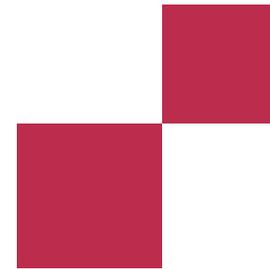


# Confidential Computing

---



Hardwaregestützte sichere Speicherung und Verarbeitung von Daten

# Verwendung von Confidential Computing für den Einsatz von Cloud Services im deutschen Gesundheitswesen

## Cloud Computing: allgemein | im deutschen Gesundheitswesen

Bereits bei 50 % der deutschen Großunternehmen ist Cloud Computing erfolgreich und nutzenbringend im Einsatz. Hierbei meint Cloud Computing die dezentrale Bereitstellung von IaaS, PaaS, oder SaaS Komponenten.

Im Vergleich zu anderen Branchen findet Cloud Computing im deutschen Gesundheitswesen weniger Verwendung. Komplexe und umfangreiche regulatorische Anforderungen erschweren hier den Einsatz von Cloud Computing.



## Vorteil bei der Verwendung von Cloud Computing

Die großen Vorteile bestehen darin, Speicher, Rechenleistung, Anwendungen, Services oder künstlichen Intelligenzen nutzen zu können, ohne dafür lokale Infrastruktur aufbauen zu müssen. Ebenfalls wird die Verantwortung von Support outsourced.

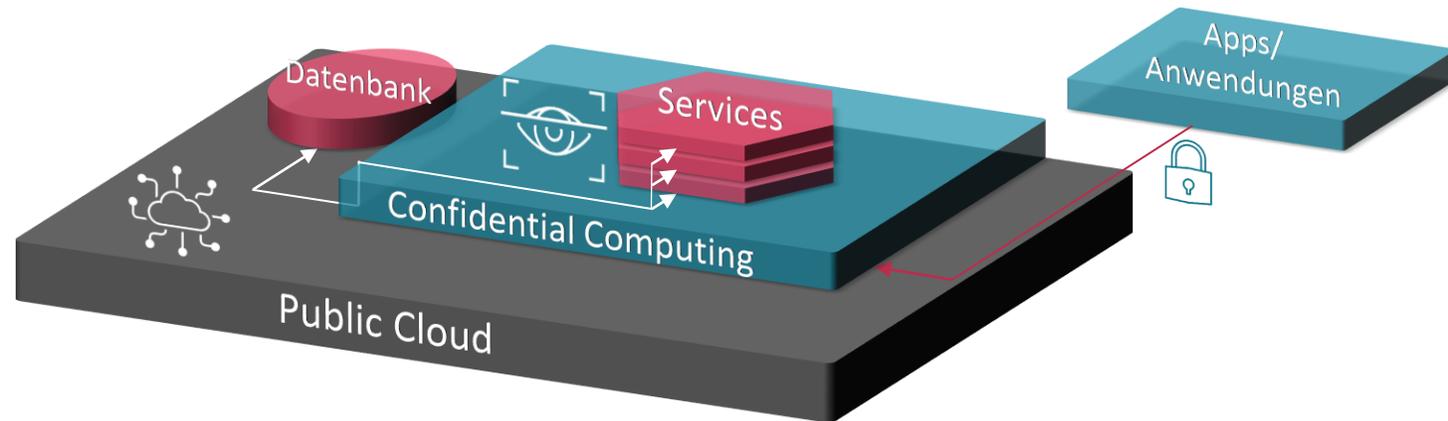
Probleme durch die Anforderungen an IT-Sicherheit und Datenschutz werden durch Confidential Computing gelöst.

# Confidential Computing zum Aufbau einer vertrauenswürdigen Cloud-Umgebung

## Confidential Computing

### Funktionsweise

- Daten werden vom Anwender verschlüsselt übertragen.
- In der Cloud werden mit spezifischen Prozessoren, die einen hochsicheren Bereiche für Schlüssel haben, die Daten verschlüsselt.
- Cold Boot und Seitenkanal-Angriffe sowie der Zugriff auf Daten durch Cloud Provider können verhindert werden.



### Anwendungsbeispiel für Confidential Computing

- Verschieden Parteien können ihre Daten gemeinsam verwenden, um gemeinsam KI-Modelle anzulernen, ohne dass die Beteiligten Zugriff auf die Daten der anderen erhalten.
- DiGAs können, durch den Einsatz von Confidential Computing schnell, sicher und kosteneffizient Cloud-Plattformen nutzen.
- Die Auswertung von Sensordaten, beispielsweise im AAL-Umfeld zur Erkennung von Stürzen, kann in der Cloud erfolgen, ohne dass Beteiligte die Patientendaten einsehen müssen.

