

AVV Anlage 2r -- Managed Service MDM

Produktspezifische Anlage zum Rahmen-Auftragsverarbeitungsvertrag

1. Bezeichnung des Services

Managed Service MDM (Mobile Device Management)

2. Gegenstand der Verarbeitung

Zentrale Verwaltung, Überwachung und Aktualisierung der mobilen Endgeräte des Auftraggebers (iOS/iPadOS und Android) über die vom Auftragnehmer betriebene Mobile-Device-Management-Plattform NinjaOne.

In der Leistungsstufe Platin sowie bei gebuchter Zusatzleistung in den Stufen Silber und Gold erfolgt ergänzend Endpoint Security durch CrowdStrike.

Enrollment und Onboarding der Geräte werden zwar gesondert als Projektleistung abgerechnet, finden aber auf derselben Plattform statt; die dabei erfolgende Verarbeitung ist von dieser Anlage mit erfasst.

3. Zweck der Verarbeitung

Sicherstellung eines aktuellen und richtlinienkonformen Zustands der mobilen Endgeräte des Auftraggebers: Steuerung der Betriebssystem-Updates, Überwachung von Gerätezustand und Konformität, Verwaltung der Sicherheitsrichtlinien, monatliche Berichterstattung sowie Fernsperrung und Fernlöschung auf Anforderung des Auftraggebers.

In den Leistungsstufen Gold und Platin zusätzlich: Ermittlung des Gerätestandorts (Location Tracking) und Durchsetzung von Nutzungseinschränkungen (Restriction Management) nach Vorgabe des Auftraggebers.

Bei enthaltener oder gebuchter Endpoint Security zusätzlich: Erkennung und Abwehr von Bedrohungen auf den verwalteten Geräten.

4. Kategorien personenbezogener Daten

- Benutzernamen, Benutzer-IDs und dienstliche E-Mail-Adressen der zugeordneten Nutzer
- Gerätekennungen (Geräteiname, Seriennummer, IMEI, UDID, Agent-ID)
- Mobilfunknummer und Mobilfunkanbieter, soweit vom Betriebssystem an die Plattform übermittelt
- IP-Adressen (intern und extern)
- Betriebssystem-, Modell- und Hardware-Informationen
- Installierte Anwendungen und Versionen; bei Verwaltung nach dem Modell getrennter Arbeitsprofile beschränkt auf den verwalteten Bereich
- Update-, Verschlüsselungs- und Konformitätsstatus, Speicherbelegung, Batteriezustand
- Zuweisungs- und Ereignisprotokolle der Verwaltungsplattform (Richtlinienzuweisung, Enrollment, Sperrung, Löschung)
- **Standortdaten** (nur Leistungsstufen Gold und Platin bei aktiviertem Location Tracking: zuletzt ermittelte Geokoordinaten und Zeitstempel)

- Sicherheitsrelevante Ereignisdaten (nur bei enthaltener oder gebuchter Endpoint Security: Bedrohungsindikatoren, aufgerufene und blockierte Adressen, Netzwerk- und Anwendungsereignisse, Bewertung des Gerätesicherheitszustands)

Besondere Kategorien (Art. 9 DSGVO): Nein -- es werden keine besonderen Kategorien gezielt verarbeitet. Der Auftragnehmer weist darauf hin, dass Standortdaten mittelbare Rückschlüsse auf besondere Kategorien zulassen können; die Bewertung obliegt dem Auftraggeber als Verantwortlichem.

5. Kategorien betroffener Personen

- Beschäftigte des Auftraggebers
- Externe Dienstleister mit zugewiesenen mobilen Endgeräten

6. Art der Verarbeitung

Erheben, Speichern, Auslesen, Abfragen, Verwenden, Verändern (Zuweisung und Durchsetzung von Richtlinien, Verteilung von Betriebssystem-Updates, Aktivierung von Einschränkungen), Übermitteln (an die in Abschnitt 9 genannten Unterauftragsverarbeiter), Einschränken (Fernsperrung), Löschen (Fernlöschung, Offboarding)

7. Ort der Verarbeitung

Standort	Anbieter	Zweck
EU (eu.ninjarmm.com)	NinjaOne LLC	MDM-Plattform: Enrollment, Richtlinienverwaltung, Update-Steuerung, Monitoring, Reporting
Irland / USA	Apple Distribution International Ltd.	Apple Push Notification service und Apple Business Manager -- Zustellung der Verwaltungsbefehle an iOS-/iPadOS-Geräte
Irland / USA	Google Ireland Limited	Android Enterprise und Managed Google Play -- Zustellung der Verwaltungsbefehle an Android-Geräte und Bereitstellung verwalteter Anwendungen
USA	CrowdStrike Inc. (Stufe Platin; in Silber und Gold nur bei Buchung)	Bedrohungserkennung -- geschützt durch EU-US Data Privacy Framework + SCCs
Deutschland (Hannover)	EXT IT GmbH	Administration, Konfiguration, Auswertung, Reporting

8. Aufbewahrungsdauer / Löschfristen

Datenkategorie	Aufbewahrungsdauer	Löschverfahren
Monitoring- und Ereignisdaten der Plattform	90 Tage	Automatische Rotation in der Verwaltungsplattform
Standortdaten (Gold/Platin)	30 Tage	Automatische Rotation in der Verwaltungsplattform
Monatliche Reports	1 Jahr	Löschung nach Ablauf
Geräteinventar und Richtlinienzuweisung	Dauer der Beauftragung	Löschung bei Vertragsende
Protokolle zu Fernsperrung und Fernlöschung	3 Jahre	Löschung nach Ablauf; Aufbewahrung zum Nachweis der Weisungslage

