VISCHER

Einführung von M365.

Wie vorgehen aus rechtlicher Sicht

David Rosenthal, Partner, VISCHER AG
24. August 2022

VGIch
Vereinigung Gesundheitsinformatik Schweiz

NEWS

Unterschiedliche Rechtsauffassungen

EDÖB rät Suva von Microsoft 365 ab

Mi 15.06.2022 - 12:00 Uhr
von Yannick Züllig und kfi

Die Suva will in die Microsoft-Cloud. Dazu holte sie eine Risikobeurteilung vom EDÖB ein. Dieser rät dem Versicherer, den Schritt zu überdenken.

Ist damit die Übung vom Tisch?

Nein!

Die Themen, die heute die Diskussion prägen …

- Risiko eines Zugriffs von US-Behörden ("**US CLOUD Act**")
- Zugriffe von **US-Nachrichtendiensten** ("Schrems II")
- **Rechtsgrundlagen** für die Auslagerung
- Bearbeitung von **Mitarbeiterdaten**
- Digitale **Souveränität** der Schweiz
- Erfordernis von **Null-Risiko**

- Eine emotionale und nicht immer sachliche Diskussion …

Fällt die Bundeskanzlei bald aus allen Wolken?

Ein einzelner Bürger klagt gegen das Public-Cloud-Projekt des Bundes. Und könnte das Vorhaben womöglich ganz stoppen.

Von Adrienne Fichter, 15.08.2022

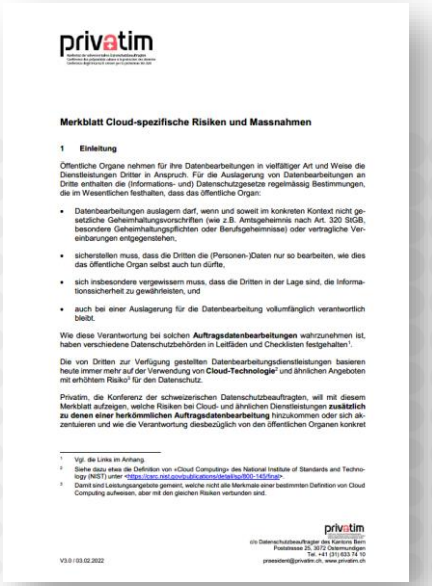
Republik.ch

Was derzeit geschieht

- **Privatwirtschaft** setzt M365 bereits seit einigen Jahren ein
- Erste Schweizer **Banken**, **Kantone** und **Spitäler** haben nun ebenfalls damit begonnen, weitere haben Projekte
- Erste **Bundesbetriebe** auch (Suva), andere verhandeln
- Erste kantonale **Datenschutzbehörden** haben entsprechende Vorhaben "akzeptiert"
- Auf **M365** folgen 6-12 Monate später weitere Anwendungen
- Neben **Microsoft** kämpfen **AWS** und **Google** um Kunden (mit Infrastruktur-Services, d.h. CaaS, PaaS, IaaS)
- Schweizer Player (z.B. **Swisscom**) agieren als Integratoren

Haltung der Behörden

- **EDÖB** agiert taktisch
  - Alle Optionen offenhalten; EU nicht vergrämen; säht Zweifel, unternimmt aber nichts
- **Kantonale Datenschutzbehörden**
  - Gespalten in drei Lager – Lawful Access als Zankapfel
  - Pragmatiker (risikobasierter Ansatz)
  - Fundamentalisten (auch kein theoretisches Risiko)
  - Isolationisten (kein Outsourcing unter Art. 320 StGB)
- **Bund, Kantone, Institutionen** akzeptieren die Risiken
  - Ausser Aufsichtsbehörden (z.B. BSV)
  - Gerichte schweigen, Staatsanwaltschaften pragmatisch



privatim

Merkblatt Cloud-spezifische Risiken und Massnahmen

1 Einleitung

Öffentliche Organe nehmen für ihre Datenbearbeitungen in vielfältiger Art und Weise die Dienstleistungen Dritter in Anspruch. Für die Auslagerung von Datenbearbeitungen an Dritte enthalten die (Informations- und) Datenschutzgesetze regelmässig Bestimmungen, die im Wesentlichen festhalten, dass das öffentliche Organ:

- Datenbearbeitungen auslagern darf, wenn und soweit im konkreten Kontext nicht gesetzliche Geheimhaltungsvorschriften (wie z.B. Amtsgeheimnis nach Art. 320 StGB, besondere Geheimhaltungspflichten oder Berufsgeheimnisse) oder vertragliche Vereinbarungen entgegenstehen;
- sicherstellen muss, dass die Dritten die (Personen-)Daten nur so bearbeiten, wie dies das öffentliche Organ selbst auch tun dürfte,
- sich insbesondere vergewissern muss, dass die Dritten in der Lage sind, die Informationssicherheit zu gewährleisten, und
- auch bei einer Auslagerung für die Datenbearbeitung vollumfänglich verantwortlich bleibt.

Wie diese Verantwortung bei solchen **Auftragsdatenbearbeitungen** wahrzunehmen ist, haben verschiedene Datenschutzbehörden in Leitfäden und Checklisten festgehalten[1].

Die von Dritten zur Verfügung gestellten Datenbearbeitungsdienstleistungen basieren heute immer mehr auf der Verwendung von **Cloud-Technologie**[2] und ähnlichen Angeboten mit erhöhtem Risiko[3] für den Datenschutz.

Privatim, die Konferenz der schweizerischen Datenschutzbeauftragten, will mit diesem Merkblatt aufzeigen, welche Risiken bei Cloud- und ähnlichen Dienstleistungen **zusätzlich zu denen einer herkömmlichen Auftragsdatenbearbeitung** hinzukommen oder sich akzentuieren und wie die Verantwortung diesbezüglich von den öffentlichen Organen konkret

1 Vgl. die Links im Anhang.
2 Siehe dazu etwa die Definition von «Cloud Computing» des National Institute of Standards and Technology (NIST) unter <https://csrc.nist.gov/publications/detail/sp/800-145/final>.
3 Damit sind Leistungsangebote gemeint, welche nicht alle Merkmale einer bestimmten Definition von Cloud Computing aufweisen, aber mit den gleichen Risiken verbunden sind.

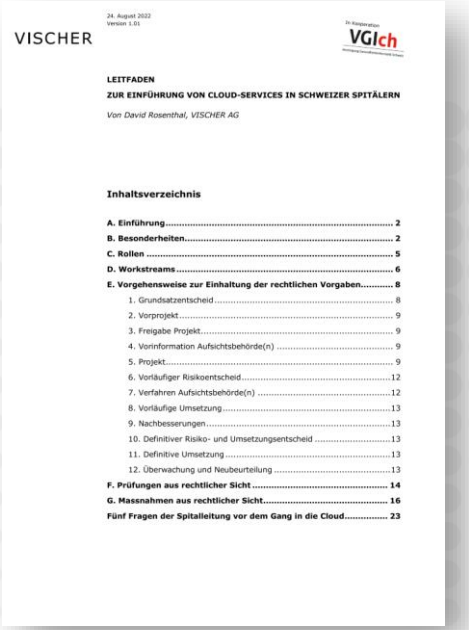
privatim
c/o Datenschutzbeauftragter des Kantons Bern
Postgasse 25, 3072 Ostermundigen
Tel. +41 (31) 633 74 10
praesident@privatim.ch, www.privatim.ch

V3.0 | 03.02.2022

Cloud-Merkblatt privatim

Die wichtigsten Cloud-Themen

- **Abhängigkeit** und Geschäftsfortführung
- **Informationssicherheit**
- Modell der **"Shared Responsibility"**
- **Datenschutz** & **Berufsgeheimnis**
- Datenbearbeitung für **Zwecke des Providers**
- Ausländischer **Behördenzugriff**
- **Vertrag** mit dem Cloud-Provider
- **Überwachung** von Mitarbeitern
- **Rechtsgrundlagen** und Verhältnismässigkeit



