

Technische und organisatorische Maßnahmen (TOM) & Restrisiko-Bewertung

MUSTER — kein Rechtsrat. Vor Verwendung durch DSB/Fachanwalt prüfen lassen.
Betreiber: [Firma] · Stand: [Datum] · Version: 1.0

Nachweis nach Art. 32 DSGVO für die Verarbeitung „KI-Nutzung über AISecurityGateway“. Ergänzt das übergeordnete SCHUTZKONZEPT.md.

1. Umgesetzte Maßnahmen

Schutzziel	Maßnahme	Status
Datenminimierung / Vertraulichkeit	PII-Filter im Gateway (Pseudonymisierung in-memory, kein PII-Speicher)	[aktiv]
Vertraulichkeit	DNS-Sperre der KI-Web-Frontends (Shadow-AI-Schutz)	[aktiv]
Vertraulichkeit	Optionale KI-API-Sperre (fängt CLI-/Desktop-Tools)	[aktiv/inaktiv]
Integrität der DNS-Ebene	DoH-Canary + Browser-Policies (DoH-Abschaltung)	[aktiv]
Egress-Kontrolle	Host-Firewall-Regeln (Port 53/853, DoH-IPs)	[aktiv/geplant]
Zugriffskontrolle	Admin-Login, Standard-Nutzer ohne lokale Admin-Rechte	[aktiv]
Nachweisbarkeit	Audit-Log (nur Metadaten), Export CSV/PDF	[aktiv]
Datenminimierung des Protokolls	Interaktive Kontexterkennung: Audit zählt nur neu eingebrachte PII, nicht den je Folge-Turn wiederholten Chat-Kontext (Maskierung bleibt für alle Inhalte aktiv)	[aktiv]
Vertraulichkeit (Medien-Kanal)	Medien-Policy: nicht text-filterbare Uploads (Bild/Video/Audio/Dokument) werden per Default entfernt (strip) bzw. abgelehnt (block) statt ungefiltert weitergeleitet	[strip/block/allow]
Verfügbarkeit	[redundante DNS-Instanzen / Backup]	[..]

Konfigurationsstand (Soll): alle o. g. Schichten gesetzt; siehe SCHUTZKONZEPT.md §1.

2. Restrisiko-Bewertung

Restrisiko (SCHUTZKONZEPT.md §2)	Eintrittswahrsch.	Auswirkung	Behandlung
Nicht verwaltete Geräte (BYOD/Gäste/IoT) [..]	[..]	[..]	Netz-Segmentierung; BYOD-Richtlinie
Privates Gerät im Mobilfunk [..]	[..]	[..]	Nutzungsrichtlinie; Verbot
Privilegierter Insider (lokale Admin-Rechte) [..]	[..]	[..]	Rechteentzug; Governance
Analoger Weg (abfotografieren/abtippen) [..]	[..]	[..]	Schulung; Governance

Bewertungsmaßstab: Art. 32 verlangt *angemessene* Maßnahmen nach Stand der Technik, **kein Nullrisiko**. Die verbleibenden Risiken werden bewusst getragen und organisatorisch behandelt (Risikomanagement, nicht Konformitätsmangel).

3. Verantwortlichkeiten & Prüfung

- Verantwortlich für Betrieb/Konfiguration: [Name/Rolle]
- Regelmäßige Überprüfung der Wirksamkeit: [Intervall, z. B. jährlich]
- Nächste Prüfung: [Datum]

Freigegeben: [Name/Funktion], [Datum]