



1. Sicherheitsrahmen und Geltungsbereich

GovRadar entwickelt und betreibt eine KI-gestützte Software-as-a-Service-Lösung für die öffentliche Verwaltung. Informationssicherheit ist ein zentraler Bestandteil des Betriebsmodells, da Kundinnen und Kunden GovRadar vertrauliche Verwaltungs-, Vergabe- und Projektdaten anvertrauen.

Der Geltungsbereich des Informationssicherheitsmanagementsystems umfasst alle Assets und Prozesse der GovRadar GmbH für Entwicklung und Betrieb der SaaS-Applikation, die zugehörigen Schnittstellen, das Hosting von Daten sowie die unterstützenden Prozesse, die für die Leistungserbringung erforderlich sind.

2. ISMS und Governance

GovRadar betreibt ein Informationssicherheitsmanagementsystem, dessen interne Prozesse an **ISO 27001:2022** ausgerichtet sind. Sicherheitsrelevante Richtlinien, Kontrollen, Verantwortlichkeiten, Lieferantenbewertungen, Zugriffsprüfungen, Backup-Tests und Vorfalldaten sind im ISMS dokumentiert und werden regelmäßig überprüft.

Die Geschäftsführung unterstützt das ISMS organisatorisch und stellt die hierfür erforderlichen Ressourcen bereit. Rollen und Verantwortlichkeiten für Informationssicherheit, operative Sicherheitsprozesse und Asset Ownership sind festgelegt.

3. Hosting und Datenstandort

GovRadar verarbeitet Kundendaten in der **Microsoft Azure Cloud** in der Region **Germany West Central**. Die Verarbeitung erfolgt damit in **Deutschland**, am Standort **Frankfurt am Main**.

Microsoft ist technischer Unterauftragsverarbeiter im Sinne der DSGVO. Zwischen GovRadar und Microsoft besteht eine vertragliche Regelung zur Auftragsverarbeitung gemäß Art. 28 DSGVO.

GovRadar wird als browserbasierter SaaS-Dienst bereitgestellt. Kundenseitig ist in der Regel keine lokale Installation erforderlich. Der Zugriff erfolgt über abgesicherte Standardverbindungen.

4. Vertraulichkeit und Mandantentrennung

Kundendaten werden ausschließlich **im Auftrag und auf Weisung** der jeweiligen Kundenorganisation verarbeitet. Eine Nutzung zu eigenen Zwecken findet nicht statt.

Die Daten verschiedener Kundenorganisationen werden durch eine konsequente **logische Mandantentrennung** voneinander getrennt. Ein Zugriff oder Datenaustausch zwischen Kundenorganisationen ist ausgeschlossen.

5. Zugriffskontrolle und Berechtigungsmanagement

Kundeninhalte werden ausschließlich **im Auftrag und auf Weisung** der jeweiligen Kundenorganisation verarbeitet. Eine Nutzung zu eigenen Zwecken findet nicht statt.

Die Daten verschiedener Kundenorganisationen werden durch eine konsequente **logische Mandantentrennung** voneinander getrennt. Ein Zugriff oder Datenaustausch zwischen Kundenorganisationen ist ausgeschlossen.

6. Kryptographie und Schutz vertraulicher Informationen

GovRadar setzt kryptographische Verfahren ein, um Vertraulichkeit, Integrität und Authentizität von Informationen zu schützen. Die Auswahl orientiert sich an anerkannten Standards und den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Kundeninhalte werden sowohl bei der Übertragung als auch bei der Speicherung geschützt. Schlüssel und Secrets werden über definierte Prozesse und Systeme verwaltet. Vergabe, Erneuerung und Deaktivierung folgen den Vorgaben des Berechtigungs- und Zugriffskonzepts.

7. Sichere Entwicklung und Änderungsmanagement

GovRadar folgt einem kontrollierten Entwicklungslebenszyklus. Softwareänderungen erfolgen versioniert, nachvollziehbar und erst nach erfolgreichen Reviews, Tests und Sicherheitsprüfungen.

Pull Requests, Code Reviews, statische Analysen, Testpipelines und dokumentierte Freigabeprozesse sind Bestandteil des Entwicklungsprozesses. Entwicklungs- und Produktionsumgebungen sind voneinander getrennt. Für Entwicklungs- und Testzwecke werden keine produktiven Kundendaten verwendet.