24. August 2022
Version 1.01

VISCHER

In Kooperation mit VGIch

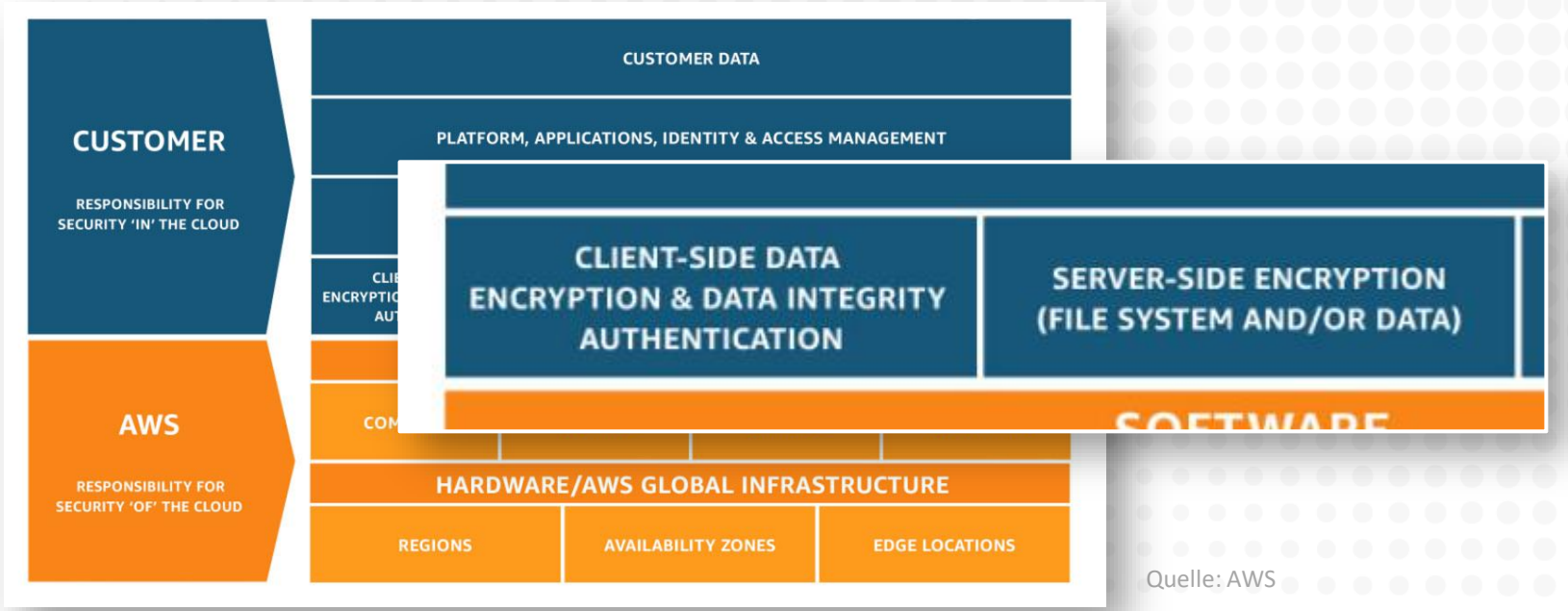
LEITFADEN
ZUR EINFÜHRUNG VON CLOUD-SERVICES IN SCHWEIZER SPITÄLERN

Von David Rosenthal, VISCHER AG

Inhaltsverzeichnis

Neuer Leitfaden

Shared Responsibility Model?



Quelle: AWS

Vorgaben Datenschutz

- Öffentlich-rechtliche Spitäler: **Rechtsgrundlage**
- Aber: In der Regel "nur" eine **Auftragsbearbeitung**
  - Keine Einwilligung der betroffenen Personen erforderlich
  - Vorgaben punkto Datensicherheit, Vertrag und Datenexporte
  - Grundsatz der Verhältnismässigkeit: Welche Alternativen gibt es?
  - Spital muss weiterhin Kontrolle haben: Ist ein Ausstieg möglich?
  - Keine nicht tragbaren Risiken eingehen: DSFA gemacht?
  - Pflicht zur Transparenz, Informationspflicht
- Nicht nur an **Patienten**, sondern auch an **Mitarbeiter** denken
  - Microsoft will Mitarbeiterdaten für eigene Zwecke bearbeiten
  - Tools erlauben dem Spital die Überwachung von Mitarbeitern

