4 · GERÄTE FÜR DIE WEITERNUTZUNG FREIGEBEN

Gelöscht und wieder nutzbar

Firmengeräte sind oft fest an Ihre Organisation gebunden. Auch nach der Löschung meldet sich ein solches Gerät beim nächsten Start wieder bei Ihrer Verwaltung an oder bleibt gesperrt. Damit es weiterverwendet oder verkauft werden kann, muss diese Bindung **vor** der Löschung gelöst werden.

PLATTFORM	BINDUNG	FREIGABE IN DIESER REIHENFOLGE
Apple iPhone, iPad, Mac	Apple Business Manager (ABM, früher DEP), MDM-Profil, Aktivierungssperre („Wo ist?“)	Aktivierungssperre per MDM aufheben → Gerät im ABM freigeben → aus MDM entfernen. Die Freigabe ist endgültig.
Samsung Galaxy-Smartphones, Tablets	Knox Mobile Enrollment (KME), Knox Manage / MDM, Google-Konto (FRP)	Gerät aus MDM abmelden → Profil in KME löschen („Delete device“) → Google-Konto entfernen.
Android allgemein Smartphones, Tablets	Zero-Touch-Registrierung, Google-Konto (Schutz vor Zurücksetzen, FRP)	Gerät aus Zero-Touch entfernen → Google-Konto abmelden → Gerät aus MDM entfernen.
Windows Notebooks, PCs	Windows Autopilot, Intune / MDM, BIOS-Passwort, Diebstahlschutz-Software	Gerät aus Autopilot und Intune löschen → BIOS-Passwort entfernen → Diebstahlschutz deaktivieren.

Wer macht was?

Die Freigabe kann technisch nur der **Eigentümer** im eigenen Verwaltungsportal auslösen (Apple Business Manager, Knox-Portal, Intune). Wir nehmen Ihnen die Arbeit dabei ab:

- Abgleich Ihrer Geräteliste: Welche Seriennummern sind noch gebunden?
- Schritt-für-Schritt-Anleitung für Ihre IT (Anlage 6) oder Freigabe gemeinsam mit Ihrer IT, auf Wunsch über ein eigenes, eingeschränktes Konto in Ihrem Portal.
- Prüfung jedes Geräts beim Eingang und nach der Löschung.

Wenn ein Gerät noch gesperrt ist

Prüfung bei Eingang
Gerät zeigt Verwaltungs- oder Aktivierungssperre

↓

Sperrliste an Sie
mit Seriennummer und Art der Sperre

↓

Freigabe durch Ihre IT
wir bestätigen und löschen erneut

↓

Daten werden immer gelöscht
auch wenn ein Gerät gesperrt bleibt: Es geht dann zurück an Sie oder in die Entsorgung

ANLAGE 6

Checkliste: Geräte vor der Abholung vorbereiten

Für Ihre IT-Abteilung. Je vollständiger diese Schritte erledigt sind, desto mehr Geräte können nach der Löschung weiterverwendet werden. Wir unterstützen gern bei jedem Punkt.

Für alle Geräte

- [ ] Geräteliste mit Seriennummern erstellen (Excel genügt)
- [ ] Daten, die Sie behalten müssen, vorher sichern
- [ ] Geräte, die zur Reparatur gehen, nicht freigeben

Apple (iPhone, iPad, Mac)

- [ ] Aktivierungssperre über das MDM aufheben (Umgehungscode) oder „Wo ist?“ durch den Nutzer abschalten
- [ ] Bei Intel-Macs: Firmware-Passwort ausschalten
- [ ] Geräte im Apple Business Manager freigeben (endgültig)
- [ ] Erst danach: Geräte aus dem MDM entfernen

Samsung und Android

- [ ] Geräte aus dem MDM / Knox Manage abmelden
- [ ] Im Knox-Portal unter Knox Mobile Enrollment: Gerät löschen
- [ ] Bei Zero-Touch: Gerät aus der Zero-Touch-Konfiguration entfernen
- [ ] Google-Konto auf dem Gerät abmelden (Schutz vor Zurücksetzen)

Windows-Notebooks und PCs

- [ ] Gerät aus Windows Autopilot löschen (Hardware-Hash)
- [ ] Gerät in Intune / MDM löschen
- [ ] BIOS- bzw. UEFI-Passwort entfernen
- [ ] Diebstahlschutz-Software (z. B. Absolute) deaktivieren

Reihenfolge ist wichtig: Bei Apple-Geräten erst die Aktivierungssperre aufheben, dann im Apple Business Manager freigeben, zuletzt aus dem MDM entfernen. Wird das MDM zuerst entfernt, fehlt der Umgehungscode für die Aktivierungssperre.