23. November 2022
Version 2.02

VISCHER

In Kooperation
VGIch
Vereinigung Gesundheitsinformatik Schweiz

LEITFADEN

ZUR EINFÜHRUNG VON CLOUD-SERVICES IN ÖFFENTLICHEN ORGANEN UND SCHWEIZER SPITÄLERN

Von David Rosenthal, VISCHER AG

Inhaltsverzeichnis

A. Einführung

Will ein öffentliches Organ oder Schweizer Spital Cloud-Services wie etwa M365 von Microsoft einführen, ist aus rechtlicher Sicht nebst einem passenden Vertrag vor allem eine Compliance- und Risikobeurteilung erforderlich. Handelt es sich um ein öffentlich-rechtliches Spital oder Organ, muss in der Regel zusätzlich die Datenschutzaufsicht involviert und ihr das Projekt zur Stellungnahme vorgelegt werden. Die rechtlichen Vorgaben sind in diesem Fall etwas strenger. Der Einsatz von Cloud-basierten Lösungen ist in der Schweiz jedoch auch für öffentlich-rechtliche Spitäler und Organe möglich.

Dieser Leitfaden dient lediglich der Information und stellt keine Rechtsberatung dar. Er beansprucht auch keine Vollständigkeit.[1] Wenn in der Folge wird nur vom "Organ" gesprochen wird, sind damit immer auch Spitäler gemeint.

B. Besonderheiten

Der Einsatz eines Cloud-Services unterscheidet sich rechtlich grundsätzlich nicht von einem IT-Outsourcing, wie es schon seit Jahrzehnten auch von öffentlichen Organen in der Schweiz betrieben wird. Die drei wichtigsten Unterschiede sind, dass (i) die Dienstleister ihren Sitz regelmässig im Ausland haben und von dort auch Leistungen erbringen, (ii) ihre Verträge und Leistungen standardisiert sind und sich immer wieder ändern und (iii) den Kunden teilweise andere Verantwortlichkeiten zukommen als in der Vergangenheit.

Die Diskussion um den Einsatz von Cloud-Services wird nicht immer objektiv und mit ausreichendem Verständnis für Technik und Recht geführt. Das kann die Umsetzung eines Cloud-Projekts erschweren.

Dies sind die in der Praxis wichtigsten Themen für Cloud-Projekte:

- **Abhängigkeit und Geschäftsfortführung:** Wie weit werden wir von unserem Cloud-Provider abhängig und wie gehen wir damit um? Haben wir einen Plan B? Was passiert, wenn der Provider uns den "Saft abdreht"? Dies wird bei sachlicher Beurteilung regelmässig als das gewichtigste Risiko betrachtet. Hierunter fallen Themen wie etwa Backup-Konzepte aber auch eine Exit-Strategie und die Evaluation möglicher alternativer Anbieter für den Notfall. Die Notwendigkeit einer raschen Migration von einem Provider zum anderen sollte auch bei der technischen Konzeption berücksichtigt werden (z.B. Einsatz von Container-Technologie). Leider funktionieren jedenfalls die grossen Hyperscaler heute noch sehr unterschiedlich, so dass ein Wechsel nicht einfach ist.

---

[1] Etwaige Updates werden über die VGI und https://www.rosenthal.ch angeboten. Dort kann der Leitfaden auch kostenlos heruntergeladen werden.

- **Ausländischer Behördenzugriff:** Besteht Grund zur Annahme, dass ausländische Behörden auf die in der Cloud-Lösung gespeicherten Patientendaten und sonstigen Personendaten zugreifen werden (sog. *Lawful Access*)? Dies ist das derzeit prominenteste Thema, wird aber leider wenig sachlich diskutiert. Stichworte sind der "US CLOUD Act" und "Schrems II". In der Praxis ist das Risiko in der Regel minim, wenn gewisse Massnahmen getroffen werden. Nach herrschender Ansicht muss das Risiko eines solchen Behördenzugriffs nicht null sein, nach einer Minderheitsmeinung schon. Letztere will jede Bekanntgabe von Daten in Länder ohne angemessenen Datenschutz verbieten, selbst wenn ein nur theoretisches Risiko eines Behördenzugriffs besteht; nach dieser Ansicht sind im Ergebnis die Cloud-Dienste aller drei grossen Hyperscaler verboten.
- **Shared-Responsibility-Modell:** Cloud-Services sind nicht "plug & play". Dem Kunden kommt in der Konfiguration, Steuerung und Nutzung eine erhebliche Eigenverantwortung zur Gewährleistung der Sicherheit und anderer Aspekte einer Lösung zu. Er muss den Provider zudem überwachen (z.B. Prüfung von Audit-Berichten und Logs). Dies verlangt Know-how und Ressourcen, was viele überfordert.
- **Vertrag mit dem Cloud-Provider:** Die Standardverträge der Provider entsprechen normalerweise nicht den Vorgaben des Schweizer Rechts, insbesondere nicht im Bereich des Berufs- und Amtsgeheimnisses. Sie müssen daher angepasst werden, was die Provider ungern tun und in der Regel einige Verhandlungsmacht erfordert. Zum Glück konnte mit gewissen Providern wie Microsoft Standard-Vertragsergänzungen ausgearbeitet werden, mit welchen Cloud-Lösungen sich auch für Beruf- und Amtsgeheimnisträger in der Schweiz einsetzen lassen.[2] Ein Problem bleibt aber der Umstand, dass sich Cloud-Services wie auch die Verträge der Cloud-Provider regelmässig ändern. Hinzu kommt, dass praktisch alle Cloud-Provider bezüglich ihrer Datenbearbeitung nicht wirklich transparent sind, auch in ihren Verträgen sind. Zusagen werden oft nur mündlich gemacht. Ob ein Vertrag für einen Kunden angepasst werden kann, wird in der Regel im Ausland entschieden, was Verhandlungen mühsam macht.
- **Bearbeitung von Daten für eigene Zwecke:** Einigen Cloud-Providern ist es wichtig, Daten ihrer Kunden auch für eigene Zwecke analysieren und sonst bearbeiten zu können (z.B. wie die Mitarbeiter des Kunden die Services nutzen oder für das Training von KI-Systemen). Dies ist datenschutzrechtlich problematisch,

---

[2] Im Falle von Microsoft bietet sich für öffentliche Organe der SIK-Rahmenvertrag an oder aber die Vereinbarung der Vertragsergänzungen M329, M744 bzw. M905 und ggf. M795 sowie die Verwendung des Data Protection Addendums vom September 2022 an (Stand Oktober 2022).

weshalb solche Nutzungen ausgeschlossen oder eingeschränkt werden müssen. Das gilt speziell für öffentlich-rechtliche Spitäler. Über solche Nutzungen ist zudem zu informieren.

- **Überwachung von Mitarbeitern:** Immer mehr Cloud-Services bieten nebst der Kernfunktionalität auch Funktionen an, mit denen ein Unternehmen seine Mitarbeiter überwachen kann. Dies kann gegen den Datenschutz verstossen, da eine Verhaltensüberwachung am Arbeitsplatz an sich verboten ist. Es ist daher bei der Implementation und Konfiguration von Cloud-Services darauf zu achten, welche Funktionen aktiviert sind oder werden.
- **Informationssicherheit:** Die von den grossen Hyperscalern betriebene Informationssicherheit wird allgemein als hochstehend bewertet. Allerdings kann sie nur wirken, wenn der Kunde die Cloud-Services auch von seiner Seite her entsprechend konfiguriert und nutzt. Dies ist möglich, wird aber im Aufwand und der Komplexität oft unterschätzt. Cloud-Services sind zudem in der Regel aus dem Internet von jedem Punkt aus erreichbar, d.h. es sind zusätzliche Sicherheitsvorkehrungen zu treffen.
- **Berufs- und Amtsgeheimnis:** Es gibt zwar Stimmen, die der Ansicht sind, ein Berufs- oder Amtsgeheimnisträger darf geschützte Daten nur mit der Einwilligung der betreffenden Personen oder mit einer amtlichen Entbindung einem Cloud-Provider zugänglich machen, jedenfalls dann, wenn dieser seinen Sitz im Ausland hat. Dies entspricht aber nicht der herrschenden Ansicht. Eine generelle "Entbindung" vom Berufs- oder Amtsgeheimnis für die Nutzung der Cloud durch eine vorgesetzte Behörde ist nach der hier vertretenen Ansicht sowieso nicht möglich. Wesentlich ist, dass eine angemessene Informationssicherheit gewährleistet ist und es keinen Grund zur Annahme eines ausländischen Behördenzugriffs gibt. Hierzu gehören auch bestimmte technische und organisatorische Vorkehrungen, wie z.B. bestimmte Vertragsklauseln zum Schutz der eigenen Daten. Teilweise wird auch vertreten, dass bestimmte Amtsgeheimnisse einem erhöhten Schutz (gegenüber "normalen" Amtsgeheimnissen) unterliegen; nach der hier vertretenen Ansicht ist diese Unterscheidung künstlich und nicht zielführend – es muss so oder so eine Risikobeurteilung im Einzelfall vorgenommen werden. In der Praxis wird üblicherweise nicht unterschieden, sondern stattdessen ein Schutzniveau gewählt, dass dem höchsten Schutzbedarf der jeweils bearbeiteten Daten entspricht. Damit eine Auslagerung in die Cloud rechtlich per se ausgeschlossen ist, müsste eine spezialgesetzliche Regelung dies so ausdrücklich vorsehen; das kommt in der Regel nicht vor.
- **Rechtsgrundlagen, Verhältnismässigkeit:** Öffentliche Organe und Spitäler, die öffentlich-rechtlicher Natur sind oder mindestens einen öffentlichen Leistungsauftrag haben, unterstehen kan-

tonalem Recht – oft sogar demjenigen mehrerer Kantone. Darum müssen sie das kantonale Datenschutzrecht einhalten, d.h. über eine gesetzliche Grundlage für das Vorhaben verfügen, es muss verhältnismässig sein und die sonstigen Vorgaben des kantonalen Datenschutzrechts müssen eingehalten sein. Ferner müssen in vielen Kantonen heiklere Projekte der Datenschutzbehörde zur "Vorabkontrolle" vorgelegt werden. Die gesetzliche Grundlage bezieht sich auf den Geschäftsprozess bzw. die Datenbearbeitung, die mit dem Cloud-Service unterstützt werden soll. Diese muss aufgezeigt werden, ebenso die Einhaltung der datenschutzrechtlichen Vorgaben und dass mit dem Vorhaben keine hohen Risiken (d.h. Nachteile) für betroffene Personen (Patienten, Mitarbeiter etc.) verbunden sind (sogenannte Datenschutz-Folgenabschätzung oder DSFA). Beides gilt auch dann, wenn kein Cloud-Service genutzt wird. In Bezug auf den Grundsatz der Verhältnismässigkeit muss ferner dargelegt werden, warum das Organ oder Spital keine (aus datenschutzrechtlicher Sicht) weniger problematische Alternative zum Cloud-Service hat und auf die Nutzung der Cloud angewiesen ist. Diese Überlegungen und Abklärungen sind zu dokumentieren. Zur Vorabkontrolle siehe weiter hinten.

Im Anhang zu diesem Merkblatt sind die *fünf Fragen* formuliert, welche sich die Leitung eines Organs im Zusammenhang mit dem Gang in die Cloud aus strategischer Sicht bzw. projektbezogen stellen und eine gute Antwort haben sollte, bevor es für den Betrieb wichtige oder heikle Anwendungen oder Daten in die Cloud verlegt.

Aus rechtlicher Sicht müssen die obigen Themen und weiteren rechtlichen Voraussetzungen für jedes Cloud-Projekt geprüft und das Ergebnis der Prüfung dokumentiert werden. Ferner ist eine umfassende Beurteilung der mit dem Cloud-Projekt verbundenen Risiken erforderlich.

C. Rollen

Für jedes Cloud-Projekt gibt es verschiedene Stakeholder, welche beteiligt werden sollten. Dies sind typischerweise:

- **Projekteigner:** Er definiert die geschäftlichen Vorgaben für das Vorhaben, ist für das Vorhaben verantwortlich und "sponsert" es, finanziert es und trifft auch die Geschäftsentscheide, soweit diese nicht einem höheren Leitungsorgan überlassen wird oder werden muss. Der Projekteigner kommt üblicherweise aus dem Fach. Er definiert auch den Umgang mit den vom Vorhaben betroffenen Daten und ist daher auch derjenige, der dafür verantwortlich ist und die diesbezüglichen Risikoentscheide trifft. Es ist entscheidend, dass es jeweils eine für die Lösung und die damit bearbeiteten Daten verantwortliche Stelle gibt.
- **Projektleiter:** Er führt die Umsetzung des Projekts (Projektmanagement) und koordiniert die Aktivitäten.