Vorgaben Berufsgeheimnis

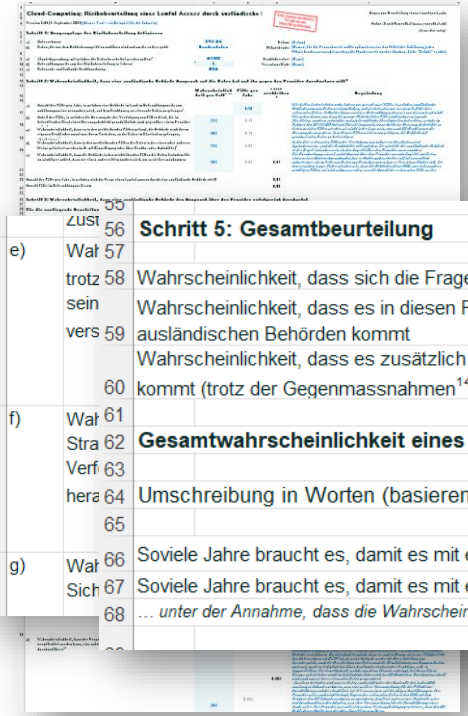
- **Offenbarung** gegenüber Provider vs. ausländischer Behörde
- **Bedingungen** für den Beizug eines Cloud-Providers
  - Datensicherheit und Verwendungskontrolle ist angemessen
  - Beizug geschäftlich begründet
  - Beizug widerspricht nicht der Erwartung der geschützten Person
  - Beizug verletzt keine gesetzliche oder vertragliche Pflicht
  - Subordinationsverhältnis des Cloud-Providers
- **Ergebnis:** Auslagerung in die Cloud erlaubt, sofern kein Grund zur Annahme, dass ein ausländischer Lawful Access erfolgt
  - Es braucht keine Entbindung vom Arztgeheimnis
  - Lawful Access: Gesundheitsdaten sind nicht stärker gefährdet

Prüfpunkte kantonaler Datenschützer

- Vertragsgestaltung
- Orte der Datenbearbeitung inkl. ausländische Behördenzugriffe
- Vertraulichkeit, Geheimnisschutz, Verschlüsselung und Schlüsselmanagement
- Daten über die Nutzerinnen und Nutzer der Cloud-Dienste
- Unterauftragsverhältnisse
- Meldepflichten (von Änderungen)
- Kontrollrecht und -möglichkeit
- Informationssicherheitsmassnahmen
- Pflichten bei Vertragsauflösung

Erfolgreich durchgeführt vom USB/UKBB

Beurteilung ausländischer Lawful Access

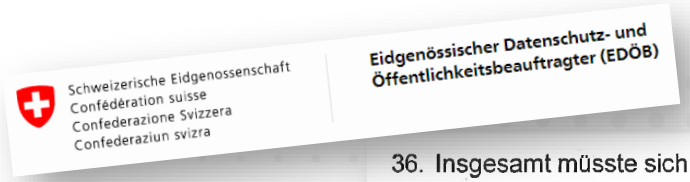


Input: Bisherige Erfahrungen mit Anfragen ausländischer Behörden, technische und organisatorische Massnahmen

Schritt 5: Gesamtbeurteilung		
Wahrscheinlichkeit, dass sich die Frage eines Lawful Access über den Cloud-Provider überhaupt stellt (1 Fall in der Periode = 100%)		6.25%
Wahrscheinlichkeit, dass es in diesen Fällen trotz der Gegenmassnahmen[14)] zu einem erfolgreichen Lawful Access durch die betreffenden ausländischen Behörden kommt		2.84%
Wahrscheinlichkeit, dass es zusätzlich zu einem erfolgreichen Lawful Access durch einen ausländischen Nachrichtendienst ohne Rechtsweggarantie kommt (trotz der Gegenmassnahmen[14)])		0.40%
Gesamtwahrscheinlichkeit eines erfolgreichen Lawful Access über den Cloud-Provider in der Betrachtungsperiode:* **		0.58%
Umschreibung in Worten (basierend auf Hillson****):	Sehr tief	
Soviele Jahre braucht es, damit es mit einer Wahrscheinlichkeit von **90 Prozent** mindestens ein Mal zu einem Lawful Access kommt:		1'988
Soviele Jahre braucht es, damit es mit einer Wahrscheinlichkeit von **50 Prozent** mindestens ein Mal zu einem Lawful Access kommt:		598
… unter der Annahme, dass die Wahrscheinlichkeit sich über Zeit weder erhöht noch reduziert (wie bei einem Münzwurf)		

