

MDM-Checkliste

Konfiguration & Jugendschutz.

Alle wichtigen Einstellungen für die Einrichtung und den Betrieb von Smartphones, Tablets und Laptops, ergänzt um Einstellungen für Kinder und Jugendliche.

9**Prüfbereiche**

von Grundkonfiguration bis
Notfall

71**Prüfpunkte**

zum Abhaken und
Dokumentieren

25**Kinder & Jugendliche**

zusätzliche Schutzeinstellungen

Kunde / Einrichtung

MDM-System

 Bearbeiter/in

 Datum

 Geräte (Typ / Anzahl)

So nutzen Sie die Checkliste: Haken setzen, wenn der Punkt konfiguriert und getestet ist. Nicht relevante Punkte mit „-“ markieren. Der Funktionsumfang hängt von Plattform (Apple, Android, Windows) und MDM-System ab.

1 Allgemeine MDM-Grundkonfiguration

8 Punkte

- ☐ Geräte-Registrierung automatisiert (Apple DEP, Samsung Knox, Android Zero-Touch, Windows Autopilot)
- ☐ Hintergrundbild hinterlegt (max. 3 MB)
- ☐ Sperrbildschirm hinterlegt (max. 3 MB)
- ☐ Begrüßungstext festgelegt
- ☐ Gerätezuweisung zu Benutzerkonten oder Gerätegruppen
- ☐ Richtlinien nach Gerätetyp (Smartphone, Tablet, Laptop)
- ☐ Standardprofile definiert (Basisrichtlinien für alle Nutzer)
- ☐ Standortverfolgung aktiviert (nur falls datenschutzkonform und notwendig)

2 Sicherheitsrichtlinien

8 Punkte

- ☐ Passwort-/PIN-Richtlinie (Länge, Komplexität, Ablaufzeit)
- ☐ Geräteverschlüsselung erzwingen
- ☐ Sperrbildschirm-Zeitlimit festlegen
- ☐ Jailbreak-/Root-Erkennung aktivieren
- ☐ Automatische Gerätesperre bei Inaktivität
- ☐ Remote-Wipe (Gerät löschen bei Verlust oder Diebstahl)
- ☐ Remote-Lock (Gerät aus der Ferne sperren)
- ☐ Anti-Phishing und App-Integritätsprüfung (sofern unterstützt)

3 App-Management

7 Punkte

- ☐ Genehmigte App-Whitelists und Blacklists (z. B. Tinder, Bumble, Reddit, Facebook, TikTok und Erwachseneninhalte)
- ☐ Automatische Installation von Pflicht-Apps
- ☐ Installation unbekannter Apps verhindern
- ☐ App-Updates erzwingen oder zentral steuern
- ☐ Containerisierung geschäftlicher Apps (Work Profile, Managed Apps)
- ☐ Trennung von privaten und geschäftlichen Daten (BYOD)
- ☐ Jugendschutzfilter eingerichtet (Relution)

4 Netzwerk- & Verbindungsrichtlinien

6 Punkte

- ☐ WLAN-Profil mit sicheren SSIDs und Zertifikaten verteilen
- ☐ VPN-Profil automatisch konfigurieren
- ☐ Nutzung öffentlicher WLANs einschränken oder Warnhinweis anzeigen
- ☐ Mobile Hotspot-Funktion deaktivieren (optional)
- ☐ Proxy- und Firewall-Regeln für mobilen Datenverkehr
- ☐ Nutzungszeiten für offenes Internet festlegen (z. B. nur 16:00 bis 18:00 Uhr)

5 Geräteverwaltung & Monitoring

5 Punkte

- ☐ Regelmäßige Compliance-Prüfung (z. B. Jailbreak, OS-Version, Verschlüsselung)
- ☐ Geräteinventar (Modell, Seriennummer, OS-Version)
- ☐ Automatische Warnmeldungen bei Richtlinienverstößen
- ☐ Reporting-Dashboard für Sicherheitsstatus und Nutzung
- ☐ Automatische Richtlinienaktualisierung bei Änderungen

6 Benutzer- & Datenschutz

4 Punkte

- ☐ DSGVO-konforme Datenschutzeinstellungen
- ☐ Klare Trennung von Unternehmens- und privaten Daten (insbesondere bei BYOD)
- ☐ Transparente Information der Nutzer über den Umfang des MDM
- ☐ Zugriff nur auf dienstlich relevante Daten und Funktionen

7 Update- & Wartungsmanagement

4 Punkte

- ☐ Automatische Betriebssystem-Updates aktivieren oder zeitlich steuern
- ☐ Patch-Management (kritische Sicherheitsupdates priorisieren)
- ☐ Rollout-Fenster für Updates definieren
- ☐ Testgruppe für neue OS-Versionen einrichten

8 Notfallmaßnahmen

4 Punkte

- ☐ Remote-Wipe und Remote-Lock getestet
- ☐ Backup- und Wiederherstellungsstrategie vorhanden
- ☐ Kontaktpunkte für Support und Helpdesk definiert
- ☐ Notfallrichtlinie bei Geräteverlust oder Sicherheitsvorfall

9**Kinder & Jugendliche**

Zusätzliche Schutzeinstellungen für Schule, Hort und Elternhaus finden Sie auf den nächsten beiden Seiten.

