

Die 35-Punkte DSGVO-Checkliste für Dienst-Smartphones

Verbindliche Prüfkriterien für ambulante Pflegedienste, Kanzleien, Praxen & KMU

■ ■ ■ Dringendes Haftungs-Risiko (Art. 33 DSGVO & § 203 StGB):

Sobald Mitarbeiter Standard-WhatsApp oder ungesicherte Apps auf Dienst-Smartphones nutzen, synchronisiert die App das gesamte betriebliche Adressbuch auf US-Server. Befinden sich darin Patientendaten, Klienten oder Mandantenkontakte, liegt ein meldepflichtiger Datenschutzverstoß vor, der Bußgelder bis zu 20.000 € oder strafrechtliche Konsequenzen für Geschäftsführer nach sich ziehen kann.

KATEGORIE 1: DATENTRENNUNG & CONTAINERISIERUNG (Art. 32 DSGVO)

- [] **Strikte Trennung von Privat- und Geschäftsdaten:** Automatisches Android Enterprise Arbeitsprofil oder Apple MDM Managed Open-In aktiv.
- [] **WhatsApp Adressbuch-Abschottung:** Verhinderung des Zugriffs von Consumer-Messengern auf Klienten- & Patientenstammdaten.
- [] **Zwischenablagen-Schutz (Copy/Paste):** Kopieren von Texten aus geschäftlichen Apps in private Apps ist zentral unterbunden.
- [] **Getrennter App-Store:** Mitarbeiter können im geschäftlichen Bereich nur vom Admin freigegebene Apps installieren.
- [] **Dokumenten-Verschlüsselung:** Dateien in geschäftlichen Apps werden mit Hardware-gestützter Verschlüsselung (AES-256) abgelegt.

KATEGORIE 2: NOTFALL- & DIEBSTAHLSCHUTZ (Art. 33/34 DSGVO)

- [] **3-Sekunden Remote Wipe (Fernlöschung):** Bei Geräteverlust oder Diebstahl können alle Geschäftsdaten sofort aus der Ferne gelöscht werden.
- [] **Selektiver Wipe bei Mitarbeiter-Austritt:** Beim Ausscheiden von Personal werden nur Geschäftsdaten gelöscht; private Daten bleiben unangetastet.
- [] **Automatische Bildschirmsperre:** Erzwungene Sperre nach maximal 2 Minuten Inaktivität.
- [] **Sichere PIN-Mindestanforderungen:** Mindestens 6 Ziffern oder biometrische Entsperrung; simple PINs (0000, 1234) sind blockiert.
- [] **Selbstzerstörung bei Brute-Force:** Automatisches Zurücksetzen der Geschäftsdaten nach 5 fehlerhaften Entsperrversuchen.

KATEGORIE 3: CLOUD-SOVERÄNITÄT & ABFLUSSVERHINDERUNG (§ 203 StGB)

- [] **Verbot unverschlüsselter US-Cloud-Backups:** Automatische Backups von WhatsApp & Fotos in ungesicherte Google Drive / iCloud Konten sind deaktiviert.
- [] **DSGVO-konforme Serverstandorte:** MDM-Verwaltung und Cloud-Backups laufen ausschließlich in zertifizierten deutschen Rechenzentren (Nürnberg/Falkenstein).
- [] **USB- & Datenübertragungs-Sperre:** Übertragung sensibler Daten via USB-Kabel an private PCs ist systemweit gesperrt.
- [] **Screenshot-Prävention:** Erstellung von Bildschirmfotos in vertraulichen Patienten-/Mandanten-Apps ist deaktiviert.

KATEGORIE 4: COMPLIANCE, UPDATES & ORGANISATION

- [] **Automatische Sicherheits-Patches:** Sicherheitsupdates von iOS & Android werden binnen 14 Tagen zentral forciert.
- [] **Gültiger AV-Vertrag nach Art. 28 DSGVO:** Ein schriftlicher Auftragsverarbeitungsvertrag mit dem MDM-Provider liegt vor.
- [] **Dienstvereinbarung zur Handynutzung:** Alle Mitarbeiter haben eine schriftliche Nutzungsvereinbarung unterzeichnet.

- [] **Verzeichnis von Verarbeitungstätigkeiten (VVT):** Der Einsatz mobiler Dienstgeräte ist im betrieblichen VVT dokumentiert.
- [] **Regelmäßiges Audit:** Mindestens einmal jährlich wird der Flottenstatus auf Jailbreaks / Rooting geprüft.

Muster-Dienstvereinbarung zur Diensthandy-Nutzung

Kostenlose Rechtsvorlage für Arbeitgeber zur verbindlichen Regelung der Smartphone-Nutzung

Dienstvereinbarung über die Überlassung und Nutzung betrieblicher Mobilgeräte

Zwischen:

Arbeitgeber: _____

Mitarbeiter/in: _____

§ 1 Vertragsgegenstand & Eigentum

Dem/der Mitarbeiter/in wird für die Dauer des Arbeitsverhältnisses ein Dienst-Smartphone (Modell: _____, IMEI: _____) zur Ausübung der dienstlichen Aufgaben überlassen. Das Gerät bleibt ausschließliches Eigentum des Arbeitgebers.

§ 2 Mobile Device Management (MDM) & Datenschutz

1. Das Gerät wird über das zentrale Verwaltungssystem **SafeMDM** betreut. Hierbei wird ein getrennter, verschlüsselter geschäftlicher Arbeitsbereich (Container) eingerichtet.
2. Private Apps (inklusive Standard-WhatsApp, Instagram, Social Media) haben technisch bedingt keinerlei Zugriff auf geschäftliche Kontakte, Dienstpläne oder Kundendaten.
3. Die Überwachung von privaten Telefonaten, privaten Chatnachrichten oder Standortdaten im privaten Bereich findet ausdrücklich **nicht** statt.

§ 3 Sorgfaltspflichten & Gerätesicherheit

1. Das Mobilgerät ist stets durch eine persönliche PIN (mind. 6 Stellen) oder biometrische Merkmale (Fingerabdruck/FaceID) gegen unbefugten Zugriff zu schützen.
2. Ein Verlust oder Diebstahl des Geräts ist der Geschäftsleitung **unverzüglich (binnen 2 Stunden)** zu melden, damit eine sofortige Fernsperrung (Remote Wipe) zum Schutz personenbezogener Daten eingeleitet werden kann.
3. Das Einspielen von Sicherheits-Updates des Betriebssystems darf nicht unbegründet verzögert werden.

§ 4 Beendigung des Arbeitsverhältnisses

Mit Beendigung des Arbeitsverhältnisses ist das Dienstgerät nebst Zubehör im ordnungsgemäßen Zustand an den Arbeitgeber zurückzugeben. Bei Ausscheiden wird der geschäftliche Bereich per Fernlöschung rückstandsfrei entfernt.

Ort, Datum: _____

Unterschrift Arbeitgeber

Unterschrift Mitarbeiter/in

Brauchen Sie Unterstützung bei der rechtssicheren Umsetzung?

SafeMDM schützt Ihre Diensthandy-Flotte ab 2,90 € / Gerät / Monat – 100% DSGVO-konform, in 10 Minuten eingerichtet.

Buchen Sie jetzt Ihren kostenlosen 15-Minuten Quick-Audit: <https://meet.nevyron.com/turan/15min>