

T.I.S.P./T.P.S.S.E. Community Meeting 2025

Berlin, 04. - 05.11.2025

Betrieb einer privaten cloudbasierten Plattform trotz überbordender Regulatorik

Stefan Haibach, Geschäftsführer, ITSG GmbH

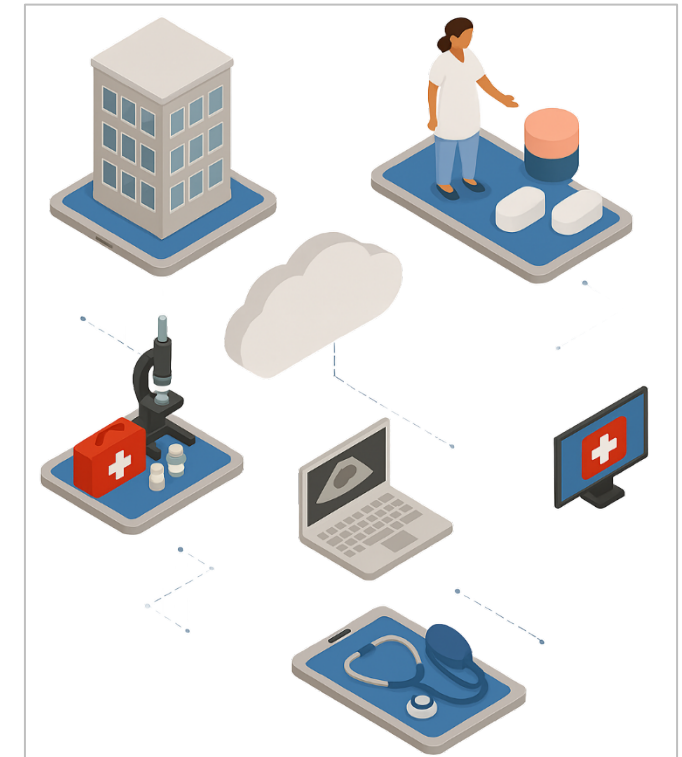
Philipp C. Rothmann, externer DSB, ITSG GmbH

- Zentrale IT-Dienstleisterrolle für die GKV; Betrieb sicherer digitaler Lösungen.
- Eigentümer- und Governance-Struktur aus GKV-Trägern.
- Rechenzentrumsbetrieb mit hoher Verfügbarkeit als Basis der Private Platform.
- Betrieb redundanter Systeme über drei Standorte in Frankfurt für maximale Ausfallsicherheit.
- Spezialisierung auf mandantenfähige Infrastrukturen für sensible Sozial- und Gesundheitsdaten.
- Integration von Hybrid-Cloud-Optionen wie Azure für erweiterte Flexibilität.



ITSG

- Digitalisierung transformiert das Gesundheitswesen grundlegend.
- Zentrale Entwicklungen: elektronische Patientenakten, Telemedizin, KI-gestützte Diagnosen.
- Cloubasierte Plattformen ermöglichen effiziente, sichere und sektorübergreifende Datenverwaltung.
- Fördern neue Formen der Zusammenarbeit zwischen Ärzten, Patienten und Behörden.
- Gleichzeitig entstehen hohe Anforderungen an Datenschutz, Informationssicherheit und Compliance.



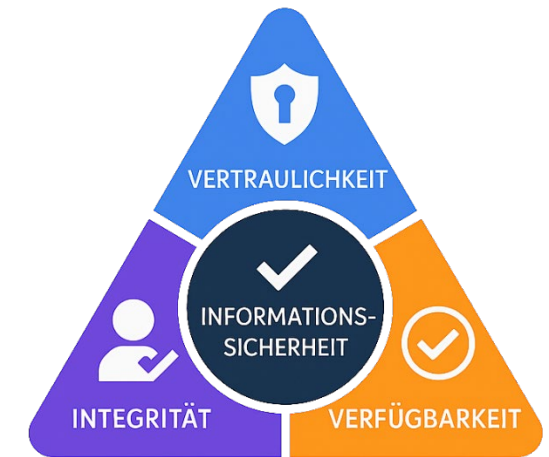
- Sensible Patientendaten stehen im Fokus des Gesundheitssystems.
- Betreiber cloudbasierter Plattformen müssen Verfügbarkeit, Vertraulichkeit und Schutz vor Missbrauch sicherstellen.