- **Informatik:** Sie definiert mit dem Projekteigner die Lösung und die benötigten Cloud-Services, bereitet das Vorhaben vor, setzt es um und betreibt es. Sie liefert den anderen Stellen die nötigen Informationen.
- **CISO:** Der Beauftragte für Informationssicherheit prüft das Vorhaben aus Sicht der Informationssicherheit und definiert die nötigen Massnahmen, welche die anderen Stellen umsetzen.
- **Beschaffung:** Die mit der Beschaffung betraute Stelle koordiniert die Verhandlungen mit dem Provider (einschliesslich Einhaltung von etwaigen beschaffungsrechtlichen Vorgaben), regelt die kommerziellen und weiteren vertraglichen Aspekte, letzteres mit der zuständigen Person aus dem Rechtsdienst.
- **Recht:** Üblicherweise eine Person aus dem Rechtsdienst ist für die Prüfung der rechtlichen Vorgaben verantwortlich und kümmert sich inhaltlich um die Vertragsprüfung.
- **Datenschutz:** Die mit der internen Datenschutzstelle betraute Person begleitet das Projekt aus der Sicht des Datenschutzes, führt die DSFA und die Compliance-Prüfung aus datenschutzrechtlicher Sicht durch.
- **Leitungsorgan:** Es entscheidet über die Umsetzung des Vorhabens und die Live-Setzung der Lösung. Es ist ferner der Risikoträger, d.h. entscheidet über die mit dem Vorhaben verbundenen, aber als tragbar beurteilten Risiken. Es ist dies in der Regel die Geschäftsleitung, der Verwaltungsrat/Spitalrat oder in einem Kanton z.B. der Regierungsrat. Die Stufe ergibt sich nach den internen Zuständigkeitsvorgaben, wobei Datenschutzbehörden bei Vorhaben mit hohen Risiken mitunter eine Eskalation auch der Entscheide verlangen (z.B. VR statt GL).
- **Aufsichtsbehörden:** Sie prüfen das Vorhaben nach den kantonalen Vorgaben. In der Regel ist dies die Aufsichtsbehörde für den Datenschutz, aber in gewissen Kantonen können auch weitere Stellen involviert sein. Die Prüfung resultiert typischerweise in einer Stellungnahme, die Empfehlungen oder Anordnungen enthalten kann. Mindestens die Datenschutzbehörden erklären in der Regel nur, ob sie Einwände haben, nehmen dem Organ die Risiko- und Compliance-Entscheide jedoch nicht ab.

In kleineren Organisationen kann dieselbe Person mit mehreren dieser Rollen betraut sein oder eine Aufgabe wird an eine externe Stelle delegiert (z.B. die Sicherstellung der Informationssicherheit, Informatikaufgaben oder die Projektleitung). Bei Bedarf können auch externe Berater beigezogen werden. Die Oberleitung und die Geschäftsentscheide müssen jedoch in der Organisation verbleiben.

D. Workstreams

Um ein Cloud-Projekt erfolgreich umzusetzen, sind verschiedene Workstreams erforderlich, die parallel zueinander ablaufen. Eine mögliche Aufteilung ist die Folgende:

- **Stream Technik:** Basierend auf den Vorgaben des Projekteigners werden die technischen Grundlagen und das Projekt erarbeitet, es wird Implementierung und der Betrieb geplant und umgesetzt. Es werden die technischen Massnahmen aus den Streams Informationssicherheit, Compliance & Risiko und Governance umgesetzt.
- **Stream Informationssicherheit:** Das Vorhaben wird auf die Anforderungen der Informationssicherheit hin (einschliesslich Geschäftsfortführung) geprüft und es werden die Massnahmen definiert, um diese hinreichend sicherzustellen. Massnahmen der Informationssicherheit können auch aus anderen Streams resultieren. Die Massnahmen werden umgesetzt oder deren Umsetzung wird überwacht.
- **Stream Compliance & Risiko:** Hier wird das Vorhaben zum Einen auf die Einhaltung der weiteren Anforderungen (einschliesslich Datenschutz und einschliesslich der Prüfung des Risikos eines ausländischen Behördenzugriffs) geprüft. Der Projektleiter leitet diese Prüfung, erhält seinen Input jedoch von den jeweiligen Stakeholdern (z.B. dem Rechtsdienst). Zum Anderen wird eine Risikobeurteilung des gesamten Vorhabens unter Beteiligung aller Stakeholder durchgeführt. Ihr Ergebnis fliesst später in den Stream Geschäftsentscheid. Aus beiden Prüfungen resultieren in der Regel (weitere) zu treffende Massnahmen.
- **Stream Governance:** Es werden die Massnahmen definiert bzw. aufgegriffen, die aus den anderen Streams resultieren und nicht technischer Natur sind oder die Informationssicherheit betreffen (z.B. Anbieterprüfung, personelle Massnahmen). Die Massnahmen werden umgesetzt oder deren Umsetzung wird überwacht.
- **Stream Vertrag:** Der Vertrag mit dem Provider wird ausgehandelt (kommerziell, rechtlich) und abgeschlossen. Es werden dabei die Vorgaben aus dem Stream Compliance & Risiko berücksichtigt.
- **Stream Aufsicht:** Soweit das anwendbare Recht vorschreibt, dass das Vorhaben einer oder mehreren Aufsichtsbehörden in Form eines Dossiers vorgelegt werden muss, wird hierzu ein eigener Stream gebildet. Daraus können Massnahmen zur Umsetzung resultieren.
- **Stream Geschäftsentscheid:** Jedes Vorhaben benötigt in der Regel zwei oder mehrere Geschäftsentscheide, dies basierend auf den Ergebnissen aus den anderen Streams.

- **Projektleitung:** Hier werden alle Streams koordiniert und die Resultate der einzelnen Streams werden zusammengetragen und eine Projektdokumentation geschaffen.

Eine mögliche Zuteilung der Streams und Rollen ist die Folgende (nach dem RACI-Modell):

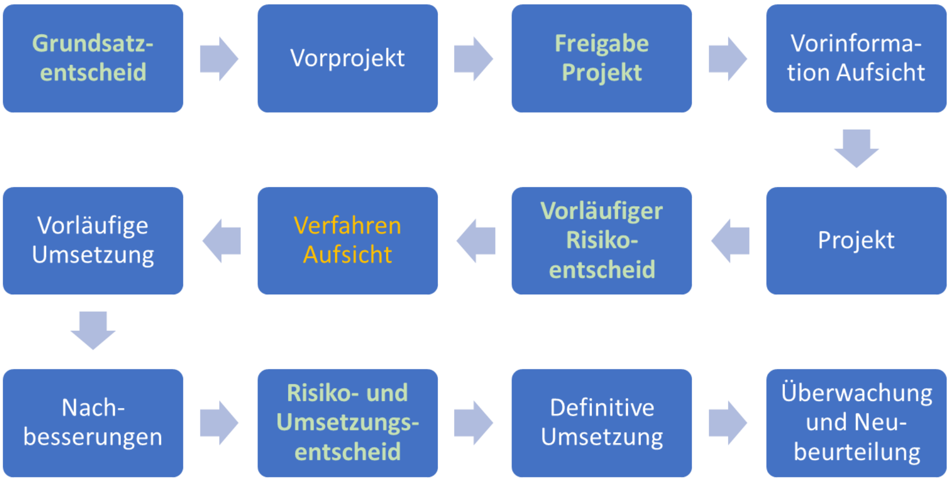
	Projekteigner	Projektleiter	Informatik	CISO	Beschaffung	Recht	Datenschutz	Leitungsorgan	Aufsichtsbehörden
Technik	A	I	**R**	C	C	C	C	I	I
Informationssicherheit	A	I	C	**R**	-	C	C	I	I
Compliance & Risiko	A	**R**	C	C	C	C	C	I	I
Governance	A	**R**	C	C	-	C	C	I	I
Vertrag	A	I	C	C	**R**	C	C	I	I
Aufsicht	A	I	C	C	-	**R**/C		I	C
Geschäftsentscheid	**R**	C	C	C	C	C	C	A	I
Projektleitung	A	**R**	C	C	C	C	C	I	-

Legende: R = responsible, A = accountable, C = consulted, I = informed

Im Stream "Aufsicht" wird je nach Aufsichtsbehörde die Datenschutzstelle oder der Rechtsdienst federführend (R) sein. Die eigentliche geschäftliche Verantwortlichkeit liegt letztlich beim Projekteigner und für die Geschäftsentscheide beim Leitungsorgan.

E. Vorgehensweise zur Einhaltung der rechtlichen Vorgaben

Die nachfolgende Beschreibung stellt dar, wie vorgegangen werden kann, damit die rechtlichen Vorgaben im Rahmen eines Cloud-Vorhabens eingehalten werden. Sie setzt nicht auf einer bestimmte Projekt-Methodik wie HERMES auf, sondern erklärt aus Sicht des Rechts und Risikos, wie sinnvollerweise vorzugehen ist (zum Abgleich mit HERMES vgl. die Darstellung im Anhang). Die Vorgehensweise ist selbstverständlich nicht fix und muss auf die jeweilige Projekt-Methodik zugeschnitten werden. Der Ablauf ergibt sich aber aus gewissen Sach- und Rechtszwängen.



1. **Grundsatzentscheid:** Die meisten Organisationen betrachten den Gang in die Cloud als strategischen Entscheid, der einen entsprechenden Grundsatzentscheid des Leitungsorgans erfordert. Hierbei wird kein konkretes Vorhaben beschlossen, sondern das Verständnis geschaffen, dass gewisse Informatikbedürfnisse sich in Zukunft nur noch mit Cloud-basierten Lösungen befriedigen lassen werden, diese Cloud-Lösungen oft von ausländischen Anbietern stammen und eine Datenbearbeitung im Ausland erfolgen kann, auch wenn es sensible Daten (namentlich Patientendaten) betrifft. Experten sind sich allerdings einig, dass öffentliche Organe und Spitäler wie auch Unternehmen der Privatwirtschaft diesbezüglich keine völlig freie Wahl haben werden. Das betrifft Infrastrukturanwendungen wie die Büroautomation wie auch spezialisierte Anwendungen z.B. zur Auswertung bestimmter Datenkategorien. Dies erfordert einen Bewusstseinsprozess des Leitungsorgans, welcher zur Folge haben kann, dass sich das Leitungsorgan angesichts der zahlreichen Schlagzeilen zu Cloud-Themen (z.B. Stichwort "CLOUD Act") unwohl fühlt und daher sichergestellt haben will, dass etwaige Cloud-Vorhaben mit aller Sorgfalt und rechtskonform durchgeführt werden. Hier bietet sich an, dem Leitungsorgan wie vorliegend aufzuzeigen, wie die Organisation dies für Cloud-Vorhaben sicherstellen will um diesbezüglich einen Grundsatzentscheid zum "Gang in die Cloud" zu treffen. Alternativ kann dieser Grundsatzentscheid im Rahmen eines ersten Projekts (z.B. Einführung von M365 oder Teilen davon) gefällt werden.

2. **Vorprojekt:** Üblicherweise gibt es für jedes Cloud-Vorhaben ein Vorprojekt, in welchem abgeklärt wird, was beschafft werden soll und ob es basierend auf den sofort verfügbaren Angaben des Providers punkto Abdeckung der betrieblichen Bedürfnisse, Technik, Informationssicherheit und Recht überhaupt in Frage kommen kann. Die rechtliche Vorprüfung darf sich auf Plausibilität

beschränken, etwa ob bereits andere vergleichbare Organisationen den Cloud-Service einsetzen oder der Provider einem Fragebogen zufriedenstellende Antworten liefert. Der Provider sollte gefragt werden, ob der Vertragspartner des Organs eine Gesellschaft im EWR oder der Schweiz sein wird, ob er sich sonst zur Einhaltung der DSGVO (englisch: GDPR) oder des Schweizer Rechts verpflichtet und ob die Daten im EWR oder der Schweiz gespeichert werden. Der erste und letzte Punkt ist besonders wichtig. Die rechtliche Vorprüfung sollte allerdings nicht zu schwer gewichtet werden; erfahrungsgemäss finden sich mit etablierten Providern meistens über kurz oder lang Lösungen zur Einhaltung der rechtlichen Vorgaben. Diese werden im nachfolgenden Projekt erarbeitet. Im Rahmen dieses Vorprojekts wird ein Projektantrag für die Prüfung und ggf. Umsetzung des Cloud-Vorhabens verfasst, die dann im Rahmen eben dieses Projekts stattfindet, d.h. in einer Phase, in welcher die Voraussetzungen für eine Umsetzung des Cloud-Vorhaben definiert wird.