Kinder & Jugendliche Schutzeinstellungen.

Für Geräte in Schule, Hort und Elternhaus. Die Vorgaben richten sich nach Altersgruppe und lassen sich je Plattform und MDM-System unterschiedlich umsetzen.

9.1 Geräteeinrichtung & Schutz

4 Punkte

- ☐ Geräte im betreuten Modus (Supervised) einrichten, z. B. über Apple School Manager oder Android Enterprise
- ☐ Konfigurationsprofil gegen Entfernen schützen, Zurücksetzen auf Werkseinstellungen sperren
- ☐ Altersgruppen definieren und Geräten zuweisen (z. B. Grundschule, Sek I, Sek II)
- ☐ Änderungen an Konto, Passcode und Einstellungen durch das Kind sperren

9.2 Inhalte & Altersfreigaben

4 Punkte

- ☐ Altersfreigaben für Apps, Filme und Serien je Altersgruppe begrenzen (USK, FSK, PEGI)
- ☐ Explizite Inhalte in Musik, Podcasts und Nachrichten sperren
- ☐ Jugendschutzfilter je Altersgruppe zuweisen (siehe Bereich 3)
- ☐ Ungeeignete Apps blockieren: Dating, Erwachsenen- und Glücksspielangebote sowie Social Media unter der Altersgrenze

9.3 Web & Internet

4 Punkte

- ☐ Web-Inhaltsfilter: Kinder nur mit freigegebenen Seiten (Whitelist), Jugendliche mit Kategorienfilter
- ☐ SafeSearch erzwingen, YouTube im eingeschränkten Modus
- ☐ Umgehung verhindern: VPN- und Proxy-Erstellung sowie Änderung der DNS-Einstellungen sperren
- ☐ Zeitfenster für offenes Internet festlegen (siehe Bereich 4, z. B. 16:00 bis 18:00 Uhr)

9.4 Apps & Käufe

3 Punkte

- ☐ Installation nur aus freigegebenem App-Katalog (Self-Service-Store)
- ☐ App-Käufe und In-App-Käufe sperren, Passwortabfrage für jeden Kauf
- ☐ Installieren und Löschen von Apps durch das Kind einschränken

9.5 Kommunikation, Spiele & Medien

4 Punkte

- ☐ Nachrichten, FaceTime und Messenger nur mit freigegebenen Kontakten oder deaktiviert
- ☐ Game Center: Multiplayer und Freundesanfragen sperren
- ☐ AirDrop und Dateifreigabe per Bluetooth deaktivieren
- ☐ Screenshots, Bildschirmaufnahme, Kamera und Mikrofon nach Einsatzzweck begrenzen (Persönlichkeitsrechte, Mobbing)

9.6 Nutzungszeiten & Standort

2 Punkte

- ☐ Nutzungs- und Ruhezeiten festlegen (z. B. Gerätesperre nachts, Schulzeiten)
- ☐ Gerät nur bei Verlust oder Diebstahl orten, Umfang und Zweck transparent erklärt

9.7 Eltern, Schule & Recht

4 Punkte

- ☐ Information und Einwilligung der Erziehungsberechtigten (Nutzungsvereinbarung) liegt vor
- ☐ Kinder und Jugendliche altersgerecht über Umfang und Zweck der Verwaltung informiert
- ☐ Ansprechperson und Meldeweg bei Mobbing oder ungeeigneten Inhalten benannt
- ☐ Filter, Altersgrenzen und App-Listen regelmäßig überprüft (z. B. halbjährlich)

Empfehlung nach Altersgruppe

Richtwerte zum Anpassen an Ihre Einrichtung.

BEREICH	KINDER (BIS 12 JAHRE)	JUGENDLICHE (13 BIS 17 JAHRE)
Apps	Nur freigegebene Apps	Altersfreigabe begrenzt, Blacklist
Internet	Whitelist, SafeSearch	Kategorienfilter, SafeSearch
Käufe	Gesperrt	Gesperrt oder nur mit Freigabe
Kommunikation	Aus oder nur Familie und Klasse	Freigegebene Kontakte und Messenger
Nutzungszeit	Feste, kurze Zeitfenster	Zeitfenster plus Ruhezeit nachts

Geprüft von

Datum

Unterschrift

Die Checkliste ersetzt keine Rechtsberatung. Datenschutz- und Jugendschutzvorgaben bitte mit Ihrer Datenschutzbeauftragten oder Ihrem Rechtsbeistand abstimmen.