nach § 10 AVRAG)

ANGABE	EINTRAG
Name, Abteilung	_____
Firmengerät mit Inventarnummer oder Privatgerät mit Modell	_____
Richtlinie erhalten und gelesen: Datum, Unterschrift	_____
Für [Unternehmen]: Name, Datum, Unterschrift	_____

09 —

Checkliste: die Richtlinie einführen

Zehn Schritte von der Bestandsaufnahme bis zur regelmäßigen Überprüfung.

- ☐ Bestand erheben, welche Geräte heute auf E-Mail, Chats und Dateien zugreifen (NIST 5.1.2); Variante A oder B und private Nutzung von Firmengeräten entscheiden (SYS.3.2.2.A1).
- ☐ Zugelassene Geräte und Mindestversionen festlegen, Update-Zeitraum bei der Beschaffung prüfen (SYS.3.2.2.A2, SYS.3.2.1.A5).
- ☐ Lizenzen prüfen: Microsoft Intune, Microsoft Entra ID P1 oder P2.
- ☐ HR und Betriebsrat einbinden, Betriebsvereinbarung oder Zustimmung klären (§§ 96, 96a ArbVG, § 10 AVRAG).
- ☐ Datenschutzinformation erstellen (Art. 13 DSGVO) und den Datenschutztext im Unternehmensportal anpassen.
- ☐ App-Schutzrichtlinien (Stufe 2) einrichten, bedingten Zugriff erst im Modus „Nur Bericht“ prüfen, dann einschalten.
- ☐ Mit einer kleinen Pilotgruppe beginnen, dann für alle einführen (NIST 5.3.6).
- ☐ Mitarbeitende schulen: Phishing, Updates, Apps aus vertrauenswürdigen Quellen, welche Daten erhoben werden (NIST 4.3.10).
- ☐ Meldeweg für Verluste einrichten, Löschaktionen an einem Testgerät üben, Austrittsprozess ergänzen.
- ☐ Richtlinie und Einstellungen [jährlich] und vor neuen Betriebssystemversionen prüfen (SYS.3.2.2.A20).

Checkliste und Mustertext sind Empfehlungen von TOMORIS. Gesetzlich vorgegeben sind die genannten Pflichten aus DSGVO, ArbVG und AVRAG, für NIS2-Einrichtungen zusätzlich aus § 32 Abs. 4 lit. i NISG 2026, § 2 NISV 2026 und Anhang Nr. 12.5 DVO (EU) 2024/2690.

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

KOSTENLOS PRÜFEN

NIS2-Betroffenheitscheck

tomoris.com/tools/nis2-check

UMSETZUNG BESPRECHEN

Kontakt aufnehmen

tomoris.com/contact

contact@tomoris.com

10

Quellen

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

- BSI IT-Grundschutz-Kompodium, Edition 2023 (Gesamt-PDF)**
Kapitel Aufbau der Bausteine und Modalverben; gelesen am 25.10.2026
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...
- BSI IT-Grundschutz, Edition 2023: SYS.3.2.1 Allgemeine Smartphones und Tablets**
1.3, 2.9, A1 bis A8, A10, A11, A16, A18, A32; gelesen am 25.10.2026
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...
- BSI IT-Grundschutz, Edition 2023: SYS.3.2.2 Mobile Device Management**
1.3, 2.4, A1, A2, A4, A6, A17, A20, A22; gelesen am 25.10.2026
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...
- NIST SP 800-124 Rev. 2: Security of Mobile Devices in the Enterprise**
3.1.2, 3.1.11, 3.1.13, 4.2.2, 4.3.3, 4.3.6, 4.3.10 bis 4.3.12, 5.1.2, 5.1.3, 5.3.4.2, 5.3.6, 5.5
doi.org/10.6028/NIST.SP.800-124r2
- Microsoft Learn: Übersicht über App-Schutzrichtlinien**
Vorteile, Geräte ohne Registrierung, Anforderungen, Zurücksetzen
learn.microsoft.com/de-de/intune/app-management/protection/over...
- Microsoft Learn: Datenschutzframework für App-Schutzrichtlinien**
Stufe 1 und 2, bedingter Start; gelesen am 25.10.2026
learn.microsoft.com/de-de/intune/app-management/protection/data...
- Microsoft Learn: Welche Informationen erhält meine Organisation?**
nie, immer und möglicherweise sichtbar; Stand 20.8.2026
learn.microsoft.com/de-de/intune/user-help/enrollment/data-visi...
- Microsoft Learn: Apple-Benutzerregistrierung in Intune**
Methoden, Einstellungen, Einschränkungen; Stand 20.8.2026
learn.microsoft.com/de-de/intune/device-enrollment/apple/user-e...
- Microsoft Learn: MAM und persönliche Arbeitsprofile (Android)**
Datenschutz, Szenarien, Zusammenfassung; Stand 19.8.2026
learn.microsoft.com/de-de/intune/app-management/protection/mam-...
- Microsoft Learn: App-basierter bedingter Zugriff mit Intune**
Lizenzen, Rollen, Funktionsweise; Stand 20.8.2026
learn.microsoft.com/de-de/intune/device-security/conditional-ac...
- Microsoft Learn: Migrieren einer genehmigten Client-App zur App-Schutzrichtlinie**
Schreibschutz ab 30.6.2026, Richtlinie für mobile Geräte; Stand 1.6.2026
learn.microsoft.com/de-de/entra/identity/conditional-access/mig...
- Microsoft Learn: Geräteaktion Zurückziehen**
Plattformen, Benutzererfahrung; Stand 20.8.2026
learn.microsoft.com/de-de/intune/device-management/actions/reti...
- ArbVG, tagesaktuelle Fassung im RIS**
§ 96 Abs. 1 Z 3, § 96a Abs. 1 Z 1 und Abs. 2; gelesen am 25.10.2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...
- AVRAG, § 10 Kontrollmaßnahmen, RIS**
§ 10 Abs. 1; gelesen am 25.10.2026
www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetze...
- Verordnung (EU) 2016/679 (DSGVO), EUR-Lex**
Art. 5 Abs. 1 lit. c, Art. 13 Abs. 1 und 2, Art. 33 Abs. 1 und 5
eur-lex.europa.eu/eli/reg/2016/679/oj/deu
- Durchführungsverordnung (EU) 2024/2690, EUR-Lex**
Anhang Nr. 12 und 12.5; anwendbar nach § 2 NISV 2026
eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/deu
- NISG 2026, § 32 Risikomanagementmaßnahmen, RIS**
§ 32 Abs. 4 lit. i, gültig ab 1.10.2026; gelesen am 25.10.2026
www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetze...
- NISV 2026, BGBl. II Nr. 290/2026, RIS**
§ 2, kundgemacht am 1.10.2026
www.ris.bka.gv.at/eli/bgbII/2026/290