3. **Freigabe Projekt:** Basierend auf dem Bericht des Vorprojekts und Projektantrag wird das Leitungsorgan die Durchführung des Projekts freigeben. Die Umsetzung ist damit noch nicht beschlossen. Ein Entscheid ist trotzdem erforderlich, weil die Vorbereitung eines Cloud-Vorhabens mit den nötigen Abklärungen technischer, organisatorischer und rechtlicher Art einen gewissen Aufwand mit sich bringt, der entsprechende Mittel erfordert. Dieses Projekt kann mehrere Monate beanspruchen. Es resultiert eine Projektdokumentation, die als Basis für die weiteren Entscheide dient. Diese Freigabe muss nicht zwingend auf oberster Leitungsstufe erfolgen. Sie hat eher "verfahrensrechtlichen" Charakter (Freigabe der Mittel); ein Cloud-Risiko wird damit nicht eingegangen, von den Risiken, die mit ersten technischen Tests verbunden sind, einmal abgesehen.

4. **Vorinformation Aufsichtsbehörde(n):** An dieser Stelle empfiehlt es sich, etwaige Aufsichtsbehörden über das Projekt zu informieren, ihnen kurz das Vorgehen zu erläutern, das geplante Format (und die Tiefe) der Dokumentation und etwaige besondere Bedürfnisse abzufragen. Zwingend ist dies jedoch nicht. Eine eigentliche Beurteilung wird sie erst vornehmen wollen, wenn ihr alle Unterlagen vorliegen.

5. **Projekt:** Im Rahmen des Projekts werden entsprechend den vorstehend erläuternden Streams (i) die technische und organisatorische Umsetzung des Vorhabens (sowohl bezüglich Implementation inklusive Migration als auch Betrieb) vorbereitet, (ii) die Massnahmen zur Informationssicherheit werden festgelegt und eine diesbezügliche Risikobeurteilung wird durchgeführt, (iii) es werden die vertraglichen Grundlagen geschaffen und (iv) es findet die Compliance-Prüfung und eine generelle Risikobeurteilung

statt. Im Rahmen der Compliance-Prüfung kann aus Sicht des Datenschutzes und Arbeitsrechts angezeigt sein, weitere interne Stellen (z.B. HR, Vertretung von Mitarbeitern) zu begrüssen. Die Projektleitung stellt sicher, dass die Ergebnisse aus den Streams dokumentiert und in entsprechenden Dokumenten zusammengeführt werden.

Ziel ist aus *rechtlicher* Sicht und für die Zwecke eines Risikoentscheids eine Dokumentation erstellt werden, welche einerseits dem Leitungsorgan einen ersten Entscheid für die Umsetzung des Projekts inklusive Beurteilung und Abnahme der Risiken ermöglicht und andererseits den Aufsichtsbehörden erlaubt, die Einhaltung der gesetzlichen Vorgaben und die vorgenommene Risikobeurteilung zu prüfen (um zu entscheiden, ob sie Anpassungen verlangen oder intervenieren müssen). Darin sollte daher in der Sache enthalten sein:

- **Beschreibung** des Vorhabens, einschliesslich einer Erläuterung, warum das Vorhaben nötig ist und welche Alternativen geprüft und verworfen wurden und welche Massnahmen zur Sicherstellung der Informationssicherheit, des Daten- und Geheimnisschutzes, der Geschäftsfortführung und sonst zum Schutz der Interessen des Organs vorgesehen sind. Für Details kann auf weitere Unterlagen verwiesen werden.

  Als Teil dieser Beschreibung wird eine sog. Schutzbedarfsanalyse (**Schuban**) erwartet, d.h. einer Darstellung, welche Daten, Funktionen und Komponenten zum Einsatz kommen und wie hoch ihr Bedarf an Schutz punkto Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit ist (z.B. bei Amtsgeheimnisdaten wird der Bedarf an Vertraulichkeit sehr hoch sein). Ist der Schutzbedarf in einem Punkt mehr als "normal" (was in Cloud-Projekten jedenfalls bezüglich der Vertraulichkeit meistens der Fall ist), muss in der Regel eine Risikoanalyse durchgeführt und anhand ihres Ergebnisses entsprechende Massnahmen zur Sicherung des Schutzziels festgelegt werden. In der Praxis läuft es in Cloud-Projekten oft so, dass für alle Daten und Komponenten ein Schutzstandard gewählt wird, der so oder so hoch genug ist. Sollte jedoch eine Cloud-Lösung ausnahmsweise keine heiklen Daten bearbeiten und auch sonst keinen hohen Schutzbedarf ausweisen, kann die Lösung mit sehr viel geringeren Anforderungen umgesetzt werden.

- Der mit dem Provider vorgesehene **Vertrag** mit den nötigen standardisierten oder individuellen Zusatzvereinbarungen zum Schutz der Daten und Einhaltung der rechtlichen Vorgaben. Dieser Vertrag muss nicht unterzeichnet sein, aber Aufsichtsbehörden wollen sehen, welche Regelungen vorgesehen sind und diese prüfen können. Die Verhandlungen dazu finden im Rahmen des Projekts statt, wobei seitens der Provider in aller Regel mit standardisierten Zusatzvereinbarungen gearbeitet wird, die im Rahmen früherer Projekte anderer vergleichbarer Kunden erarbeitet wurden.

Im Falle von Microsoft wird ein öffentlich-rechtliches Spital oder (kantonales) öffentliches Organ entweder auf die Verträge der SIK abstellen oder eine analoge Vereinbarung, die Microsoft mit verschiedenen Universitätsspitälern abgeschlossen hat, verwenden. Private Spitäler werden die Zusatzvereinbarungen M329, M744 und ggf. M795 vereinbaren, nebst dem DPA vom September 2022. Ferner wird sich das Leitungsorgan ein vertrauliches Microsoft-Papier zum Umgang mit Mitarbeiterdaten vorlegen lassen müssen, da dieser Umgang in den Verträgen nicht sehr detailliert beschrieben ist.

Mit anderen Hyperscalern müssen nebst den Standardverträgen in der Regel ähnliche Vertragsergänzungen abgeschlossen werden. Die darin zu regelnden Punkte werden nachfolgend noch dargelegt.

Zu den zu treffenden Massnahmen vgl. auch hinten.

- Beurteilung der **Informationssicherheits-Risiken** inklusive der getroffenen oder noch zu treffenden Massnahmen zur Minimierung oder Eliminierung dieser Risiken; hierbei darf nicht nur der Cloud-Service (und damit die Massnahmen seitens des Providers) betrachtet werden, sondern auch die Sicherheit und Massnahmen seitens des Organs, einschliesslich die korrekte Konfiguration und Bedienung des Cloud-Services (hierfür verfügen die meisten Organisationen oder Berater über etablierte Vorgehensweisen; sie werden hier daher nicht näher erläutert). In der Praxis ist zuweilen auch von einer "technischen" Risikobeurteilung die Rede.
- Beurteilung des **Risikos eines ausländischen Behördenzugriffs**. Dies gehört an sich zu den Risiken der Informationssicherheit, wird aber regelmässig nach einer separaten Methodik beurteilt, weil hier auch rechtliche Aspekte zu berücksichtigen sind. Verbreitet ist hierbei die vom Autor dieses Papiers entwickelte Methode, die als Open Source[3] kostenlos mit ausführlicher FAQ[4] zur Verfügung steht. Sie wird oft im Rahmen eines Workshops mit allen Stakeholdern durchgeführt. Es ist dieselbe Methode, die der Kanton Zü-

---

[3] https://www.rosenthal.ch/downloads/Rosenthal_Cloud_Lawful_Access_Risk_Assessment.xlsx.

[4] https://www.rosenthal.ch/downloads/Rosenthal-LA-method-FAQ.pdf (nur auf Englisch).

rich zum Standard für seine Cloud-Projekte erklärt hat und die von der Bundeskanzlei in ihrem Bericht zu den Rechtsgrundlagen der Cloud-Nutzung durch die Bundesverwaltung als "gute Praxis" bezeichnet wurde.

- Beurteilung der **Datenschutz-Risiken.** In der Praxis geht es um eine sog. Datenschutz-Folgenabschätzung (**DSFA**). Hierbei wird geprüft, ob mit der geplanten Datenbearbeitung bzw. dem Cloud-Vorhaben für die betroffenen Personen (z.B. Patienten, Einwohner, Mitarbeiter) die Gefahr von Schäden oder sonstigen Nachteilen oder das Risiko einer Verletzung von Grundrechten (d.h. der Bearbeitungsgrundsätze und dem Grundsatz der Gesetzmässigkeit einer jeden Datenbearbeitung) besteht, welche Massnahmen getroffen werden (damit es nicht dazu kommt) und welches Restrisiko verbleibt. Es darf vereinfacht gesagt nicht hoch sein. Die Prüfung ist für jede Datenbearbeitung zu dokumentieren. Unter dem revidierten DSG wird eine DSFA ab September 2023 auch für private Spitäler Pflicht.
- Beurteilung der sonstigen **rechtlichen Vorgaben**. Hierbei sind in erster Linie Vorgaben des Datenschutzes und des Schutzes des Berufs- und Amtsgeheimnisses zu treffen, aber im weiteren Sinne auch Vorgaben, die sich aus einer guten Corporate Governance geben, welche das Leitungsorgan bzw. die Organisation verpflichtet, Risiken für die eigene Organisation zu erkennen und angemessen damit umzugehen. In der Praxis bietet sich eine Beurteilung anhand eines standardisierten Anforderungskatalogs unter Mitwirkung der einzelnen Stakeholder an (dazu hinten), nötigenfalls unter Beizug eines Spezialisten. Können bestimmte Vorgaben nicht oder nicht vollständig eingehalten werden, kann eine Risikobeurteilung aufzeigen, ob sich das Vorhaben trotzdem umsetzen lässt. Dies wiederum ist ein Risiko- bzw. Geschäftsentscheid, welches der Projekteigner und letztlich das Leitungsorgan treffen muss.
- Beurteilung der **weiteren Risiken**. Nebst den Risiken der Informationssicherheit können Cloud-Vorhaben (wie auch andere IT-Vorhaben) weitere Risiken bergen, denen sich eine Organisation bewusst sein sollte. Zu nennen ist hier beispielsweise das Abhängigkeitsrisiko, das im Falle einer Cloud-basierten Lösung insofern höher ist, als ein Organ in erhöhtem Masse als beim "on prem"-Betrieb einer Lösung davon abhängig ist, dass der Provider seine Leistungen erbringt. Diese Risiken werden ebenfalls typischerweise in einem Workshop unter Beteiligung aller Stakeholder zu Handen des Leitungsorgans beurteilt und dokumentiert.

Die Ergebnisse aus den einzelnen Prüfungsschritten bzw. Komponenten werden vorzugsweise in einem Dokument mit entsprechenden Anhängen zusammengefasst. In der Praxis ist in diesem Zusammenhang häufig von einem Konzept für Informationssicherheit und Datenschutz (**ISDS-Konzept**) die Rede; je nach lokalem Recht und lokaler Sitte ist hierzu sogar ein bestimmtes Format vorgeschrieben. Die Projekt-Methodik HERMES definiert ebenfalls, was der Inhalt eines ISDS-Konzepts sein muss. Nach der hier vertretenen Ansicht greifen die ISDS-Konzepte klassischer Machart zu kurz, da der Blick für eine Beurteilung eines Cloud-Einsatzes ggf. über die Informationssicherheit und den Datenschutz hinaus geöffnet werden sollte.