Zentrale Herausforderungen

- Strenge Vorgaben zu Datenschutz und Informationssicherheit.
- Einhaltung nationaler und europäischer Regelwerke (z. B. DSGVO, § 393 SGB V).
- Nachweis höchster Sicherheitsstandards für alle Beteiligten (Patienten, Ärzte, IT, Behörden).

Ziel

- Entwicklung einer Cloud-Plattform, die Compliance, Skalierbarkeit und Innovationskraft vereint.



Was ist Sozialdatenschutz?

- Schutz personenbezogener Daten im Rahmen sozialer Leistungen.
- Besonders schützenswert: Patientendaten im Gesundheitswesen.

Zentrale Gesetze und Vorschriften

- § 35 SGB I (Sozialgeheimnis): Verarbeitung nur mit gesetzlicher Grundlage oder Einwilligung. §§ 67 ff.
SGB X: Regelungen zu Erhebung, Verarbeitung, Nutzung, Speicherung, Übermittlung und Löschung von Sozialdaten.
- § 284 SGB V: Spezielle Regelungen für Krankenkassen.
- DSGVO & BDSG: Ergänzende Datenschutzgesetze, aber Vorrang der spezialgesetzlichen Regelungen im SGB X.

Technische und organisatorische Anforderungen

- Verarbeitung nur in der EU oder in Staaten mit Angemessenheitsbeschluss.
- Cloud-Anbieter müssen strenge Datenschutzanforderungen erfüllen (z. B. ISO/IEC 27001, C5-Testat).

Rechte der Betroffenen

- Auskunft, Berichtigung, Löschung, Widerspruch, Datenübertragbarkeit (außer bei spezialgesetzlichen Einschränkungen).

Aktuelle Entwicklungen

- Gesundheitsdatennutzungsgesetz (GDNG, 2024): Erleichtert Gesundheitsdaten-Nutzung für Forschung, setzt neue Anforderungen an Datenschutz.
- Digital-Gesetz (DigiG, 2024): Fördert Digitalisierung, regelt elektronische Patientenakte.

Fazit

- Sozialdatenschutz ist essenziell für den vertrauensvollen Umgang mit Gesundheitsdaten und sichere digitale Gesundheitsversorgung.

Schutz personenbezogener Gesundheitsdaten

- DSGVO und § 22 BDSG als gesetzliche Grundlage.
- Privacy by Design & Default: Datenschutz von Anfang an integrieren.
- Datenminimierung & Zweckbindung: Nur notwendige Daten werden verarbeitet, immer zweckgebunden.
- Transparente Einwilligung: Patienten behalten Kontrolle über ihre Daten und deren Freigabe.
- Pseudonymisierung & Verschlüsselung: Schutz der Daten bei Speicherung und Übertragung.
- Verarbeitungsverträge (AVV): Klare Verantwortlichkeiten zwischen Cloud-Anbieter und Datenverantwortlichem.



Beispiel

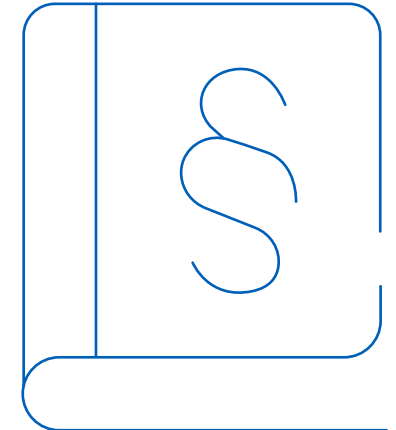
- Patient steuert gezielt, welche Ärzte Zugriff auf die elektronische Patientenakte erhalten.

Neue Anforderung ab 1. Juli 2025

- Cloud-Anbieter im Gesundheitswesen müssen ein C5-Typ-2-Testat des BSI vorweisen.

Vorteile des C5-Testats

- Regelmäßige Prüfung der technischen und organisatorischen Maßnahmen (TOMs).
- Transparenz und Auditierbarkeit: Prüfbarkeit gegenüber Behörden und Krankenkassen.
- Rechtskonformität: Nur Cloud-Computing-Dienste mit gültigem Testat dürfen genutzt werden.



Praktischer Nutzen

- IT-Entscheider können sich auf nachweislich sichere und kontrollierte Cloud-Dienste verlassen.



