

## AVV Anlage 2s -- Endpoint Security Mobile (CrowdStrike)

### Produktspezifische Anlage zum Rahmen-Auftragsverarbeitungsvertrag

---

#### 1. Bezeichnung des Services

##### **Endpoint Security Mobile (CrowdStrike)**

Diese Anlage gilt für den eigenständig gebuchten Service Endpoint Security Mobile -- auch dann, wenn der Auftraggeber die Geräte über ein eigenes Mobile Device Management verwaltet. Wird der Service als Zusatzleistung innerhalb des Services Managed Service MDM (Stufen Silber und Gold) gebucht oder ist er dort in der Leistungsstufe Platin enthalten, gilt die produktspezifische Anlage 2 des Managed Service MDM.

Die Anlage gilt nicht für den Service Endpoint Security (CrowdStrike MDR Complete) für Windows-Clients und Server; dafür besteht eine eigene Anlage.

---

#### 2. Gegenstand der Verarbeitung

Betrieb der CrowdStrike-Schutzanwendung auf den mobilen Endgeräten des Auftraggebers (iOS/iPadOS und Android); Betrieb des CrowdStrike-Mandanten, Pflege der Erkennungsrichtlinien sowie Erkennung von Bedrohungen auf Anwendungs-, Netzwerk- und Konfigurationsebene.

Eine prozessbasierte Bedrohungserkennung (Endpoint Detection and Response) und eine Managed Detection & Response mit 24/7-Analystenteam finden nicht statt; die Betriebssysteme mobiler Endgeräte lassen den dafür erforderlichen Systemzugriff nicht zu.

---

#### 3. Zweck der Verarbeitung

Erkennung und Abwehr von Bedrohungen auf den mobilen Endgeräten des Auftraggebers -- insbesondere Phishing- und Schadlinks, schadhafte Anwendungen, unsichere Netzwerkverbindungen und manipulierte Geräte -- sowie Benachrichtigung des Auftraggebers über sicherheitsrelevante Vorfälle.

---

#### 4. Kategorien personenbezogener Daten

- Benutzernamen, Benutzer-IDs und dienstliche E-Mail-Adressen der zugeordneten Nutzer
- Gerätekennungen (Gerätename, Seriennummer, CrowdStrike-Agent-ID)
- IP-Adressen (intern und extern)
- Betriebssystem-, Modell- und Konfigurationsinformationen, Verschlüsselungs- und Update-Status
- Installierte Anwendungen und Versionen; bei getrennten Arbeitsprofilen beschränkt auf den verwalteten Bereich
- **Aufgerufene und blockierte Adressen** (Domains und URLs), soweit für die Prüfung auf Phishing- und Schadlinks erforderlich
- Merkmale genutzter Netzwerkverbindungen (z.B. WLAN-Kennung, Zertifikatsauffälligkeiten)
- Bedrohungsindikatoren, Alarmmeldungen und vorfallsbezogene Analysedaten
- Bewertung des Gerätesicherheitszustands

**Besondere Kategorien (Art. 9 DSGVO):** Nein -- es werden keine besonderen Kategorien gezielt verarbeitet. Der Auftragnehmer weist darauf hin, dass aufgerufene Adressen 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, Analysieren, Einschränken (Blockieren einer Verbindung oder einer Adresse), Löschen (bei Offboarding)

## 7. Ort der Verarbeitung

| Standort               | Anbieter         | Zweck                                                                                   |
|------------------------|------------------|-----------------------------------------------------------------------------------------|
| USA                    | CrowdStrike Inc. | Bedrohungserkennung und -analyse -- geschützt durch EU-US Data Privacy Framework + SCCs |
| Deutschland (Hannover) | EXT IT GmbH      | Administration, Konfiguration, Bearbeitung und Weiterleitung von Meldungen              |

Verwaltet der Auftraggeber die Geräte über ein eigenes Mobile Device Management, ist dessen Anbieter **kein** Unterauftragsverarbeiter der EXT IT GmbH, sondern Auftragsverarbeiter des Auftraggebers.

## 8. Aufbewahrungsdauer / Löschfristen

| Datenkategorie                      | Aufbewahrungsdauer                                  | Löschverfahren                        |
|-------------------------------------|-----------------------------------------------------|---------------------------------------|
| Ereignis- und Telemetriedaten       | Gemäß gebuchter Retention der CrowdStrike-Plattform | Automatische Rotation bei CrowdStrike |
| Aufgerufene und blockierte Adressen | 30 Tage, sofern nicht Bestandteil eines Vorfalls    | Automatische Rotation bei CrowdStrike |
| Alarm- und Vorfallsdaten            | Dauer der Beauftragung                              | Löschung bei Vertragsende             |
| Geräteinventar im Mandanten         | Dauer der Beauftragung                              | Löschung bei Vertragsende             |

## 9. Eingesetzte Unterauftragsverarbeiter

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

| Nr. | Firma            | Sitz               | Verarbeitungszweck                                      | Drittlandtransfer | Garantien      |
|-----|------------------|--------------------|---------------------------------------------------------|-------------------|----------------|
| Z2  | CrowdStrike Inc. | Austin, Texas, USA | Bedrohungserkennung und -analyse 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

- **Die Prüfung aufgerufener Adressen ist eine Verarbeitung von Beschäftigtendaten mit besonderem Eingriffsgewicht.** Der Auftraggeber ist Verantwortlicher und stellt vor Inbetriebnahme 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.
- Die Auswertung dient ausschließlich der Erkennung und Abwehr von Bedrohungen. Eine Verwendung der Daten zur Verhaltens- oder Leistungskontrolle von Beschäftigten erfolgt nicht. Der Auftragnehmer erstellt keine Auswertungen des Surfverhaltens und stellt dem Auftraggeber keine solchen bereit.
- **Privat mitgenutzte Geräte (BYOD):** Bei getrennten Arbeitsprofilen wirkt die Schutzanwendung nur im verwalteten Bereich; private Anwendungen und der private Datenverkehr außerhalb des verwalteten Bereichs werden nicht verarbeitet. Der Auftraggeber stellt eine wirksame Nutzungsvereinbarung mit den betroffenen Personen sicher.
- Inhalte der Kommunikation (Nachrichten, Telefonate) und Bildschirminhalte werden nicht verarbeitet. Standortdaten werden im Rahmen dieses Services nicht verarbeitet.
- Im Rahmen der Abwehr kann eine Verbindung oder eine Adresse blockiert werden. Eine Netzwerkisolierung des gesamten Geräts, wie sie auf Windows-Clients möglich ist, findet nicht statt.
- CrowdStrike verarbeitet Daten unter dem EU-US Data Privacy Framework. Zusätzlich sind Standardvertragsklauseln (SCCs) vereinbart.

## Änderungshistorie

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

Stand: 2026-09-02