Änderungen an sicherheitsrelevanten Systemen und Prozessen werden kontrolliert und dokumentiert.

8. Logging, Monitoring und Nachvollziehbarkeit

System- und sicherheitsrelevante Ereignisse werden protokolliert und überwacht, um Abweichungen, Fehlverhalten und potenzielle Sicherheitsvorfälle frühzeitig zu erkennen.

Für die Zusammenarbeit innerhalb einer Kundenorganisation werden Bearbeitende und Bearbeitungszeitpunkte nachvollziehbar gespeichert. Ergänzend werden technische Logs für definierte Zeiträume vorgehalten, um Sicherheit, Stabilität und forensische Nachvollziehbarkeit des Betriebs sicherzustellen.

9. Incident Management

GovRadar verfügt über definierte Prozesse zur Erkennung, Meldung, Klassifizierung, Bearbeitung und Nachbereitung von Sicherheitsvorfällen. Sicherheitsvorfälle werden dokumentiert, nach Schweregrad bewertet und anhand festgelegter Verantwortlichkeiten bearbeitet.

Bei bestätigten relevanten Sicherheitsvorfällen werden betroffene Kundenor-

ganisationen informiert und über wesentliche Maßnahmen sowie den weiteren Verlauf auf dem Laufenden gehalten.

10. Datensicherung, Wiederherstellung und Notfallvorsorge

Für produktive Systeme und Daten bestehen geregelte Sicherungs- und Wiederherstellungsverfahren. Backups werden regelmäßig durchgeführt und die Wiederherstellbarkeit wird durch wiederkehrende Restore-Tests überprüft.

Ergänzend betreibt GovRadar Maßnahmen des Business Continuity Managements (BCM), um auf widrige Situationen und Notfälle vorbereitet zu sein. Relevante Szenarien werden regelmäßig überprüft und praktisch geprobt.

11. Datenschutz und Datenlebenszyklus

GovRadar verarbeitet personenbezogene Daten als Auftragsverarbeiter im Sinne von Art. 28 DSGVO. Ein Auftragsverarbeitungsvertrag (AVV) steht für Kundinnen und Kunden zur Verfügung.

Kundeninhalte werden nach Ende des Vertragsverhältnisses gemäß dokumentiertem Löschprozess gelöscht. Die Umsetzung wird regelmäßig anhand von Löschprotokollen und Stichproben kontrolliert.

12. Lieferanten- und Subprozessorenmanagement

Lieferanten mit Relevanz für Informationssicherheit, Datenschutz oder Verfügbarkeit werden vor ihrer Nutzung bewertet und mindestens jährlich überprüft. Die Bewertung umfasst insbesondere Sicherheitsnachweise, Zugriffskontrollen, Datenschutzerfordernisse und Verfügbarkeitsaspekte.

Für die kundendatenrelevante Leistungserbringung ist Microsoft Azure der zentrale technische Unterauftragsverarbeiter für Hosting und Cloud-Infrastruktur in Deutschland.

13. Compliance und Nachweise

GovRadar richtet seine internen Prozesse an ISO 27001:2022 aus. Eine eigene Zertifizierung wird 06/2026 angestrebt. Für die eingesetzte Cloud-Infrastruktur stützt sich GovRadar auf anerkannte Zertifizierungen, Auditberichte und Trust-Center-Dokumentation der eingesetzten Anbieter.

14. Einordnung für prüfende Stellen

GovRadar bietet damit einen klar eingegrenzten und dokumentierten Sicherheitsrahmen für den Einsatz in der öffentlichen Verwaltung. Dazu gehören insbesondere:

- Verarbeitung von Kundeninhalten in Deutschland
- logische Mandantentrennung
- rollenbasierte Zugriffskontrolle
- kryptographischer Schutz bei Übertragung und Speicherung
- kontrollierte Softwareentwicklung
- geregeltes Incident Management
- dokumentierte Backup- und Wiederherstellungsverfahren
- strukturierte Lieferantensteuerung
- ISMS-orientierte Governance und Nachweisfähigkeit

So erhalten IT-Verantwortliche und prüfende Stellen eine belastbare Grundlage, um Sicherheitsniveau, Betriebsmodell und Nachweisfähigkeit von GovRadar effizient einzuordnen.