Die Projekt-Phase ist jene Phase eines Cloud-Vorhabens, in welcher jedenfalls aus Sicht des Rechts und des Risikos die meisten Arbeiten stattfinden. Hier werden die Grundlagen geschaffen. Sie ist aber auch aus Sicht der anderen Streams anspruchsvoll, vor allem, wenn es sich um das erste Cloud-Projekt handelt, da hier auch die technischen Grundlagen erarbeitet und die Massnahmen definiert (aber noch nicht notwendigerweise umgesetzt werden), die das Vorhaben später absichern sollen. Dazu ist es aber erforderlich, sie zu kennen und sie nötigenfalls zu testen. Diese Phase kann mehrere Monate in Anspruch nehmen.

6. **Vorläufiger Risikoentscheid:** Basierend auf der Dokumentation aus dem vorherigen Schritt, einschliesslich der darin ausgewiesenen Risiken und etwaigen Anträge betreffend weitere Massnahmen, trifft das Leitungsorgan einen vorläufigen Risikoentscheid, d.h. es entscheidet, ob es die Risiken als tragbar erachtet, welche allfällig weiteren Massnahmen erforderlich sind, ob das Vorhaben etwaigen Aufsichtsbehörden vorgelegt werden kann und ob mit der Umsetzung einstweilen weitergemacht werden soll. In öffentlichen Organen kann dem Leitungsorgan allenfalls ein Gremium vorgelagert sein, welches das Vorhaben vorberät. Dies ist auf der Zeitachse zu berücksichtigen.

7. **Verfahren Aufsichtsbehörde(n):** Soweit Aufsichtsbehörden konsultiert oder deren Zustimmung eingeholt werden muss, geschieht dies unter Vorlage der Projektdokumentation. Die Prüfung der Aufsichtsbehörden kann je nach Komplexität und Auslastung der Behörde einen oder mehrere Monate dauern. Sie wird in der Regel erst beginnen, wenn die Projektdokumentation einigermassen vollständig ist, auch wenn die Verträge noch nicht unterzeichnet sind. Im Rahmen des Verfahrens können Besprechungen und weitere Eingaben nötig sein, um Fragen der Aufsichtsbehörden zu beantworten.

   Sieht das kantonale Recht eine Vorabkontrolle durch die Datenschutzbehörde vor, wird das Verfahren üblicherweise mit einer Stellungnahme abgeschlossen, welche Empfehlungen oder Vorgaben zum Vorhaben enthält. Das Organ muss Stellung nehmen, ob es diese Empfehlungen umsetzen will oder nicht, da die Verantwortung für die Datenschutzkonformität letztlich bei ihm bleibt; die Datenschutzbehörden sind in aller Regel sehr risikoavers und werden sich hüten, für Cloud-Projekte einen "Persil-Schein" auszustellen, sondern den Entscheid letztlich dem Organ überlassen (und hierbei mitunter verlangen, dass er vom obersten Leitungsorgan getroffen wird). Sie wenden für die Prüfung u.a. das Merkblatt "Cloud-spezifische Risiken und Massnahmen" von Privatim an[5], haben aber teilweise aber auch eigene Anforderungen definiert oder daraus in konkreter Form abgeleitet. Will das Organ eine empfohlene oder verlangte Massnahme nicht umsetzen, muss die Datenschutzbehörde in der Regel entscheiden, ob sie angesichts der damit verbundenen Risiken dagegen rechtlich vorgehen will oder nicht; bei Cloud-Vorhaben ist uns kein Fall bekannt, wo eine Datenschutzbehörde das trotz Kritik am Vorhaben getan hat. Die Einzelheiten dieses Verfahrens sind im kantonalen Recht geregelt; finden die Bestimmung mehrerer Kantone Anwendung, weil ein Spital Leistungsaufträge aus verschiedenen Kantonen hat, wird in der Regel nur die Datenschutzbehörde des Sitzkantons konsultiert (geregelt ist dies aber nirgends).

8. **Vorläufige Umsetzung:** Je nach Einschätzung der Situation kann mit den Umsetzungsarbeiten basierend auf dem vorläufigen Risikoentscheid im Bewusstsein weitergemacht werden, dass von Seiten der Aufsichtsbehörden noch Einwände erfolgen können und Nachbesserungen erforderlich sein werden. Daher macht es Sinn, eine vorläufige Umsetzung mit der jeweiligen Aufsichtsbehörde abzusprechen. Soweit für die weiteren Arbeiten erforderlich, werden an diesem Punkt oft erste Bestellungen vorgenommen. Die Möglichkeit für weitere Vertragsanpassungen und einen Abbruch der Übung, basierend auf dem Entscheid der Aufsichtsbehörden, sollte aber vorbehalten werden, soweit dies möglich ist.

9. **Nachbesserungen:** Je nach dem Feedback aus den Verfahren der Aufsichtsbehörden sind noch Nachbesserungen am Vorhaben umzusetzen.

10. **Definitiver Risiko- und Umsetzungsentscheid:** Steht der definitiven Umsetzung des Cloud-Vorhabens nichts mehr im Weg, kann auch der entsprechende definitive Risiko- und Umsetzungsentscheid durch das Leitungsorgan erfolgen. Allenfalls wird es sich noch einen separaten Entscheid betreffend "Go Live" vorbehalten, falls es dies von der Erfüllung weiterer Massnahmen abhängig machen will. Mit dem Entscheid werden in der Praxis auch

---

[5] https://www.privatim.ch/de/uberarbeitetes-privatim-merkblatt-cloud-spezifische-risiken-und-massnahmen-2/.

allfällige Entscheide zur Umsetzung aufgrund der Empfehlungen der Aufsichtsbehörde(n) getroffen (z.B. falls diese verlangen, dass gewisse Abklärungen getroffen werden müssen, über die zu entscheiden ist). In diversen Kantonen haben die Datenschutzbehörden bisher verlangt, dass der definitive Risiko- und Umsetzungsentscheid vom jeweils obersten Leitungsorgan des Spitals oder anderen öffentlichen Organs getroffen wird (also vom Verwaltungsrat, Spitalrat oder bei Kantonen vom Regierungsrat). Die Entscheide werden aber in der Regel von unteren Gremien vorbereitet oder "vorentschieden".

11. **Definitive Umsetzung:** Es erfolgt die Umsetzung einschliesslich der im Rahmen der Compliance-Prüfung und Risiko-Beurteilung definierten Massnahmen.
12. **Überwachung und Neubeurteilung:** Die Risiko-Beurteilung und Abnahme der Risiken durch das Leitungsorgan ist bei Cloud-Vorhaben keine einmalige Angelegenheit, sondern muss in periodischen Abständen (i.d.R. alle drei bis fünf Jahre) oder im Falle von Risiko-erhöhenden Entwicklungen wiederholt werden. Ferner ist die Umsetzung der Massnahmen zu überwachen. Die Massnahmen ihrerseits sehen diverse Formen der Überwachung des Cloud-Services, des Providers und der Entwicklungen vor, welche der Risikobeurteilungen zugrunde gelegen haben. Hierzu empfiehlt sich ein periodischer Bericht an das Leitungsorgan im Rahmen des IKS (i.d.R. jährlich).

Diese Vorgehensweise ist mit der von vielen öffentlichen Institutionen verwendeten HERMES-Projektmethode kompatibel. Der Abgleich zum HERMES-Phasenmodell ist im Anhang erläutert.

F. Prüfungen aus rechtlicher Sicht

Die Prüfungen aus rechtlicher Sicht müssen verschiedene Aspekte abdecken:

- **Vorgaben des Datenschutzes:** Dies betrifft einerseits die Zulässigkeit der Datenbearbeitung als solches (d.h. des Geschäftsprozesses, der mit dem Vorhaben unterstützt werden soll) und andererseits die mit dem Cloud-Service verbundene Auslagerung der Datenbearbeitung an den Provider (einschliesslich der damit ggf. verbundenen Bekanntgabe von Personendaten ins Ausland und Bearbeitung von Personendaten für eigene Zwecke des Providers).
- **Vorgaben des Berufs- und Amtsgeheimnisses:** Dies betrifft vor allem die Tatsache, dass dem Provider (und seinen Mitarbeitern) Zugang zu geheimnisgeschützten Daten gewährt wird und sich dieser ggf. im Ausland befindet, wo die Daten einem mehr oder weniger wahrscheinlichen Zugriff durch ausländische Behörden ausgesetzt sind. Zu berücksichtigen ist, dass das Berufs- und Amtsgeheimnis mit dem Datenschutz nicht deckungsgleich ist

(insbesondere, falls Daten juristischer Personen betroffen sind, die der Datenschutz nicht oder nicht mehr lange schützt und dies nicht durch eine Spezialnorm kompensiert wird). Selbstverständlich besteht das Risiko einer Geheimnisverletzung auch bei einem Provider im Inland – auch dieser arbeitet mit Mitarbeitern, die sich möglicherweise nicht an die Vorgaben halten. Bei den Hyperscalern wird aber mitunter vertreten, dass die Zahl der beigezogenen Personen ungleich höher ist als bei einem Schweizer Provider. Dem ist entgegenzuhalten, dass bei den Hyperscalern möglicherweise eine grössere Zahl an Prozessen vollautomatisiert abläuft, ohne dass Mitarbeiter überhaupt die Gelegenheit haben, auf die Daten zuzugreifen. In der Regel haben Berufs- und Amtsgeheimnisgeschützte Daten den höchsten Schutzbedarf, sogar noch über besonders schützenswerten Personendaten. Beim Amtsgeheimnis kommt hinzu, dass betroffene Personen sich nicht aussuchen können, dass das öffentliche Organ Daten über sie bearbeitet.

- **Weitere aufsichtsrechtliche Vorgaben:** Bei öffentlichen Organen können je nach Kanton (abgesehen von den hier nicht diskutierten beschaffungsrechtlichen Vorgaben) noch weitere gesetzliche Vorgaben bestehen, die bei der Beauftragung eines Providers zu beachten sind.
- **Gute Cloud Praxis:** Die Leitungsorgane eines Spitals oder öffentlichen Organs sind wie die Leitungsorgane jeder anderen Organisation verpflichtet für eine gute und ordentliche Unternehmensführung zu sorgen. Soll ein Cloud-Vorhaben umgesetzt werden, ist sicherzustellen, dass die damit für die Stakeholder (Eigner, Mitarbeiter, Einwohner, Patienten etc.) verbundenen Risiken erkannt und angemessen behandelt werden. Soweit Restrisiken verbleiben und für die Stakeholder tragbar sind, müssen die zuständigen Organe sie gegenüber den Chancen abwägen und entscheiden, ob sie sie eingehen können und wollen. Um die im Rahmen eines Cloud-Vorhabens typischen Risiken zu eliminieren oder reduzieren, können erfahrungsgemäss eine Reihe von Vorkehrungen getroffen werden. Die Erfüllung dieser Anforderungen der "guten Praxis" sollten im Rahmen der rechtlichen Prüfung ebenfalls beurteilt werden, auch wenn sie nicht (wie etwa bei FINMA-regulierten Finanzinstituten) aufsichtsrechtlich vorgeschrieben sind.

Für die Prüfung der datenschutzrechtlichen Vorgaben haben sich wie bereits erwähnt in der Praxis bestimmte Formen wie die Schuban, die DSFA und ISDS-Konzepte etabliert oder sind sogar gesetzlich oder aufsichtsrechtlich vorgeschrieben, weshalb diese auch im Falle eines Cloud-Vorhabens in dieser Form durchgeführt werden sollen. Die kantonalen Datenschützer wiederum werden sich für ihre Prüfung an das bereits erwähnte Cloud-Merkblatt von Privatim halten[6] und haben teilweise auch eigene, präzisierende oder weitergehende Vorgaben kommuniziert.

Die rechtliche Prüfung kann wie folgt strukturiert werden:

- **Prüfung der einzelnen Datenbearbeitungen.** Diese muss durchgeführt werden, wenn eine neue oder in relevanter Weise geänderte Datenbearbeitung zur Diskussion steht. Die Auslagerung von einem "on prem"-Betrieb in einen Cloud-Betrieb stellt häufig eine solche relevante Anpassung dar, weil sich die Risiken verändern und neue Datenbearbeitungen (z.B. von Mitarbeiterdaten) hinzukommen. Allerdings kann in diesen Fällen (d.h. wo es "nur" um die Verlagerung einer bereits bestehenden Datenbearbeitung in die Cloud) eine reduzierte, auf die Cloud-spezifischen Aspekte beschränkte Datenschutzprüfung durchgeführt werden.

