Security & Compliance – One Pager
heronOS - KI Basierte Digitale Fachkräfte

KI-SaaS Plattform für KI-basierte digitale Fachkräfte von heronOS – sichere, DSGVO konforme Bereitstellung von KI-Services für Unternehmenskunden.

1. Informationssicherheit

- ISO 27001: vorbereitet, Stand 08/2025
- SOC 2 Typ II: Audit abgeschlossen (jährlich erneuert)
- BSI C5: in Prüfung
- Incident Response: 24×7-SOC, standardisierte Runbooks, Eskalationspfade
- Schwachstellenmanagement: Monatliche Scans, jährlicher externer Pen-Test, SBOM verfügbar

2. Datenschutz & DSGVO

- Datenresidenz: EU / Deutschland (ISO 27001-zertifizierte Rechenzentren, Deutsche Telekom
- Rechte der Betroffenen: Export/Löschung binnen 30 Tagen, Self-Service per Ticketanforderung möglich
- Privacy-by-Design: Pseudonymisierung, Datenminimierung, Privacy Impact Assessments
- Auftragsverarbeitung (DPA/AVV): vorhanden inkl. TOMs & Sub-Prozessorliste

3. Verschlüsselung & Zugriff

- Transportverschlüsselung: TLS 1.2+
- Speicherverschlüsselung: AES-256 at rest, Customer-Managed Keys optional
- Zugriffskontrolle: RBAC/ABAC, SSO via SAML 2.0 / OIDC, SCIM-Provisioning
- Audit & Logging: (SIEM/Splunk/ELK) Vollständige Audit-Trails, exportierbar ins Kundensystem

4. Betriebs- & Ausfallsicherheit

- Verfügbarkeit: 99,9 % SLA (Multi-AZ-Betrieb, automatisiertes Failover)
- Backups & DR: Tägliche Backups, 35 Tage Retention, RPO ≤ 1 h, RTO ≤ 4 h
- Monitoring: 24×7 Überwachung, automatisierte Alarme, Health-Dashboard
- Change Management: ITIL-konform, DevSecOps-Pipeline mit Code-Review & Security-Gates

5. KI-spezifische Sicherheit

- Modell-Governance: Versionierung, Auditierbarkeit, A/B-Rollouts
- Output-Kontrolle: PII-Redaktion, Toxicity-/Policy-Filter, Halluzinations-Monitoring
- Transparenz: Dokumentierte Datenquellen (kein Training mit Kundendaten ohne Opt-in)
- Fairness & Bias: regelmäßige Evaluation & Benchmarking

6. Ansprechpartner

- Datenschutzbeauftragter (DPO): heydata GmbH, erreichbar unter privacy@heronOS.com
- Security Incident Kontakt: info@heronOS.com