

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN (TOMS)

gemäß Art. 32 DSGVO

Anlage A zum Auftragsverarbeitungsvertrag (AVV) für die Software Surveillance Hub
G&G Sicherheitstechnik GmbH

0. ÜBERBLICK

Der Auftragsverarbeiter setzt angemessene technische und organisatorische Maßnahmen nach Art. 32 DSGVO um, um ein dem Risiko angemessenes Schutzniveau sicherzustellen. Die Maßnahmen werden regelmäßig überprüft und bei Bedarf angepasst.

1. ZUTRITTSKONTROLLE (PHYSISCH)

Ziel: Unbefugten Personen den Zutritt zu Datenverarbeitungsanlagen verwehren.

SAAS:

- Cloud-Rechenzentren in der **EU/EWR-Region** mit ISO 27001-Zertifizierung
- Mehrstufige Zutrittskontrollen (Badge, biometrisch, Überwachung)
- Videokontrolle, Logging, Besucherprotokoll

ON-PREM (VERANTWORTUNG KUNDE):

- Serverräume abschließbar
- Zutritt nur für autorisierte Personen (IT/Administration)
- Physische Sicherung (Rack-Schlösser, Gebäudesicherung)

2. ZUGANGSKONTROLLE (LOGIN-SCHUTZ)

Ziel: Unbefugte Nutzung der Systeme verhindern.

- **Passwort-Hashing mit MD5/SHA-1**
- Mindestlänge 12+ Zeichen (konfigurierbar)
- **MFA ab Beta Version verpflichtend**
- Session-Timeouts, automatische Abmeldung

3. ZUGRIFFSKONTROLLE (RBAC + RECHTE)

Ziel: Zugriffe nur nach „Need-to-Know“ und „Least-Privilege“.

- Granulares Rollen- und Berechtigungssystem (Admin / Operator / Viewer)
- Mandantenisolierung im SaaS-Betrieb
- Strikte Trennung von Entwicklungs- und Produktivsystemen

4. WEITERGABEKONTROLLE

Ziel: Verhindern, dass personenbezogene Daten unbefugt weitergegeben werden.

- Transportverschlüsselung **TLS 1.2/1.3**
- Logging jeder Datenübermittlung (z. B. Export von Alarmbildern) ab Beta Version
- Verschlüsselung von Alarmbildern im Objektspeicher ab Beta Version

5. EINGABEKONTROLLE (AB BETA VERSION)

Ziel: Nachvollziehbarkeit, wer Daten eingegeben, verändert oder gelöscht hat.

- **Audit-Logs** für:
 - Logins/Logouts
 - Konfigurationsänderungen
 - Rollenänderungen
 - Datenexporte
 - Alarmbild-Abrufe
- Unveränderliche Log-Speicherung (append-only)

6. AUFTRAGSKONTROLLE

Ziel: Verarbeitung nur auf dokumentierte Weisung des Verantwortlichen.

- Vertragliche Festlegung gemäß AVV
- Support-Zugriffe nur nach Freigabe des Kunden (Ticket-ID + MFA)
- Verpflichtung aller Mitarbeitenden auf Vertraulichkeit

7. VERFÜGBARKEITSKONTROLLE & RESILIENZ

Ziel: Schutz vor Verlust oder Beschädigung von Daten.

SAAS-BETRIEB

- Redundante Cloud-Infrastruktur (Multi-AZ, Load Balancer) ab Beta Version
- Tägliche Backups (DB, Objektspeicher)
- Monitoring & automatisches Failover ab Beta Version

ON-PREM

- Kunde setzt Backups, Monitoring & Hardware-Redundanz selbst um
- Anbieter liefert Härtingsleitfaden

8. TRENNUNGSKONTROLLE

Ziel: Sicherstellen, dass Daten verschiedener Kunden getrennt verarbeitet werden.

- Mandantenfähige Architektur
- Getrennte Datenbankebenen / logische Isolation

9. VERSCHLÜSSELUNG

Ziel: Schutz personenbezogener Daten vor Einsicht durch Unbefugte.

- **TLS** für alle externen Verbindungen
- **Verschlüsselung von Alarmbildern und Passwörtern in Datenbank**
- Kein Klartext-Passwort in Logs oder Speicher

10. DATENSCHUTZ DURCH TECHNIKGESTALTUNG (PRIVACY BY DESIGN)

- Standardmäßig kurze Retention für Alarmbilder (konfigurierbar ab Beta Version)
- Minimale Datenerhebung (E-Mail, Rollen, Alarmbilder)
- Keine dauerhafte Videoüberwachung → **nur Snapshots bei Alarm**
- Standardmäßig restriktive Rollen

11. DATENSCHUTZ DURCH VOREINSTELLUNGEN (PRIVACY BY DEFAULT)

- E-Mail-Benachrichtigungen optional pro Nutzer
- Standard-Rollen: nur minimale Berechtigungen
- Standard-Löschfristen aktiv

12. PSEUDONYMISIERUNG & MINIMIERUNG

- Interne IDs statt Klarnamen, wo möglich
- Alarmbilder enthalten Metadaten, aber keine unnötigen Informationen
- Keine Analyse / kein Profiling

13. PROTOKOLLIERUNG & MONITORING

- Zentralisiertes Log-Monitoring
- Überwachung auf Verfügbarkeitsvorfälle ab Beta Version

14. PATCH- & SCHWACHSTELLEN-MANAGEMENT

- Regelmäßige Updates (OS, Frameworks)
- Kritische Sicherheitsupdates innerhalb von **≤ 7 Tagen**

15. INCIDENT-RESPONSE-MANAGEMENT

- Dokumentiertes Incident-Response-Verfahren
- Benennung eines Security-Verantwortlichen
- Meldung von Datenschutzverletzungen an Verantwortliche **innerhalb 48h**
- Root-Cause-Analysis nach Vorfällen

16. UNTERAUFTRAGSVERARBEITER (SUBPROZESSOREN)

Alle Subprozessoren:

- werden nach Art. 28 DSGVO vertraglich gebunden
- erfüllen Sicherheitspflichten
- befinden sich in der **EU/EWR-Region** oder nutzen SCC bei Drittländern

17. SPEZIFISCHE MAßNAHMEN FÜR ALARMBILD-SPEICHERUNG

Diese Maßnahmen betreffen genau euer System:

- Speicherung nur bei klar definiertem Alarm
- Verschlüsselung aller Bilddateien (ab Beta Version)
- Zugriff nur für berechnigte Rollen
- Protokollierung jedes Abrufs (ab Beta Version)

- Automatische Löschung nach Retention

18. BEWERTUNG & REGELMÄßIGE WIRKSAMKEITSKONTROLLE

- Jährliche Überprüfung der TOMs
- Protokollierung sämtlicher Änderungen
- Offboarding-Prozesse für Benutzer und Admins