  Es geht dabei um die Prüfung der Rechtsgrundlagen, die Einhaltung etwaiger rechtlicher Einschränkungen und der Bearbeitungsgrundsätze (Transparenz, Zweckbindung, Verhältnismässigkeit etc.) sowie der weiterhin bestehende Möglichkeit der Gewährleistung der Betroffenenrechte. Ferner wird hier der Umstand der Delegation der Datenbearbeitung an den Provider beurteilt, einschliesslich der damit verbundenen Bekanntgabe ins Ausland.

  Sollte der Provider Personendaten des Organs auch für eigene Zwecke bearbeiten und dies überhaupt zulässig sein, so stellt dies ebenfalls eine Datenbearbeitung als solche dar, die hier zu prüfen ist.

  Diese Prüfung wird in der Praxis typischerweise im Rahmen einer DSFA vorgenommen.

- **Risiko eines ausländischen Behördenzugriffs.** Es muss geprüft werden, ob die getroffenen technischen und organisatorischen Massnahmen so wirksam sind, dass sie einen entsprechenden Zugriff mit hinreichender Zuverlässigkeit bzw. Gewissheit verhindern. Dies bedingt u.a. Analyse der Rechtslage in denjenigen Ländern, in denen aufgrund des gewählten Anbieters und der anbieterseitigen Zugriffsmöglichkeiten ein Zugriffsrisiko mindestens theoretisch besteht (zur Methodik siehe oben).

  Systematisch gesehen gehört die Beurteilung des Risikos eines ausländischen Behördenzugriffs zum Themenkomplex der Informationssicherheit und ist an sich nicht eine rechtliche Prüfung. Da sie jedoch eine Prüfung des ausländischen Rechts beinhaltet

---

[6] https://www.privatim.ch/de/uberarbeitetes-privatim-merkblatt-cloud-spezifische-risiken-und-massnahmen-2/.

und die klassischen Verfahren zur Beurteilung von Informationssicherheitsrisiken das Risiko eines ausländischen Behördenzugriffs (im Sinne eines Lawful Access) nicht erfassen können, wird es oft im Rahmen der rechtlichen Prüfung und gesondert beurteilt.

- **Prüfung der Compliance-Anforderungen.** Sie umfasst die datenschutzrechtliche Prüfung der Auftragsbearbeitung (d.h. der Frage, ob und wie die Datenbearbeitung an den Provider ausgelagert wird) sowie die Prüfung der weiteren Anforderungen (Berufs- und Amtsgeheimnis, ggf. aufsichtsrechtliche Anforderungen, Gute Cloud Praxis) und grenzt sich damit gegenüber der Prüfung der Datenbearbeitung "als solche" ab (in der Praxis kann sich dies alles natürlich auch vermischen).

  In der Praxis wird hierbei analog zur Beurteilung der Informationssicherheit geprüft, ob bestimmte für Cloud-Vorhaben typischerweise erforderliche Massnahmen getroffen wurden oder noch getroffen werden. Ein grosser Teil dieser Massnahmen betrifft bestimmte Regelungen, die der Vertrag mit dem Provider aufweisen muss. Hinzu kommen weitere Anforderungen an den Provider (z.B. ob er und seine Unterauftragnehmer überprüft wurden), seine Services (z.B. ob sie bestimmte, für die Einhaltung des Datenschutzes erforderliche Vorgaben erfüllen) und an die intern und im Hinblick auf die Services, deren Implementierung und deren Überwachungen zu treffenden Massnahmen (z.B. ob eine vernünftige Exit-Planung besteht). Einige dieser Massnahmen sind nachfolgend zusammengefasst; weitere finden sich auch im Cloud-Merkblatt von Privatim.[7] Die Prüfung ist schriftlich zu dokumentieren.

  Einige dieser Massnahmen sind auch für vorstehend erwähnte Analyse des Risikos eines ausländischen Behördenzugriffs, für eine etwaige DSFA von Relevanz.

G. Prüfraster für die Praxis (Umsetzungshilfe)

In der Praxis kann es schwierig sein, den vielen Anforderungen aus Sicht des Rechts und des Risikos den Überblick zu behalten. Wir haben daher ein Werkzeug entwickelt, das ein Prüfraster zur Beurteilung von Cloud-Projekten der öffentlichen Hand (einschliesslich Spitäler) aus Sicht von Recht und Risiko bietet.

Das Werkzeug definiert ca. 140 konkrete Anforderungen, die sich aus dem Datenschutz, dem Berufs- und Amtsgeheimnis und der "Guten Cloud Praxis" für öffentliche Organe ergeben, einschliesslich aller Anforderungen von Privatim. Es bietet ein Raster von rund 60 Risiken, mit denen sich Cloud-Vorhaben gesamtheitlich beurteilen lassen und es

---

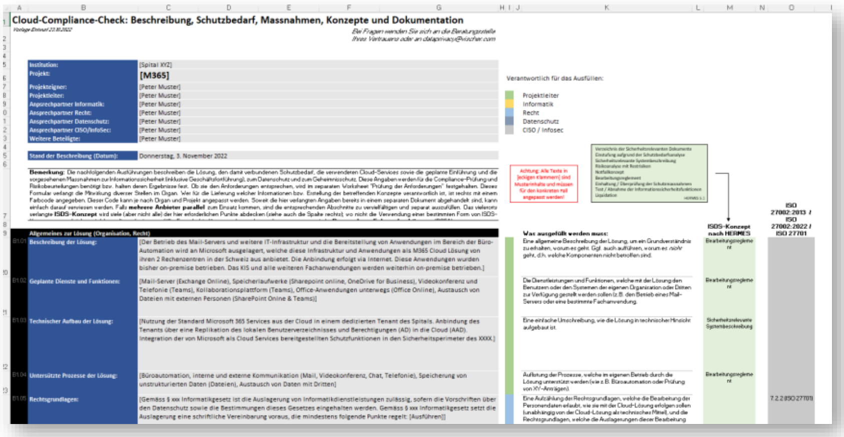
[7] https://www.privatim.ch/de/uberarbeitetes-privatim-merkblatt-cloud-spezifische-risiken-und-massnahmen-2/.

enthält ein Formular, mit welchem alle für die Dokumentation eines Cloud-Vorhabens aus Sicht des Rechts und Risikos normalerweise nötigen Angaben abgefragt werden. Es sieht die Durchführung einer Schuban ebenso vor wie einer DSFA.

Das Werkzeug nennt sich "CCRA-PS",[8] ist Excel-basiert und wurde im Rahmen diverser Projekte in verschiedenen Kantonen entwickelt und basiert auf den Erfahrungen aus zahlreichen Cloud-Vorhaben in sensitiven Bereichen. Es wird zudem weiterentwickelt. Mit seiner Freigabe wird das Werkzeug allen Institutionen des öffentlichen Rechts und allen Spitälern in der Schweiz (mit ihren Beratern) zur Nutzung für ihre Cloud-Projekte kostenlos zur Verfügung stehen.[9]

Es enthält fünf Arbeitsblätter:

- **Beschreibung der Lösung.** Hier nach einem vordefinierten Raster festgehalten, worum es bei der Lösung geht, wie Daten bearbeitet werden, welchen Schutzbedarf sie haben, welche Massnahmen definiert sind und wo und weitere wichtige Aspekte des Vorhabens. Das Arbeitsblatt führt durch den Raster durch und erklärt, was einzufüllen ist. Wie weit das Organ gehen will, muss es allerdings selbst entscheiden. Der Inhalt dieses Arbeitsblatts kann – mit den referenzierten Unterlagen – als ISDS-Konzept benutzt werden. Einzufügen sind hier auch die Risikobeurteilung aus Sicht der Informationssicherheit, die Risikobeurteilung eines ausländischen Lawful Access und etwaige weitere Konzepte (wie z.B. ein Exit-Konzept).



Cloud-Compliance-Check: Beschreibung, Schutzbedarf, Massnahmen, Konzepte und Dokumentation

Bei Fragen wenden Sie sich an die Beratungsstelle Ihres Vertrauens oder an dataprivacy@vischer.com

Institution: [Spital XYZ]
Projekt: [M365]
Projekteigner: [Peter Muster]
Projektleiter: [Peter Muster]
Anpsrechpartner Informatik: [Peter Muster]
Ansprechpartner Recht: [Peter Muster]
Ansprechpartner Datenschutz: [Peter Muster]
Ansprechpartner CISO/InfoSec: [Peter Muster]
Weitere Beteiligte: [Peter Muster]

Stand der Beschreibung (Datum): Donnerstag, 3. November 2022

Verantwortlich für das Ausfüllen:
🟩 Projektleiter
🟨 Informatik
🟦 Recht
▨ Datenschutz
⬜ CISO / Infosec

Achtung: Alle Texte in [eckigen Klammern] sind Musterinhalte und müssen für den konkreten Fall angepasst werden!

Verzeichnis der Sicherheitsrelevanten Dokumente
Einstufung aufgrund der Schutzbedarfsanalyse
Sicherheitsrelevante Systembeschreibung
Risikoanalyse mit Restrisiken
Notfallkonzept
Bearbeitungsreglement
Einhaltung / Überprüfung der Schutzmassnahmen
Test / Abnahme der Informationssicherheitsfunktionen
Liquidation
HERMES 5.1

Bemerkung: Die nachfolgenden Ausführungen beschreiben die Lösung, den damit verbundenen Schutzbedarf, die verwendeten Cloud-Services sowie die geplante Einführung und die vorgesehenen Massnahmen zur Informationssicherheit (inklusive Geschäftsfortführung), zum Datenschutz und zum Geheimnisschutz. Diese Angaben werden für die Compliance-Prüfung und Risikobeurteilungen benötigt bzw. halten deren Ergebnisse fest. Ob sie den Anforderungen entsprechen, wird im separaten Worksheet "Prüfung der Anforderungen" festgehalten. Dieses Formular verlangt die Mitwirkung diverser Stellen im Organ. Wer für die Lieferung welcher Informationen bzw. Erstellung der betreffenden Konzepte verantwortlich ist, ist rechts mit einem Farbcode angegeben. Dieser Code kann je nach Organ und Projekt angepasst werden. Soweit die hier verlangten Angaben bereits in einem separaten Dokument abgehandelt sind, kann einfach darauf verwiesen werden. Falls **mehrere Anbieter parallel** zum Einsatz kommen, sind die entsprechenden Abschnitte zu vervielfältigen und separat auszufüllen. Das vielerorts verlangte **ISDS-Konzept** wird viele (aber nicht alle) der hier erforderlichen Punkte abdecken (siehe auch die Spalte rechts); wo nicht die Verwendung einer bestimmten Form von ISDS-