Excel: https://www.rosenthal.ch/downloads/Rosenthal_Cloud_Lawful_Access_Risk_Assessment.xlsx
Vgl. auch den Beitrag unter https://bit.ly/2HaEet5 und Anhang unter https://bit.ly/2H8MyZY.
FAQ: https://www.rosenthal.ch/downloads/Rosenthal-LA-method-FAQ.pdf

Beurteilung ausländischer Lawful Access


Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

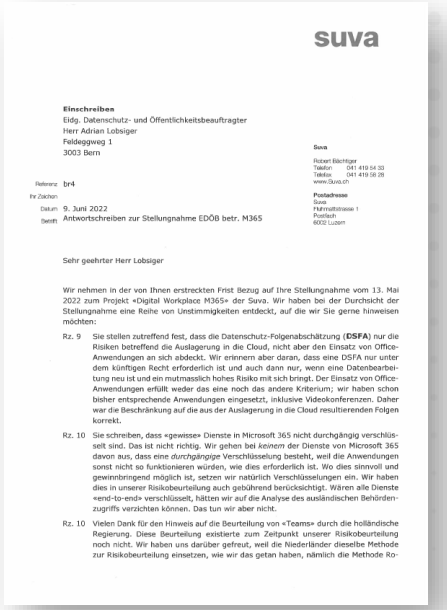
Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)

36. Insgesamt müsste sich die Zulässigkeit der Auslagerung und der damit einhergehenden Möglichkeit einer Datenbekanntgabe in die USA als Staat ohne angemessenes Datenschutzniveau selbst bei einer Bejahung der rechtlichen Zulässigkeit des risikobasierten Ansatzes der Suva als problematisch erweisen. Zum einen nahm sie diese Bewertung unter Anwendung von organspezifischen Kriterien vor, deren Geeignetheit zweifelhaft erscheint. Hinzu kommt, dass die Suva die Wahrscheinlichkeit eines Zugriffs durch US Behörden in ihrer Schätzung auf einen vernachlässigbar tiefen Wert gesenkt hat, dessen Herleitung aus Sicht des EDÖB in tatsächlicher Hinsicht unzureichend begründet bleibt.

37. Die Suva hat die Wahrscheinlichkeit eines Zugriffs durch eine Fremdbehörde nicht nur tief ausgewiesen, sondern aufgrund der angewandten Berechnungsmethode mit einer bis auf Hundertstel von Prozenten resp. mit auf Hunderte von Jahren extrapolierten Wahrscheinlichkeiten beziffert. Dieser Anspruch auf Wertgenauigkeit weckt Zweifel, steht er doch in einem offensichtlichen Kontrast zu den weiten Ermessensbandbreiten, die das Berechnungsmodell den Bearbeitungsverantwortlichen für die Annahmen einräumt, aus denen sich das bezifferte Risiko ableitet.

Auszug aus: Stellungnahme EDÖB vom 13. Mai 2022 zum M365-Projekt der Suva

Beurteilung ausländischer Lawful Access



suva

Einschreiben
Eidg. Datenschutz- und Öffentlichkeitsbeauftragter
Herr Adrian Lobsiger
Feldeggweg 1
3003 Bern

Suva
Robert Bächtiger
Telefon 041 419 64 33
Telefax 041 419 58 28
www.suva.ch

Postadresse
Suva
Fluhmattstrasse 1
Postfach
6002 Luzern

Referenz br4
Ihr Zeichen
Datum 9. Juni 2022
Betreff Antwortschreiben zur Stellungnahme EDÖB betr. M365

Sehr geehrter Herr Lobsiger

Wir nehmen in der von Ihnen erstreckten Frist Bezug auf Ihre Stellungnahme vom 13. Mai 2022 zum Projekt «Digital Workplace M365» der Suva. Wir haben bei der Durchsicht der Stellungnahme eine Reihe von Unstimmigkeiten entdeckt, auf die wir Sie gerne hinweisen möchten:

Rz. 9 Sie stellen zutreffend fest, dass die Datenschutz-Folgenabschätzung (**DSFA**) nur die Risiken betreffend die Auslagerung in die Cloud, nicht aber den Einsatz von Office-Anwendungen an sich abdeckt. Wir erinnern aber daran, dass eine DSFA nur unter dem künftigen Recht erforderlich ist und auch dann nur, wenn eine Datenbearbeitung neu ist und ein mutmasslich hohes Risiko mit sich bringt. Der Einsatz von Office-Anwendungen erfüllt weder das eine noch das andere Kriterium; wir haben schon bisher entsprechende Anwendungen eingesetzt, inklusive Videokonferenzen. Daher war die Beschränkung auf die aus der Auslagerung in die Cloud resultierenden Folgen korrekt.

Rz. 10 Sie schreiben, dass «gewisse» Dienste in Microsoft 365 nicht durchgängig verschlüsselt sind. Das ist nicht richtig. Wir gehen bei *keinem* der Dienste von Microsoft 365 davon aus, dass eine *durchgängige* Verschlüsselung besteht, weil die Anwendungen sonst nicht so funktionieren würden, wie dies erforderlich ist. Wo dies sinnvoll und gewinnbringend möglich ist, setzen wir natürlich Verschlüsselungen ein. Wir haben dies in unserer Risikobeurteilung auch gebührend berücksichtigt. Wären alle Dienste «end-to-end» verschlüsselt, hätten wir auf die Analyse des ausländischen Behördenzugriffs verzichten können. Das tun wir aber nicht.

Rz. 10 Vielen Dank für den Hinweis auf die Beurteilung von «Teams» durch die holländische Regierung. Diese Beurteilung existierte zum Zeitpunkt unserer Risikobeurteilung noch nicht. Wir haben uns darüber gefreut, weil die Niederländer dieselbe Methode zur Risikobeurteilung einsetzen, wie wir das getan haben, nämlich die Methode Ro-

Replik der Suva (online)

- Diese Prüfung – ob das defizitäre US-Recht zur Anwendung kommt –, hat der EDÖB unterlassen, mit dem Argument, es fehle ein risikobasierter Ansatz. Damit werden zwei **Fragen vermischt**: Unter welchen Voraussetzungen und worauf sind diese Gesetze überhaupt anwendbar, und – falls sie es sind – mit welcher Wahrscheinlichkeit macht sie sich eine Behörde zunutze. Nur die zweite Frage verdient den Namen "risikobasierter Ansatz". Die erste Frage darf man aber nicht ausser Acht lassen.
- Das **Formular von David Rosenthal** verwendet Wahrscheinlichkeitswerte nicht, weil ein Genauigkeitsanspruch besteht, sondern zur Selbstreflexion bei einer ansonsten gefühlsmässigen Risikoeinschätzung (das zeigt die Stellungnahme des EDÖB) und als Instrument der Risikokommunikation. Selbstverständlich gilt "garbage in, garbage out", aber bei welcher Einschätzung nicht?

Kommentar David Vasella auf datenrecht.ch

EDÖB tut nichts …

2. Der EDÖB sieht zurzeit keine Veranlassung, den ihm zur Kenntnis gebrachten Sachverhalt von Amtes wegen zu untersuchen. Je nach Entwicklung der sachverhältlichen Situation und Rechtslage behält er sich jedoch vor, in einem späteren Zeitpunkt aufsichtsrechtlich tätig zu werden.

Beurteilung ausländischer Lawful Access

tes Vorgehen für die Risikobeurteilung definiert.

Das Modell von David Rosenthal zur Ermittlung der Restrisiken eines Lawful Access ist breit abgestützt und anerkannt. Es wird deshalb für die Risikobeurteilung beim Einsatz von Cloud-Lösungen in der kantonalen Verwaltung als Standard festgelegt. Das Restrisiko und die durchgeführten Berechnungen zum Lawful Access sind in den ISDS-Konzepten der entsprechenden Cloud-Lösungen auszuweisen.