Bis zum 30. Juni 2025 gilt als aktuelles C5-Testat im Sinne des Absatzes 3 Nummer 2 ein C5-Typ1-Testat. Ab dem 1. Juli 2025 gilt als aktuelles C5-Testat im Sinne des Absatzes 3 Nummer 2 ein aktuelles C5-Typ2-Testat. Eine Verarbeitung nach Absatz 3 Nummer 2 ist ferner auch zulässig, soweit für die im Rahmen des Cloud-Computing-Dienstes eingesetzten Cloud-Systeme und die Cloud-Technik anstelle eines aktuellen C5-Testats ein Testat oder Zertifikat nach einem Standard vorliegt, dessen Befolgung ein im Vergleich zum C5-Standard vergleichbares oder höheres Sicherheitsniveau sicherstellt. Das Bundesministerium für Gesundheit wird ermächtigt, durch Rechtsverordnung ohne Zustimmung des Bundesrates im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik festzulegen, welche Standards die Anforderungen nach Satz 3 erfüllen.

Quelle: https://www.gesetze-im-internet.de/sgb_5/__393.html

ISO/IEC 27001

- ISMS-Rahmenwerk
- Risiken systematisch steuert
- Kontinuierlich verbessert.

ISO/IEC 27017

- Ergänzende Sicherheitskontrollen
- Speziell für Cloud-Dienste
- Cloud-spezifische Bedrohungen adressieren

ISO/IEC 27018

- Schutz personenbezogener Daten in Clouds
- Fokus auf Einwilligung, Transparenz und Löschprozesse.

Diese Zertifizierungen beweisen, dass Betreiber Risiken erkennen, minimieren und höchste Datenschutz- und Sicherheitsstandards erfüllen.

Zertifizierte Cloud-Plattform im Krankenhaus

- Ärzte haben sicheren, ortsunabhängigen Zugriff auf Patientendaten.
- Patienten steuern Freigaben für Behandler.
- Alle Zugriffe und Änderungen werden revisionssicher protokolliert.

Vorteile

- Effizientere Abläufe für Ärzte.
- Transparenz und Kontrolle für Patienten.
- Auditierbare Prozesse für Behörden.



Kombination aus DSGVO, C5-Testat und ISO-Zertifikaten garantiert

- Vertraulichkeit, Integrität und Verfügbarkeit der Daten
- Rechtskonformer, auditierbarer Betrieb der Cloud
- Vertrauen bei Patienten, Ärzten, IT-Teams und Behörden
- Zukunftsfähige Infrastruktur für innovative Versorgungsmodelle

Für IT-Entscheider

- Investitionssicherheit und solide Basis für digitale Transformation

Fazit und Ausblick

Cloud-Plattform kombiniert:

- Datenschutz, rechtliche Vorgaben und internationale Standards
- Schafft Voraussetzungen für nachhaltige, sichere digitale Transformation

Nutzen:

- Fördert Patientenschutz und Innovation im Gesundheitswesen
- Vorteil für alle Beteiligten



Problemstellung

- Historisch gewachsene ITSG-Infrastruktur mit mehreren Mandanten und Plattformen
- Fragmentierte IT-Landschaft, z. B. durch Netzwerk-Segmente und Firewall-Cluster
- Skalierungsprobleme aufgrund langer Beschaffungsprozesse und langsamer Servicebereitstellung
- Erschwerte Anpassungen (Upsizing/Downsizing) und ineffiziente Ressourcennutzung

Zielbild – Future Shift

- Konsolidierung der Landschaft bei Beibehaltung der Mandantentrennung
- Bereitstellung einer mandantenfähigen Private Platform
- Workloads werden per Lift & Shift auf die neue Plattform gehoben, Trennung erfolgt logisch oder physisch

