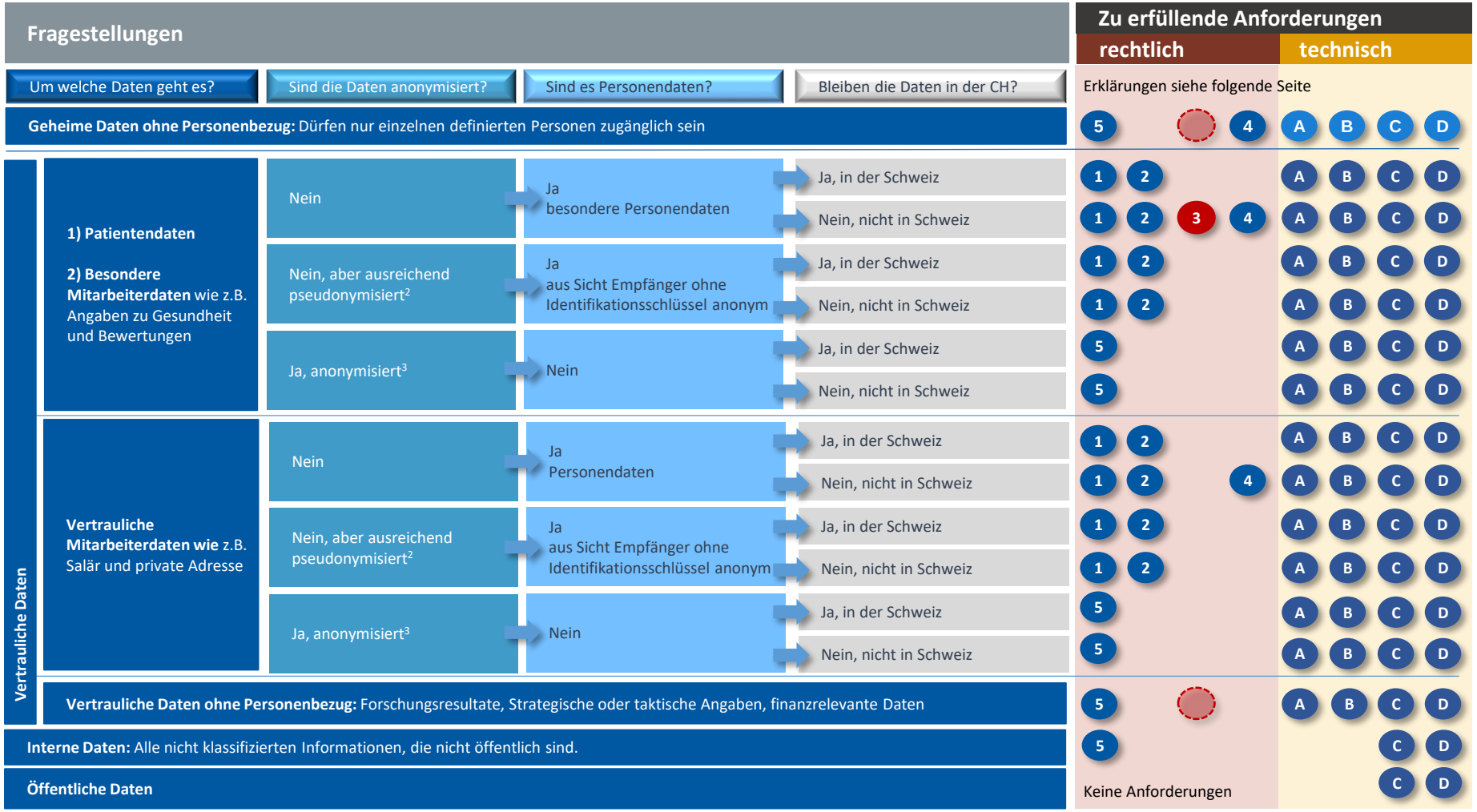
Nutzung von Cloud-Lösungen[1] - Datenschutz-Anforderungen (1/2)



1) Lösung, bei der Speicherplatz (Hosting), Betriebssystem, Runtime und Software eines Anbieters im Auftragsverhältnis genutzt und hierzu Daten über das Internet transferiert werden (Software as a Service) oder anderweitige Onlinedienste ohne End-to-End Verschlüsslung.

2) Daten können nur noch mit unverhältnismässigem Aufwand durch Dritte einer bestimmten Person zugeordnet werden und der Identifikationsschlüssel muss in Besitz des Auftraggebers sein. Sofern dies gegeben ist, können die Daten gegenüber dem Empfänger/Auftragnehmer als anonymisiert betrachtet werden.

3) Im Unterschied zur Pseudonymisierung ist eine Anonymisierung irreversibel; d.h. der Rückschluss auf eine Person ist niemals möglich.

Sofern Daten unter das Amtsgeheimnis fallen, ist eine Entbindung nötig.