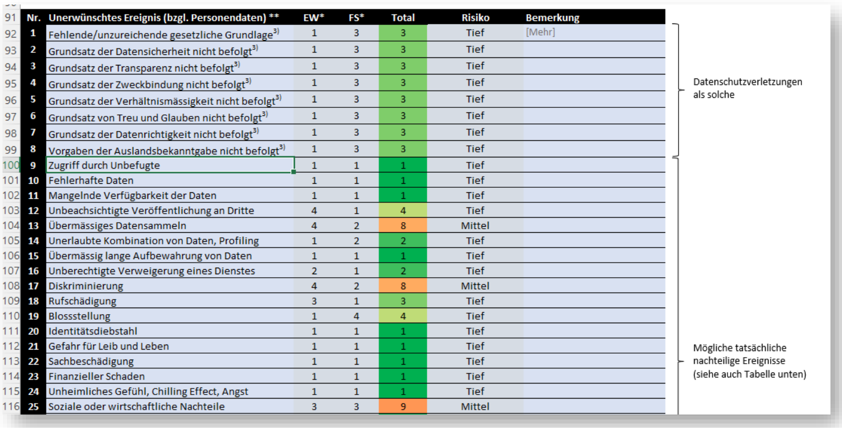
	Allgemeines zur Lösung (Organisation, Recht)		Was ausgefüllt werden muss:	ISDS-Konzept nach HERMES	ISO 27002:2013 / ISO 27002:2022 / ISO 27701
B1.01	Beschreibung der Lösung:	[Der Betrieb des Mail-Servers und weitere IT-Infrastruktur und die Bereitstellung von Anwendungen im Bereich der Büro-Automation wird an Microsoft ausgelagert, welche diese Infrastruktur und Anwendungen als M365 Cloud Lösung von ihren 2 Rechenzentren in der Schweiz aus anbietet. Die Anbindung erfolgt via Internet. Diese Anwendungen wurden bisher on-premise betrieben. Das KIS und alle weiteren Fachanwendungen werden weiterhin on-premise betrieben.]	Eine allgemeine Beschreibung der Lösung, um ein Grundverständnis zu erhalten, worum es geht. Ggf. auch aufführen, worum es *nicht* geht, d.h. welche Komponenten nicht betroffen sind.	Bearbeitungsreglement	
B1.02	Geplante Dienste und Funktionen:	[Mail-Server (Exchange Online), Speicherlaufwerke (Sharepoint online, OneDrive for Business), Videokonferenz und Telefonie (Teams), Kollaborationsplattform (Teams), Office-Anwendungen unterwegs (Office Online), Austausch von Dateien mit externen Personen (SharePoint Online & Teams)]	Die Dienstleistungen und Funktionen, welche mit der Lösung den Benutzern oder den Systemen der eigenen Organisation oder Dritten zur Verfügung gestellt werden sollen (z.B. den Betrieb eines Mail-Servers oder eine bestimmte Fachanwendung.	Bearbeitungsreglement	
B1.03	Technischer Aufbau der Lösung:	[Nutzung der Standard Microsoft 365 Services aus der Cloud in einem dedizierten Tenant des Spitals. Anbindung des Tenants über eine Replikation des lokalen Benutzerverzeichnisses und Berechtigungen (AD) in die Cloud (AAD). Integration der von Microsoft als Cloud Services bereitgestellten Schutzfunktionen in den Sicherheitsperimeter des XXXX.]	Eine einfache Umschreibung, wie die Lösung in technischer Hinsicht aufgebaut ist.	Sicherheitsrelevante Systembeschreibung	
B1.04	Unterstützte Prozesse der Lösung:	[Büroautomation, interne und externe Kommunikation (Mail, Videokonferenz, Chat, Telefonie), Speicherung von unstrukturierten Daten (Dateien), Austausch von Daten mit Dritten]	Auflistung der Prozesse, welche im eigenen Betrieb durch die Lösung unterstützt werden (wie z.B. Büroautomation oder Prüfung von XY-Anträgen).	Bearbeitungsreglement	
B1.05	Rechtsgrundlagen:	[Gemäss § xxx Informatikgesetz ist die Auslagerung von Informatikdienstleistungen zulässig, sofern die Vorschriften über den Datenschutz sowie die Bestimmungen dieses Gesetzes eingehalten werden. Gemäss § xxx Informatikgesetz setzt die Auslagerung eine schriftliche Vereinbarung voraus, die mindestens folgende Punkte regelt: [Ausführen]]	Eine Aufzählung der Rechtsgrundlagen, welche die Bearbeitung der Personendaten erlaubt, wie sie mit der Cloud-Lösung erfolgen sollen (unabhängig von der Cloud-Lösung als technisches Mittel), und die Rechtsgrundlagen, welche die Auslagerungen dieser Bearbeitung		7.2.2 ISO 27701

- **DSFA.** In der Datenschutz-Folgenabschätzung kann dargelegt werden, wie sich die Auslagerung bzw. das Cloud-Vorhaben auf die betroffenen Personen auswirkt.

---

[8] Cloud Compliance and Risk Assessment Public Sector.

[9] Download: https://www.rosenthal.ch/downloads/Rosenthal_CCRA-PS.xlsx.

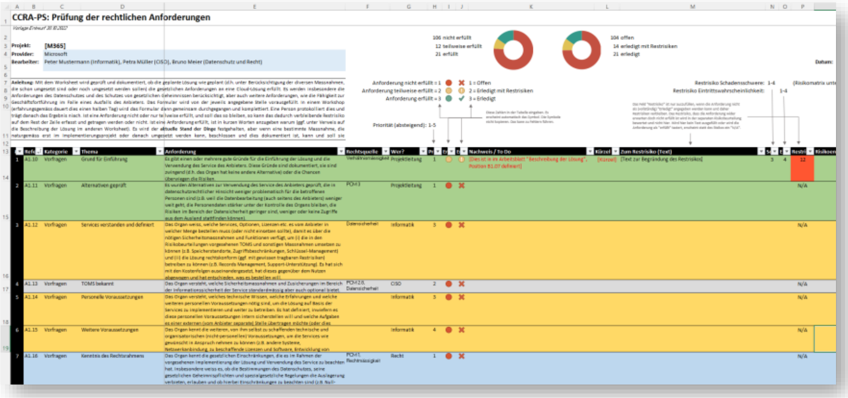


Nr.	Unerwünschtes Ereignis (bzgl. Personendaten) **	EW*	FS*	Total	Risiko	Bemerkung
1	Fehlende/unzureichende gesetzliche Grundlage[3)]	1	3	3	Tief	[Mehr]
2	Grundsatz der Datensicherheit nicht befolgt[3)]	1	3	3	Tief	
3	Grundsatz der Transparenz nicht befolgt[3)]	1	3	3	Tief	
4	Grundsatz der Zweckbindung nicht befolgt[3)]	1	3	3	Tief	
5	Grundsatz der Verhältnismässigkeit nicht befolgt[3)]	1	3	3	Tief	
6	Grundsatz von Treu und Glauben nicht befolgt[3)]	1	3	3	Tief	
7	Grundsatz der Datenrichtigkeit nicht befolgt[3)]	1	3	3	Tief	
8	Vorgaben der Auslandsbekanntgabe nicht befolgt[3)]	1	3	3	Tief	
9	Zugriff durch Unbefugte	1	1	1	Tief	
10	Fehlerhafte Daten	1	1	1	Tief	
11	Mangelnde Verfügbarkeit der Daten	1	1	1	Tief	
12	Unbeachsichtigte Veröffentlichung an Dritte	4	1	4	Tief	
13	Übermässiges Datensammeln	4	2	8	Mittel	
14	Unerlaubte Kombination von Daten, Profiling	1	2	2	Tief	
15	Übermässig lange Aufbewahrung von Daten	1	1	1	Tief	
16	Unberechtigte Verweigerung eines Dienstes	2	1	2	Tief	
17	Diskriminierung	4	2	8	Mittel	
18	Rufschädigung	3	1	3	Tief	
19	Blossstellung	1	4	4	Tief	
20	Identitätsdiebstahl	1	1	1	Tief	
21	Gefahr für Leib und Leben	1	1	1	Tief	
22	Sachbeschädigung	1	1	1	Tief	
23	Finanzieller Schaden	1	1	1	Tief	
24	Unheimliches Gefühl, Chilling Effect, Angst	1	1	1	Tief	
25	Soziale oder wirtschaftliche Nachteile	3	3	9	Mittel	

Datenschutzverletzungen als solche

Mögliche tatsächliche nachteilige Ereignisse (siehe auch Tabelle unten)

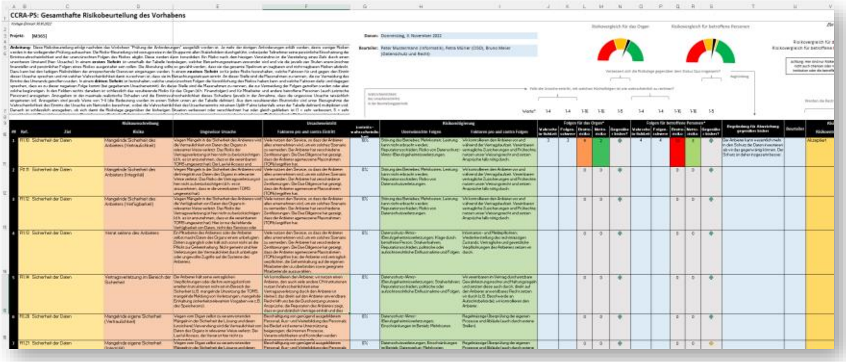
- **Prüfung der Anforderungen.** Dies ist das Kernstück des Werkzeugs. Das Arbeitsblatt definiert eine Vielzahl an wichtigeren und weniger wichtigeren Anforderungen, an welche in einem Cloud-Vorhaben aus Sicht des Datenschutzes, des Berufs- und Amtsgeheimnisses, der weiteren rechtlichen Vorgaben und der "Guten Cloud Praxis" zu denken ist. Es kann jeweils angegeben werden, ob und wie weit die Vorgabe erfüllt ist und falls nicht, welches Risiko damit verbunden ist. Es wird hier im Wesentlichen geprüft, wie gut im Rahmen des ersten Arbeitsblatts gearbeitet wurde.



CCRA-PS: Prüfung der rechtlichen Anforderungen

Projekt: [M365]
Provider: Microsoft
Bearbeiter: Peter Mustermann (Informatik), Petra Müller (CISO), Bruno Meier (Datenschutz und Recht)

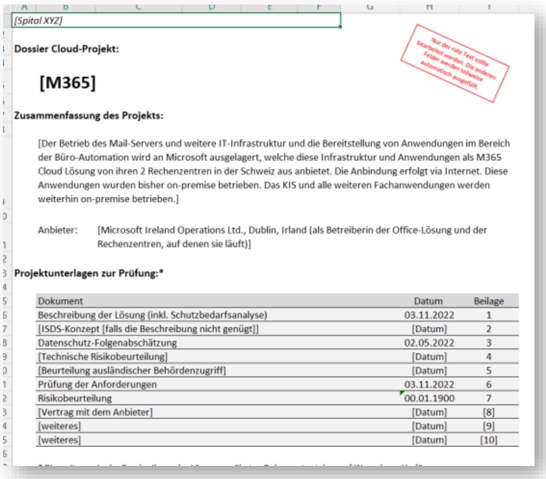
- **Risikobeurteilung.** In diesem Arbeitsblatt sind die typischen Cloud-Risiken aufgeführt, um dem Organ zu helfen, mit den Stakeholdern eine Beurteilung dieser Risiken und ihrer Folgen für das Organ und die betroffenen Personen vorzunehmen. Angezeigt wird auch die Risikobilanz gegenüber dem Status Quo.



CCRA-PS: Gesamthafte Risikobeurteilung des Vorhabens

Projekt: [M365]

- **Deckblatt.** Mit diesem Arbeitsblatt können die Ergebnisse der Prüfung mit dem Werkzeug zusammengefasst werden, damit diese der eigenen Leitung und der Aufsicht vorgelegt werden können (mit den anderen Arbeitsblättern und weiteren Dokumenten als Anhang).



[Spital XYZ]

Nur der rote Text sollte bearbeitet werden. Die anderen Felder werden teilweise automatisch ausgefüllt.

Dossier Cloud-Projekt:

[M365]

Zusammenfassung des Projekts:

[Der Betrieb des Mail-Servers und weitere IT-Infrastruktur und die Bereitstellung von Anwendungen im Bereich der Büro-Automation wird an Microsoft ausgelagert, welche diese Infrastruktur und Anwendungen als M365 Cloud Lösung von ihren 2 Rechenzentren in der Schweiz aus anbietet. Die Anbindung erfolgt via Internet. Diese Anwendungen wurden bisher on-premise betrieben. Das KIS und alle weiteren Fachanwendungen werden weiterhin on-premise betrieben.]

Anbieter: [Microsoft Ireland Operations Ltd., Dublin, Irland (als Betreiberin der Office-Lösung und der Rechenzentren, auf denen sie läuft)]

Projektunterlagen zur Prüfung:*

Dokument	Datum	Beilage
Beschreibung der Lösung (inkl. Schutzbedarfsanalyse)	03.11.2022	1
[ISDS-Konzept [falls die Beschreibung nicht genügt]]	[Datum]	2
Datenschutz-Folgenabschätzung	02.05.2022	3
[Technische Risikobeurteilung]	[Datum]	4
[Beurteilung ausländischer Behördenzugriff]	[Datum]	5
Prüfung der Anforderungen	03.11.2022	6
Risikobeurteilung	00.01.1900	7
[Vertrag mit dem Anbieter]	[Datum]	[8]
[weiteres]	[Datum]	[9]
[weiteres]	[Datum]	[10]

In der Praxis hat es sich bewährt, dass die jeweiligen Stakeholder in der Institution (z.B. Projektleitung, Informatik, Recht, Datenschutz, CISO) die ihnen zugewiesenen Themen und Anforderungen befüllen oder vorbereiten und dann in gemeinsamen Workshops die jeweiligen Arbeitsblätter vervollständigt werden. Diese Workshops werden vorzugsweise durch eine in solchen Vorhaben erfahrene Person moderiert.