# Wir unterstützen Sie beim Einsatz von Confidential Computing

Trust Broker	Architekturintegration	Anwendungskonzeption
<ul style="list-style-type: none"><li>▪ <b>Entwicklung</b> von Anwendungen mit CC</li><li>▪ <b>Bereitstellung</b> von Endpunkten und Infrastruktur</li><li>▪ <b>Betrieb der Software</b>, um Ihnen die Cloud Migration zu erleichtern.</li><li>▪ <b>Support aus allen Leveln</b>, um Ihr Alltagsgeschäft reibungslos zu gestalten.</li></ul>	<ul style="list-style-type: none"><li>▪ <b>Assessment:</b> Analyse Ihrer Systemlandschaft, um zu entscheiden, welche der verschiedenen Technologien zum Einsatz von Confidential Computing, am besten zu Ihnen passt.</li><li>▪ <b>Integration</b> der entsprechenden Cloud Services in Ihre Architektur.</li></ul>	<ul style="list-style-type: none"><li>▪ <b>Softwarekonzeption</b> von Anwendungen, die Ihre Vision in die Cloud transferieren können.</li><li>▪ <b>Entwicklung von Systemen</b> und die Bereitstellung der notwendigen Fachleuten, um Sie bei Ihren Ideen und Visionen zu unterstützen.</li></ul>

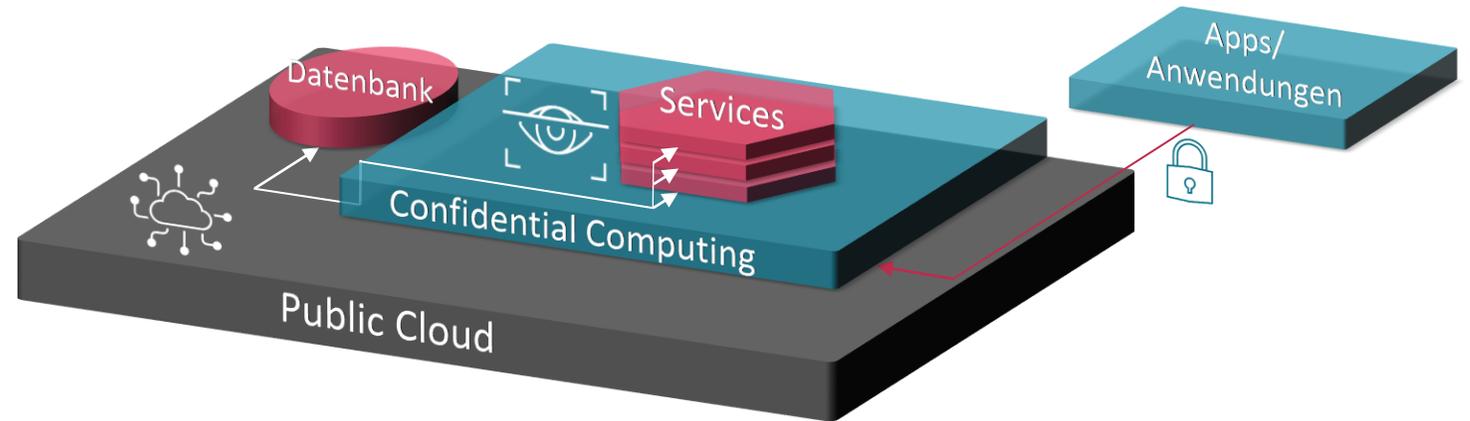


# Confidential Computing als Grundlage für den Einsatz von Cloud Services

## Confidential Computing ermöglicht die sichere Persistenz und Verarbeitung von medizinischen Daten in der Cloud

### Vorteile von Cloud Computing mit Confidential Computing

- **Sichere Anwendung:** entspricht höchsten Datenschutzanforderungen
- **Kostenoptimierung:** geringe Kosten für Cloud Deployment im Vergleich zu **On Premise Servern**
- **Intuitive Implementierung:** schnelle Reaktion auf Anforderungen
- **Bestes Nutzererlebnis:** (99.99% SLAs)



### Datensouveränität

- **Confidential Computing** gibt Ihnen die notwendigen Werkzeuge, um **volle Datensouveränität** zu erhalten.

### Mixed Cloud

- Durch die Verwendung von **offenen Standards** ist ein Wechsel des Hyperscalers problemlos möglich

### Datenschutzkonform

- Bereits durch Rechtsexperten geprüft und auditiert
- Lösung für Probleme durch CLOUD Act

# Herzlichen Dank für Ihre Aufmerksamkeit

---

Bleiben wir in Kontakt

Dr. Kai-Uwe Morgenstern

[kai-uwe.morgenstern@fbeta.de](mailto:kai-uwe.morgenstern@fbeta.de)

+49 160 7031094