9. Eingesetzte Unterauftragsverarbeiter

Für diesen Service werden die folgenden **produktspezifischen** Unterauftragsverarbeiter eingesetzt:

Nr.	Firma	Sitz	Verarbeitungszweck	Drittlandtransfer	Garantien
Z1	NinjaOne LLC	Austin, Texas, USA (EMEA-Büro: Berlin)	MDM-Plattform (Enrollment, Richtlinienverwaltung, Update-Steuerung, Monitoring, Reporting)	EU-Instanz (eu.ninjarmm.com), Daten verbleiben im EEA	Siehe Anlage 3
Z16	Apple Distribution International Ltd.	Cork, Irland (EU); Muttergesellschaft Apple Inc., USA	Apple Push Notification service und Apple Business Manager -- Zustellung der Verwaltungsbefehle an iOS-/iPadOS-Geräte, Geräte- und Zuweisungsverwaltung	USA	Siehe Anlage 3
Z17	Google Ireland Limited	Dublin, Irland (EU); Muttergesellschaft Google LLC, USA	Android Enterprise und Managed Google Play -- Zustellung der Verwaltungsbefehle an Android-Geräte, Bereitstellung verwalteter Anwendungen	USA	Siehe Anlage 3
Z2	CrowdStrike Inc. (Stufe Platin; in den Stufen Silber und Gold nur bei Buchung)	Austin, Texas, USA	Bedrohungserkennung auf mobilen Endgeräten	USA	Siehe Anlage 3

Die vollständigen DPA-Details, Zertifizierungen und Drittlandgarantien zu den oben genannten Unterauftragsverarbeitern sind zentral in **Anlage 3** geführt.

Ergänzend kommen die in Abschnitt 3 der Anlage 3 gelisteten produktübergreifenden Unterauftragsverarbeiter zum Einsatz.

10. Besondere Hinweise

- **Location Tracking (Gold/Platin) ist eine Verarbeitung von Beschäftigtendaten mit besonderem Eingriffsgewicht.** Der Auftraggeber ist Verantwortlicher und stellt vor Aktivierung die Rechtsgrundlage, die Wahrung der Beteiligungsrechte einer bestehenden Arbeitnehmervertretung (insbesondere § 87 Abs. 1 Nr. 6 BetrVG) und die Information der Betroffenen nach Art. 13 DSGVO sicher. Der Auftragnehmer aktiviert die Funktion ausschließlich nach schriftlicher Freigabe des Auftraggebers und dokumentiert den aktivierten Umfang. Eine dauerhafte Bewegungsaufzeichnung wird nicht eingerichtet; ermittelt wird der jeweils zuletzt gemeldete Standort.
- **Restriction Management** setzt Vorgaben des Auftraggebers technisch um. Der Auftragnehmer prüft die arbeits- und mitbestimmungsrechtliche Zulässigkeit der Vorgaben nicht inhaltlich; §5 des Rahmen-AVV (Weisungen und deren Prüfung) bleibt unberührt.
- **Fernlöschung** erfolgt ausschließlich auf ausdrückliche Anforderung eines vom Auftraggeber benannten Ansprechpartners. Bei getrennten Arbeitsprofilen (Android Enterprise Work Profile, iOS User Enrollment) beschränkt sie sich auf den verwalteten Bereich; bei vollständig verwalteten Unternehmensgeräten erfasst sie das gesamte Gerät einschließlich etwaiger privater Daten. Der Auftraggeber verantwortet die Zulässigkeit der Anweisung.
- **Privat mitgenutzte Geräte (BYOD):** Bei privat mitgenutzten Geräten setzt der Auftragnehmer das Modell der getrennten Arbeitsprofile ein. Der Zugriff des Auftragnehmers beschränkt sich dann auf den verwalteten Bereich; private Anwendungen, Inhalte und Standortdaten außerhalb

des verwalteten Bereichs werden nicht verarbeitet. Der Auftraggeber stellt eine wirksame Nutzungsvereinbarung mit den betroffenen Personen sicher.

- **Apple und Google** verarbeiten im Rahmen der Push-Zustellung Gerätekennungen und Push-Token. Eine Kenntnisnahme der übermittelten Verwaltungsbefehle durch Apple oder Google findet nicht statt; die Nutzdaten sind Ende-zu-Ende zwischen Verwaltungsplattform und Gerät verschlüsselt.
- **CrowdStrike** verarbeitet Daten unter dem EU-US Data Privacy Framework. Zusätzlich sind Standardvertragsklauseln (SCCs) vereinbart. In den Stufen Silber und Gold findet ohne Buchung keine Datenverarbeitung durch CrowdStrike statt.
- Der Auftragnehmer überwacht kein Nutzerverhalten und keine Bildschirminhalte. Inhalte der Kommunikation (Nachrichten, Telefonate, Browserverläufe) werden nicht verarbeitet.

Änderungshistorie

Version	Datum	Änderung	Verantwortlich
1.0	2026-09-02	Erstveröffentlichung	Geschäftsführung

Stand: 2026-09-02