H. Massnahmen aus rechtlicher Sicht

In der Praxis bereitet in Cloud-Vorhaben im öffentlich-rechtlichen Bereich erfahrungsgemäss die Einhaltung des Berufs- und Amtsgeheimnisses die grössten Sorgen, und dabei vor allem das Risiko eines ausländischen Behördenzugriffs. Dies ist auch das aus Sicht des Datenschutzes meistzitierte Thema, nebst den Interessen der Provider, die Daten ihrer Kunden auch für eigene Zwecke analysieren zu können.

Die Informationssicherheit im engeren Sinne ist in der Regel seitens der Provider kaum je ein Problem; jedenfalls die grossen Hyperscaler (Microsoft, AWS, Google) haben hier nach Beurteilung der meisten Experten mehr zu bieten, als viele Organisationen auf ihren eigenen Systemen sicherzustellen in der Lage wären.

Eine Herausforderung ist hingegen die richtige Handhabung und Überwachung der Cloud-Services und ihrer Provider durch den Kunden. Eine weitere Herausforderung ist die Abhängigkeit, in welche sich eine Organisation beim Gang in die Cloud begibt und die (allenfalls unzureichende) Möglichkeit, von einem Provider oder bestimmten Cloud-Services bei Bedarf rasch wieder loszukommen.

Diese Themen sind insofern rechtlicher Natur, weil das Recht von einer Organisation bzw. ihren Organen nicht nur verlangt, dass sie Personendaten und Geheimnispflichten ausreichend geschützt werden, sondern auch andere Risiken ausreichend kennt und im Griff hat. Angesichts der mangelnden Erfahrung mit dem Thema "Cloud" ist es für viele Organisationen eine weitere Herausforderung, hier den Überblick zu behalten.

Wir unterscheiden in der Folge zwischen vertraglichen und weiteren technischen und organisatorischen Massnahmen. Hier sind einige der wichtigsten Massnahmen:

- **Vertragliche Massnahmen.** Grundsätzlich darf bei einem seriösen Provider mangels anderer Hinweise darauf vertraut werden, dass er sich an die vertraglichen Zusagen hält; das war schon bisher bei Schweizer Providern so und es gibt keinen Grund anzunehmen, warum dies bei renommierten ausländischen Providern in Rechtsstaaten anders sein sollte. Die Standardverträge vieler Cloud-Provider genügen den Anforderungen eines öffentlichen Organs oder Spitals jedoch nicht und müssen daher erweitert werden. Dafür bieten immer mehr Provider standardisierte Zusatzvereinbarungen an. Auch diese genügen entgegen den Beteuerungen der Provider nicht immer den Anforderungen; hier braucht es ggf. externe Expertise. Hier sind einige der wichtigen Punkte, auf die in den Verträgen geachtet werden sollte:
    - **Europäische Gegenpartei:** Cloud-Provider sind meist im Ausland, oft auch im Besitz von US-Konzernen. Dies ist entgegen allen Unkenrufen kein Ausschlusskriterium. Es sollte jedoch zum Schutz vor US-Behördenzugriffen darauf geachtet werden, dass der Vertrag mit einer Tochtergesellschaft im EWR oder in der Schweiz abgeschlossen wird (UK ist hingegen nicht empfehlenswert, weil UK betr. die Herausgabe von Daten mit den USA kooperiert[10]).
    - **Datenlagerung in der Schweiz:** Soweit dies möglich ist, sollte zugesichert sein, dass die in der Cloud gespeicherten Kundendaten (nicht die Nutzungsdaten) nur in der Schweiz

---

[10] Dortige Provider unterstehen dem US CLOUD Act ebenfalls für gewisse Fälle.

(oder mindestens im EWR) gespeichert werden, auch wenn Zugriffe von ausserhalb vorbehalten bleiben, was sie fast immer werden.

- **Manuelle Zugriffe einschränken:** Soweit dies möglich ist, sollte der Provider mindestens den manuellen Zugriff (d.h. durch Menschen, nicht automatisierte Vorgänge) auf Kundendaten im Klartext eingeschränkt werden, z.B. nur auf Freigabe durch den Kunden oder nur aus dem EWR oder der Schweiz. Die Einschränkung von manuellen Zugriffen durch den Provider ist zum Schutz vor Zugriffen ausländischer Behörden besonders wichtig. Es ist davon auszugehen, dass immer mehr Provider mindestens (gegen Bezahlung oder kostenlos) die Option anbieten werden, dass ihre Cloud-Services ausschliesslich aus dem EWR heraus erbracht werden, dies aufgrund der immer intensiveren Debatte über das Risiko von Zugriffen durch US-Nachrichtendienste. Allerdings weisen auch solche Optionen oft noch Ausnahmen vor.
- **Vertraulichkeitsverpflichtung:** Der Vertrag muss eine echte Vertraulichkeitsverpflichtung enthalten (nicht nur die Pflicht, Massnahmen zur Datensicherheit zu treffen oder Daten nicht für andere Zwecke als den Vertrag zu nutzen), die auch den Mitarbeitern und Subunternehmern überbunden wird. Sie muss zeitlich solange gelten, wie ein Geheimhaltungsinteresse besteht, idealerweise zeitlich unbeschränkt. Viele US-basierte Provider wehren sich dagegen, weil ihnen solche Klauseln fremd sind.
- **Defend-your-Data-Klausel:** Jeder Provider wird die Vertraulichkeit unter den Vorbehalt stellen, dass er Kundendaten herausgeben muss, falls er nach seinem Recht dazu verpflichtet ist. Für diesen Fall sollte er allerdings nicht nur die Information des Kunden zusichern, sondern ebenso verpflichtet sein, gegen jede Herausgabeaufforderung, welche das Schweizer Recht verletzt, den Rechtsweg auszuschöpfen. Solche Klauseln sind zusehends Standard. Die Standardvertragsklauseln der Europäischen Kommission enthalten auch solche, die aber für die vorliegenden Zwecke sachlich zu eng gefasst sind.
- **Auftragsbearbeitungsvertrag:** Mittlerweile gehört es zum Standard, dass Cloud-Provider einen solchen Vertrag (auch ADV genannt) anbieten, der den Anforderungen der DSGVO entspricht. Hier muss darauf geachtet werden, dass dieser auch auf das Schweizer Datenschutzrecht (DSG und kantonale Datenschutzgesetze) Bezug nimmt und die Schweizer Besonderheiten beim Export von Daten berücksichtigt.

- **Eigene Datenbearbeitungen des Providers:** Einige Provider wie z.B. Microsoft wollen Daten, die bei der Nutzung ihrer Cloud-Services anfallen, für eigene Zwecke auswerten können. Dies tangiert die eigenen Mitarbeiter, welche diese Cloud-Services nutzen. Sie müssen daher nicht nur informiert sein, sondern es sollte darauf geachtet werden, dass ihre Daten vorgängig pseudonymisiert werden, sofern solche eigenen Datenbearbeitungen nicht ganz ausgeschlossen werden können (die DSGVO verlangt dies auch, was einer der Gründe ist, warum die Vertragspartei ihren Sitz im EWR oder in der Schweiz haben sollte). Noch grössere Vorsicht ist dort erforderlich, wo "Kundendaten" (im Falle des Spitals oder öffentlichen Organs also z.B. Patienten- oder Einwohnerdaten) für eigene Zwecke des Providers bearbeitet werden sollen. Normalerweise ist dies auszuschliessen, aber es kann Situationen geben, wo dies naturgemäss erforderlich ist (z.B. das Training einer KI des Providers, welche Bestandteil der Leistung ist); in diesen Fällen sind zusätzliche Abklärungen zu treffen (z.B. hinsichtlich der Anonymisierung der Daten und den weiteren Schutzvorkehrungen[11]).
- **Prüfrechte:** Die meisten Provider erlauben ihren Kunden eine Prüfung der Vertragskonformität nur in Bezug auf die Informationssicherheit und nur indirekt über Prüfberichte, die sie bei unabhängigen Prüfgesellschaften in Auftrag geben. Dies wird häufig akzeptiert und macht auch ökonomisch Sinn, insbesondere, wenn diese Prüfberichte nach anerkannten Standards erstellt werden und auch über die Wirksamkeit der getroffenen Sicherheitsmassnahmen Auskunft geben. Es sollte immerhin darauf geachtet werden, dass manche kantonale Datenschutzgesetze verlangen, dass Prüfungen auch durch die Datenschutzbehörden vorgenommen werden können. Dies muss im Vertrag vorgesehen werden.
- **Schweizer Recht und Gerichtsstand:** Kantonale Datenschutzbehörden vertreten regelmässig die Ansicht, dass öffentliche Organe in den Verträgen über die Nutzung von Cloud-Services ausländischer Provider mindestens für datenschutzrechtliche Klagen einen Gerichtsstand in der Schweiz und Schweizer Recht vereinbaren müssen, weil ein ausländischer Gerichtsstand und ausländisches Recht für öffentliche Organe möglicherweise nicht praktikabel sind. Der SIK-Rahmenvertrag mit Microsoft sieht dies teilweise vor; eine analoge Bestimmung ist im Rahmenvertrag diverser

---

[11] Vgl. dazu https://www.rosenthal.ch/downloads/Rosenthal-KI-Datenschutz.pdf.

    Universitätsspitaler enthalten. Andere Provider lassen sich teilweise ebenfalls darauf ein.

  - **Schutz vor nachteiligen Anpassungen:** Cloud-Services unterliegen ständigen Anpassungen. Dies gilt dementsprechend auch für die Verträge der Provider, da sie die Services regeln. Trotzdem ist sicherzustellen, dass kein Abbau von Leistungen, Sicherheit oder vertraglichem Schutz erfolgt, ohne, dass das Organ als Kunde darauf reagieren kann (wobei die Reaktion in aller Regel bedeuten wird, den betreffenden Cloud-Service innert entsprechend kurzer Frist aufgeben zu müssen). Die Ankündigungsfrist muss also genügend lang sein.
  - **Suspendierungs- und Beendigungsrechte:** Je höher die Abhängigkeit des Organs von einer Cloud-basierten Lösung, desto stärker müssen auch die vertraglichen Rechte des Providers eingeschränkt sein, die Leistungserbringung zu unterbrechen, einzuschränken oder zu beenden – jedenfalls in einer Form, welche das Organ "im Regen" stehen lassen würde, ohne dass für einen solchen Fall vorbereitet wäre.
- **Weitere technische und organisatorische Massnahmen.** Sie sollen ebenfalls den Schutz der bearbeiteten Daten, aber auch die Geschäftsfortführung (d.h. die Resilienz des Betriebs im Falle von Cloud-Ausfällen) sicherstellen. Zu denken ist insbesondere an:
  - **Verschlüsselungen:** Sie sind heute Standard und dienen vor allem dem Schutz vor externen Angreifern. Normal und zwingend ist heute eine Verschlüsselung der Daten "in transit" (d.h. bei der Übermittlung) und "at rest" (d.h. bei der Abspeicherung). In all diesen Fällen ist der Schlüssel dem Provider anvertraut, der ihn entweder selbst verwaltet oder dies dem Kunden überlässt. Aus rechtlicher Sicht macht dies keinen sehr grossen Unterschied (einer der Use Cases ist, dass wenn der Kunde den Schlüssel selbst verwaltet, er ihn nach einem Exit zerstören und damit all seine Daten unlesbar machen kann), ebenso nicht, ob der Schlüssel vom Provider oder vom Kunden erzeugt wird ("bring-your-own-key"). Normalerweise bedeutet Verschlüsselung jedoch nicht, dass der Provider bei Bedarf technisch nicht in der Lage ist, auf Kundendaten im Klartext zuzugreifen. Hierfür bräuchte es spezifische technische Vorkehrungen, die bisher nur selten in Frage kommen (insbesondere müsste der Schlüssel ausserhalb der Sphäre des Providers aufbewahrt

und die Inhalte auch ausserhalb verschlüsselt werden, was regelmässig nicht der Fall ist[12]).