Nutzung von Cloud-Lösungen[1] - Datenschutz-Anforderungen (2/2)

Rechtliche Anforderungen (zwingend)

1

Eine **vertragliche Grundlage** für die Bearbeitung von personenbezogenen Daten muss vorhanden sein (Mindestinhalt AGB des Kt. ZH). Der Anbieter muss dabei sorgfältig ausgesucht (seriöser, verlässlicher Anbieter) werden und gegenüber dem Auftraggeber weisungsgebunden sein. Rechte und Pflichten des Anbieters müssen geregelt sein; Mitarbeitende des Anbieters müssen vertraglich auf die Geltung der ärztlichen Schweigepflicht hingewiesen werden. In hiervon abweichenden vertraglichen Grundlagen ist die nachweisbare explizite Einwilligung der betroffenen Person erforderlich.
Zweckbindung muss erfüllt sein; d.h. die betroffene Person hat dem Auftraggeber die Daten zu diesem Zweck anvertraut und der Anbieter wird verpflichtet, die Daten ausschliesslich zu diesem Zweck zu bearbeiten.
Verhältnismässigkeit muss gegeben sein: d.h. es dürfen nur Daten weitergegeben werden, welche auch effektiv für die Bearbeitung benötigt werden. Werden z.B. Vor- und Nachname für die Bearbeitung nicht benötigt, dürfen diese auch nicht weitergegeben werden.

2

Bei der Bearbeitung von Personendaten muss eine **Datenschutz-Folgenabschätzung** erstellt werden. Bei besonderen Risiken (z.B. bei einer grossen Menge von Personendaten oder bei der Nutzung neuer Technologien etc.) ist zudem eine die **Vorabkontrolle** durch die kantonale Datenschutzbeauftragte erforderlich.

3

Eine nachweisbare Information und **explizite Einwilligung** der betroffenen Person ist zwingend erforderlich. Gibt eine Patientin/ein Patient keine Einwilligung, muss nach Möglichkeit für die Behandlung eine alternative Lösung zur Verfügung stehen, sofern dies gemäss kantonalem Leistungsauftrag erforderlich ist. Alternativ zur schriftlichen Zustimmung des Patienten oder bei Amtsgeheimnissen kann über den Rechtsdienst eine Bewilligung durch die Gesundheitsdirektion des Kt. ZH eingeholt werden.

4

Der **Schutz im Empfängerstaat** muss mindestens jenem der Schweiz entsprechen (vgl. Liste EDÖB). Bei Anbietern in Empfängerstaaten, welche nicht auf der Liste des EDÖB geführt sind oder welche Sitz in den USA haben, muss eine Risikobeurteilung vorgenommen und vertragliche Äquivalenz mit dem schweizerischen Datenschutzniveau hergestellt werden.

5

Auch bei nicht personenbezogenen Daten muss eine **vertragliche Grundlage** für die Bearbeitung der Daten vorhanden sein. Der Anbieter muss dabei sorgfältig ausgesucht werden. Zweckbindung und Verhältnismässigkeit muss auch hier gewahrt sein.

Technische Anforderungen (risikobasiert)

A

Transfer der Daten muss **zwingend verschlüsselt** erfolgen (minimal mittels Verschlüsselungsprotokoll wie aktuelle Version TLS, IPsec, VPN).

B

Anbieter muss die Daten **gemäss aktuellem Stand der Technik schützen**. Dabei sind insbesondere folgende Punkte zu beachten:

- Der Anbieter ist gemäss einem gängigen Standard (z.B. ISO 27001) zertifiziert.
- Prüfresultate (Zertifizierungen) müssen dem Auftraggeber bei Verlangen zur Verfügung gestellt werden.
- Der Anbieter muss über ein Informationssicherheitskonzept verfügen und den Auftraggeber bei Nachfrage über dessen Stand informieren.
- Daten sind vor Ort kryptographisch verschlüsselt.
- Der Anbieter verfügt über Prozesse, mit welchen sichergestellt wird, dass der Verlust von Daten und/oder der Missbrauch dem Auftraggeber zeitnah gemeldet wird.
- Der Anbieter verfügt über eine Liste aller Nutzer, welche auf Daten zugreifen können inkl. Administratoren.
- Zugriffe sind in Log nachvollziehbar.
- Zugriffe entsprechen dem Need-to-Know-Prinzip und wird regelmässig überprüft.
- Der Auftraggeber hat das Recht, bei Bedarf einen Audit des Anbieters durchzuführen.

C

Der für die Nutzung der Cloud verantwortliche Bereich, muss vor Nutzung der Cloud ein angemessenes **Risk Assessment** durchführen. Dabei geht es darum, Risiken zu identifizieren und diese anhand ihrer Eintretenswahrscheinlichkeit und ihrer Auswirkungen zu beurteilen sowie geeignete Massnahmen zur Minderung der Risiken zu definieren. Insbesondere stellen sich folgende Fragen:

- Ist eine **Strong Authentication** bzw. 2 Faktor Authentisierung eingerichtet?
- Wie wird der **Zugriff über private Geräte** verhindert? Kann sich ein Nutzer auch über ein privates Gerät Zugriff auf die Cloud verschaffen? Kann **Single-Sign-On** eingerichtet werden?
- Wie ist der **Zugriff von Extern durch Dritte** auf die Cloud geregelt (z.B. externe Forscher, Ärzte anderer Spitäler etc.)?
- Wie wird verhindert, dass Mitarbeitende in einer neuen Funktion oder **nach Austritt weiter Zugriff** auf die Daten haben?
- Ist die Datenübertragung **verschlüsselt** (z.B. mittels https)?
- Was geschieht, wenn das System **nicht zur Verfügung steht**? Bestehen alternative Betriebsmöglichkeiten?

D

Sofern die Daten nicht weiter benötigt werden und keine gesetzliche Aufbewahrungspflicht besteht, sind diese **nach Gebrauch zu vernichten**.