



Sicherheitsaspekte im HealthCare-Umfeld: Wechselwirkung von Datenschutz, Security und Cloud

Einleitung

Zwei Denkanstöße:

1. Umgang mit AI ChatBots
2. Umgang mit Public Cloud Anbietern

Umgang mit AI ChatBots (ChatGPT, CoPilot, BARD)

A man dressed as Pinocchio is walking in a city street. He has white face paint, a long, pointed nose, and a tall, white, conical hat decorated with red and yellow pom-poms. He is wearing a white shirt and a red vest. The background shows a busy city street with people, bicycles, and buildings.

ChatBots liefern keine Wahrheiten

ChatBots unterliegen Datenschutzrichtlinien

(z.B OpenAI: <https://openai.com/policies/privacy-policy>)





Hinweis 1

Vermeiden von
personenbezogenen Daten

Hinweis 2



Nur generische oder sogar
fiktive Informationen

A silhouette of a person walking a tightrope against a dramatic sunset sky with orange and red clouds. The person is in the center, balancing on a thin line. The background shows a horizon with mountains and a bright sun setting behind clouds.

Vorsicht bei vertraulichen Daten
(Passwörter, Bankdaten,
medizinische Daten)

Chatverläufe überprüfen (vor dem Teilen oder speichern)



Hinweis 5

Lokale Datenschutzgesetze
beachten

A wooden gavel with a brass band is positioned on a dark wooden desk. In the background, a pair of golden scales of justice is visible, along with a stack of books and a window with a grid pattern. The scene is lit with warm, soft light, creating a professional and legal atmosphere.

Keine Rechtsschutz- oder
Datenschutz-Beratung



Und im
Gesundheitswesen?

Hinweis 7

Die Risiken und Gefahren sind die gleichen, die Einsatzmöglichkeiten, die Daten und Informationen sind andere !



Fehldiagnosen und Behandlungsfehler
Haftungsfragen
Ethik und Transparenz

Beispiel aus Forschung, Entwicklung und Praxis:

Stanford University – interdisziplinäres Lernen

Stanford School of Medicine
Stanford Center for Health Education
Stanford School of Engineering

[Artificial Intelligence in Healthcare | Program | Stanford Online](#)

| COURSES | |
|--|--|
|  | Introduction to Healthcare SOM-XCHE0008 |
|  | Introduction to Clinical Data SOM-XCHE0009 |
|  | Fundamentals of Machine Learning for Healthcare SOM-XCHE0010 |
|  | Evaluations of AI Applications in Healthcare SOM-XCHE0011 |
|  | AI in Healthcare Capstone SOM-XCHE0012 |

Umgang mit Public Cloud Anbietern

A dark blue door with ornate brass handles and a keyhole. A bright light shines through the crack in the door, creating a strong lens flare effect. The text "Neue Technologien bieten neue Möglichkeiten" is overlaid on the bottom half of the image.

Neue Technologien bieten neue
Möglichkeiten



Public Cloud Anbieter unterliegen Schweizer Datenschutzrichtlinien

Interoperabilität und Daten
Portabilität richtig nutzen



Zollbereich
Kein Zutritt

Customs area
No entry

Datenhoheit und Kontrolle
sicherstellen



stay_safe

Danke für Ihre Zeit

Koordinaten für weitere Informationen:

Markus.Kaegi@UMB.ch

+41 79 286 88 17

UMB

creating time®

UMB

creating time®

BACKUP

revDSG Anforderungen und Möglichkeiten in Cloud-Services von Microsoft (Top 6)

| Anforderung revDSG | Microsoft Funktionalität | Beschreibung der Funktionalität |
|---|---|--|
| Art. 6 Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit (CIA) | MS 365 IAM & Privileged Access Management Conditional Access | <ul style="list-style-type: none">– aktive Verwaltung von privilegierten Zugriffen– Einschränkung von ständigem Zugriff auf sensible Daten oder Zugriff auf kritische Konfigurationseinstellungen |
| Art. 7 Datenschutz durch Technik & Voreinstellung | Verschlüsselung & Schlüsselmanagement | <ul style="list-style-type: none">– kein Zugang zu hochsensiblen Daten für Unbefugte (inkl. Microsoft)– Schlüssel bleiben innerhalb einer geografischen Grenze und unter Ihrer eigenen Kontrolle |

revDSG Anforderungen und Möglichkeiten in Cloud-Services von Microsoft (Top 6)

| Anforderung revDSG | Microsoft Funktionalität | Beschreibung der Funktionalität |
|---|--|---|
| Art. 12 Verzeichnis der Bearbeitungstätigkeiten | Microsoft Information Protection | <ul style="list-style-type: none">– Compliance-Beauftragte kennen die Speicherorte sensibler Informationen– Sicherheitsadministratoren setzen Richtlinien für den Datenzugriff und den Schutz vor Datenverlusten (DLP) auf der Grundlage von Labels um |
| Art. 6 Abs 5. Auf Risiken abgestimmte Massnahmen | Privacy Management & Compliance Manager | <ul style="list-style-type: none">– Identifizierung kritischer Datenschutzrisiken und Konflikte |

revDSG Anforderungen und Möglichkeiten in Cloud-Services von Microsoft (Top 6)

| Anforderung revDSG | Microsoft Feature | Beschreibung der Funktionalität |
|--|------------------------------------|--|
| Art. 25 Auskunftsrecht (Data Subject Request) | Microsoft Priva & Pureview | <ul style="list-style-type: none">– Identifizierung der personenbezogenen Daten, die Gegenstand der Anfrage sind– Identifizierung kritischer Datenschutzrisiken und Konflikte– Automatisierung von Datenschutzmassnahmen und Beantwortung von Anfragen der Betroffenen |
| Art. 22 Datenschutz- Folgeabschätzung | Microsoft 365 Compliance Center | Microsoft unterstützt das Erstellen einer Datenschutz-Folgenabschätzung für Vorgänge, die "wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führen." |