- **Informationssicherheit:** Die diversen (weiteren) Massnahmen zur Informationssicherheit werden hier nicht erläutert. Zu bedenken ist, dass solche nicht nur seitens des Providers, sondern auch seitens des Organs erforderlich sind. Wir verweisen hier unter anderem auf die "ATT&CK Matrix for Enterprise" von MITRE, welche gängige Cyber-Angriffsmuster für verschiedene Lösungen und Technologien aufzeigt,[13] so unter anderem auch für "O365".[14] Für aus dem Internet zugängliche Anwendungen bietet OWASP Hinweise auf die gängigen Angriffsszenarien.[15] Sie kann zur Prüfung der getroffenen Massnahmen benutzt werden.
- **Korrekte Konfiguration und Steuerung:** Cloud-Services sind in der Regel vollautomatisch von einer Maschine erbrachte Leistungen. Es kommt daher entscheidend darauf an, wie der Kunde sie konfiguriert und steuert (z.B. wo Daten gespeichert werden, welche Benutzer und Anwendungen darauf von wo aus mit welchen Geräten Zugriff haben, was Mitarbeiter tun können, wie diese Überwacht werden, was aufgezeichnet wird an Audit-Trails, wie Daten gesichert werden, wie Zugriffe des Providers eingeschränkt werden, welche Services aktiviert sind und welche nicht). Dies erfordert Know-how (d.h. es muss aufgebaut werden) und entsprechende Prozesse (d.h. diese müssen definiert und Verantwortlichkeiten festgelegt werden). Die Konfiguration ist keine einmalige Sache, sondern sie muss laufend überprüft, verstanden und wenn nötig angepasst werden, da sich Änderungen ergeben können – auch seitens des Providers, weil sich Cloud-Services laufend weiterentwickeln.
- **Überwachung des Providers:** Der Provider ist zwar zur Einhaltung des Vertrags verpflichtet, aber dies entbindet das Organ nicht, die Einhaltung zu überwachen. Da es dies in der Regel nicht direkt tun kann, wird es dies anhand der Prüfberichte und Audit-Trails tun müssen, die der Provider zur Verfügung stellt bzw. der Cloud-Service generiert. Es ist auch sonst zu prüfen, ob es zu Entwicklungen kommt (z.B. Zwischenfälle), die seitens des Organs Anpassungen des

---

[12] Eine Anwendung ist eine E-Mail-Verschlüsselung mittels S/MIME durch einen separaten Schlüssel; gewisse Provider bieten teilweise ebenfalls solche Optionen für andere Daten (wie z.B. die "Double-Key-Encryption" von Microsoft, die aber nach unserer Erfahrung hierzulande kaum zum Einsatz kommt). Etwas einfacher sind solche Lösungen zu realisieren, wenn ein Organ die Cloud für eigene Anwendungen benutzt und nicht Software-as-a-Service-Anwendungen wie M365.

[13] https://attack.mitre.org/.

[14] https://attack.mitre.org/matrices/enterprise/cloud/office365/

[15] https://owasp.org/.

Vorhabens auch nach dem "Go Live" erfordern (z.B. eine neue Risikobeurteilung). Hierzu sollten Prozesse mit entsprechenden Verantwortlichkeiten definiert werden.

- **Backups & BCM:** Auch Cloud-Services können ganz oder teilweise ausfallen oder die Leistung kann verweigert werden. Für diesen Fall sind Backups, ein Notfallkonzept und ggf. sogar Alternativen vorzusehen, die nicht vom betreffenden Cloud-Provider abhängen, damit die Geschäftsfortführung ("Business Continuity Management", BCM) bestmöglich sichergestellt ist.
- **Exit-Konzept:** Schon vor der Umsetzung des Vorhabens sollte klar sein in welchen Fristen und ggf. mit welchen Abstrichen ein Exit und eine Migration zu einer Nachfolgelösung eines Cloud-Services möglich ist. Ein solcher Exit sollte innerhalb derjenigen Fristen möglich sein, innert denen ein Exit gemäss Vertrag nötig werden kann, weil z.B. ein Subunternehmer beigezogen wird, der nicht akzeptabel ist, erforderliche Leistungen abgebaut werden oder eine nicht hinnehmbare Vertragsänderung ansteht. Typischerweise betragen diese Fristen weniger als 180 Tage. Dies kann z.B. erfordern, dass bereits vorgängig Alternativen für den gewählten Provider und Cloud-Service ausgelotet werden oder das Vorhaben so umgesetzt wird, dass ein "Umzug" von einem Cloud-Service zu einem anderen einfacher möglich ist (z.B. Einsatz von Container-Techniken oder zusätzlichen Abstraktionstechniken).

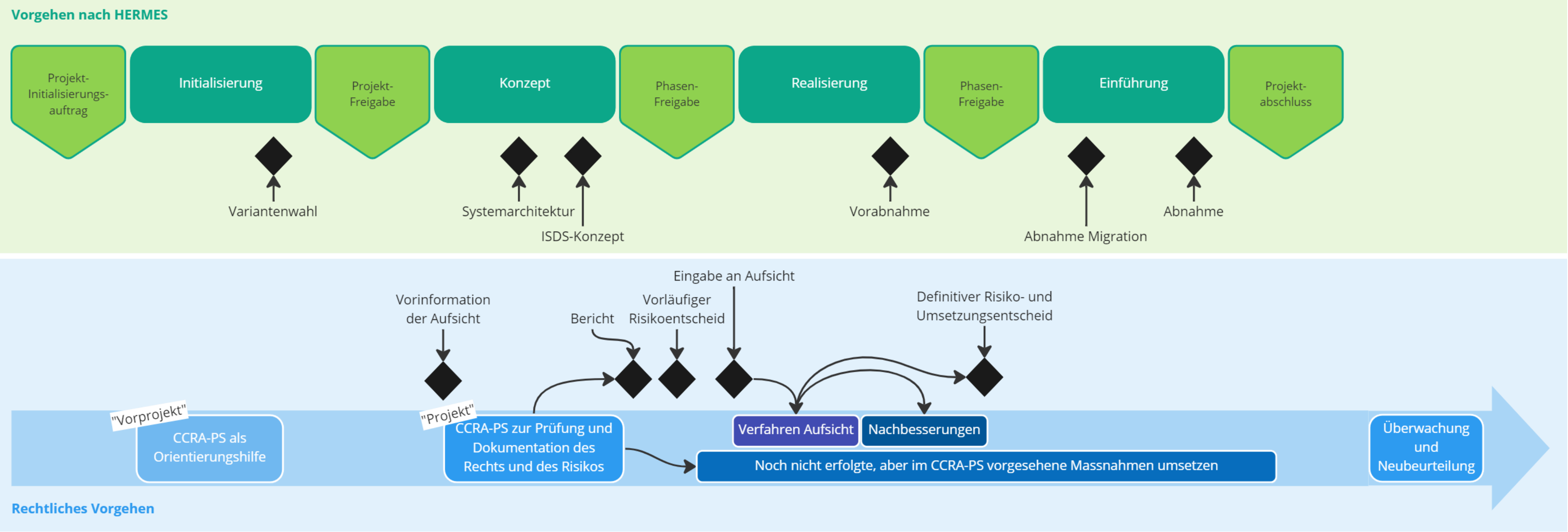
Fünf Fragen der Leitung des Organs vor dem Gang in die Cloud

Die Fragen kann sich die Leitung sowohl in strategischer Hinsicht als auch im Hinblick auf die Beurteilung oder Entscheidung über ein konkretes Cloud-Vorhaben des öffentlichen Organs bzw. Spitals stellen. Die Antworten erarbeitet sie mit der eigenen Organisation.

	Strategie und Vorgehensweise	**Beurteilung eines konkreten Vorhabens**
Motive & Alternativen	Welche Dinge erhoffen wir uns vom Gang in die Cloud und wie gut wollen wir die Alternativen kennen?	Was sind die geschäftlichen, operationellen und anderen Anforderungen an das Vorhaben und wieso überwiegt die gewählte Lösung gegenüber anderen Techniken (d.h. Alternativen zur Cloud), anderen Cloud-Providern und dem Status quo?
Compliance	Wie gehen wir vor, um die Einhaltung des Berufs- bzw. Amtsgeheimnisses und der diversen gesetzlichen, regulatorischen wie auch eigenen Vorgaben systematisch zu prüfen, zu dokumentieren und während der ganzen Laufzeit der Cloud-Vorhaben sicherzustellen?	Halten wir mit dem Vorhaben das Berufs- bzw. Amtsgeheimnis und die gesetzlichen, regulatorischen wie auch die eigenen Vorgaben ein und wie haben wir dies systematisch geprüft, dokumentiert und für die ganze Laufzeit des Cloud-Vorhabens sichergestellt?
Organisation & Internes Kontrollsystem (IKS)	Was sind wir bereit zu tun und zu verlangen, damit unsere Organisation Cloud-Provider und deren Lösungen verstehen, kontrollieren und steuern können, so dass wir sie nicht nur richtig handhaben können, sondern auch Abweichungen vom Soll rechtzeitig erkennen und beseitigen können?	Welche Vorkehrungen haben wir getroffen oder treffen wir, damit wir den Provider und seinen Cloud-Lösung mit unseren internen Mitteln so gut verstehen, kontrollieren und steuern können, dass wir die Cloud-Lösung gemäss den Anforderungen richtig handhaben, Abweichungen vom Soll rechtzeitig erkennen und sie beseitigen können werden, inklusive seiner bzw. ihrer "end-to-end" Einbindung in unser IKS?
Geschäftsfortführung	Welche Anforderungen stellen wir an die Sicherstellung der Geschäftsfortführung bei einem Ausfall oder Datenverlust und unsere Fähigkeit für einen kurzfristigen (Monate) und mittelfristigen (12-18 Monate) Ausstieg aus einem Cloud-Service und welchen Aufwand sind wir bereit dafür zu betreiben?	Was ist unser Plan für den Fall, dass der Cloud-Provider seinen Service plötzlich abstellt, die Lösung oder unsere Daten nicht mehr verfügbar sind oder wir kurzfristig (Monate) und mittelfristig (12-18 Monate) von ihm oder seiner Lösung weg müssen oder wollen?
Restrisiken	Wie stellen wir sicher, dass wir konkrete Bedrohungen, die mit einem Cloud-Vorhaben einhergehen und gewichtige Folgen für das Organ haben können, richtig einschätzen, steuern und in Bezug zu den Restrisiken stellen, die wir sonst bzw. sowieso haben?	Welche weiteren Bedrohungen, welche für das Organ gewichtige Folgen haben können, bringt das Cloud-Vorhaben mit sich, wie gut haben wir diese im Griff und wie stehen die Restrisiken zu jenen Risiken, die wir ohne das Vorhaben bzw. sowieso hätten?

CCRA-PS: Die Prüfung von Recht und Risiko im Einklang mit dem HERMES-Prozess

Verschiedene öffentliche Institutionen in den Kantonen und im Bund wollen oder müssen ihre Cloud-Projekte nach der HERMES-Projektmethode umsetzen. Diese ist mit der hier vorgestellten Vorgehensweise und der Umsetzungshilfe CCRA-PS kompatibel. Da HERMES in der üblichen Ausprägung die für Cloud-Projekte oft erforderliche Abstimmung mit den zuständigen Aufsichtsbehörden (z.B. Vorabkontrolle nach kantonalem Datenschutzrecht) nicht vorsieht, haben wir in der folgenden Grafik aufgezeigt, wie diese Abklärungen zum Recht und Risiko (die über ein ISDS-Konzept hinausgehen) in den HERMES-Standardablauf passen:



Der untere Teil der Grafik entspricht der in diesem Leitfaden näher erläuterten Vorgehensweise zum Recht und Risiko. Die Hauptarbeit findet in der Konzept-Phase statt; hier werden die rechtlichen Voraussetzungen geschaffen bzw. geprüft und die Risiken einer gesamtheitlichen Beurteilung unterzogen, was schliesslich zu einem Bericht führt, welcher zunächst der Leitung und – falls diese zustimmt und die Restrisiken für tragbar erachtet und akzeptiert – der Aufsicht vorgelegt wird. Diese prüft das Vorhaben, während mit der Realisierung (aber in Abstimmung mit der Aufsicht) üblicherweise bereits fortgefahren werden kann. Etwaige Nachbesserungen werden im Anschluss daran umgesetzt. Während der gesamten Realisierungs- und Einführungsphase werden zudem jene Massnahmen, die in der rechtlichen Prüfung vorausgesetzt, aber noch nicht umgesetzt wurden, implementiert.