Leitprinzipien

Interoperabilität: Gemeinsame Nutzung von Ressourcen und Services

Security by Design: Absicherung nach Schutzbedarf

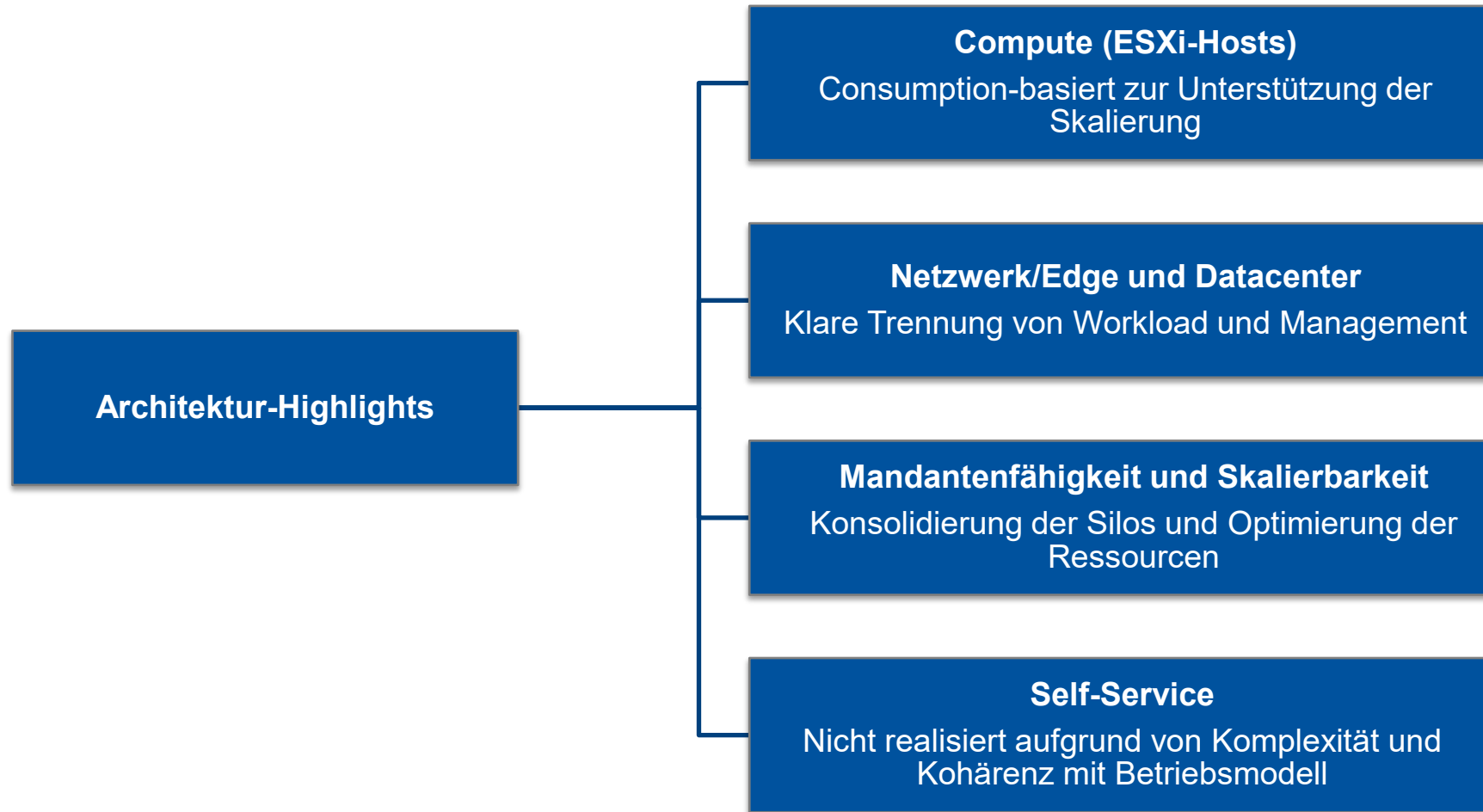
Optimierung: Fokus auf Kosten-Nutzen und schnelle Time-to-Service

Standardisierung: Orientierung an marktüblichen Standards, Herstellerunabhängigkeit

Mandantenfähigkeit: Konsequente Trennung von Ressourcen

Automatisierung: End-to-End automatisierter Betrieb

Skalierbarkeit & Flexibilität: Elastische Anpassung an Bedarf



Regulatorische Anforderungen

- DSGVO, DigiG/§ 393 SGB V und GDNG: Anforderungen an Cloud-Plattformen im Gesundheitswesen.
- C5-Anforderungen (BSI): Ab 1. Juli 2025 ist ein C5-Typ-2-Testat erforderlich für Cloud-Dienste im Geltungsbereich von § 393 SGB V.
- ISO-Standards: Einsatz anerkannter Standards wie ISO/IEC 27001, 27017, 27018.

Zukunft der ITSG Private Platform

- Shared-Infrastructure-Lösung: Nutzung von Cloud-Technologie, aber ohne Public-Cloud-Self-Service.
- Regulatorische Unsicherheit: § 393 SGB V könnte ungenau sein, juristische Prüfung empfohlen.

Fazit

- ITSG Private Platform: Sichere, regulierungskonforme, standardisierte Betriebsumgebung für sensible Gesundheitsdaten.

Danke für Ihre Aufmerksamkeit
Wir freuen uns auf Ihre Fragen und einen offenen Austausch.