In Bezug auf das Risiko des Lawful Access gilt dabei das Folgende:

Auszug aus: Beschluss des Regierungsrates des Kantons Zürich vom 30. März 2022 (Nr. 542, "M365")

Beurteilung ausländischer Lawful Access

Staatsanwaltschaft des Kantons Basel-Stadt

- Die Bedenken bezüglich einer strafrechtlichen Verantwortlichkeit beschränkt sich mit Blick auf das geplante Outsourcing in die Microsoft Cloud, gemäss Ihren Angaben, auf die Frage des "Lawful Access" ausländischer Behörden auf die geheimnisgeschützten Daten. Im Vordergrund steht dabei die Gefahr eines Zugriffs US-amerikanischer Behörden auf Grundlage des US Cloud Acts. Dieser Einschätzung kann aus Sicht der Staatsanwaltschaft zugestimmt werden.

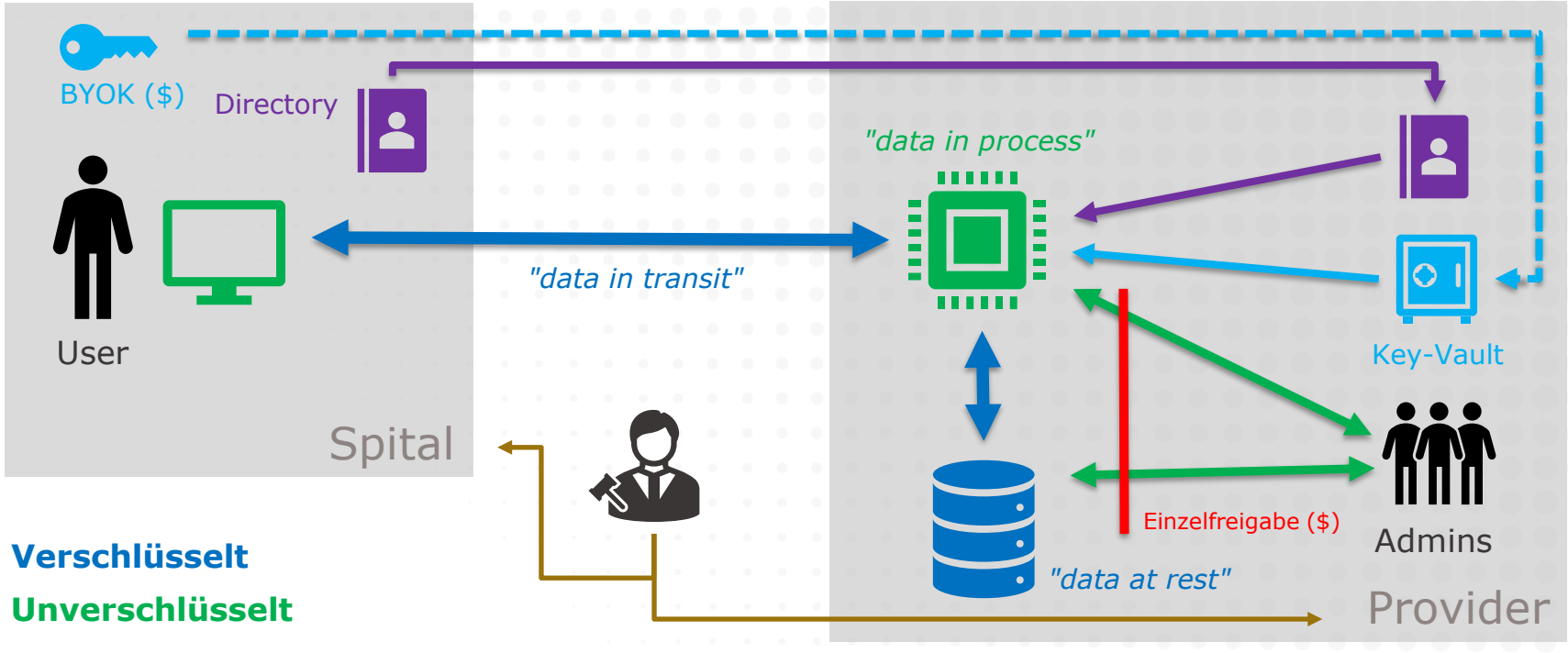
- Die Berechnung des Risikos eines ausländischen "Lawful Access" erscheint nach Ansicht der Staatsanwaltschaft grundsätzlich ein geeignetes Kriterium, um die Vertretbarkeit der Auslagerung auch vor einem strafrechtlichen Hintergrund zu beurteilen. Eine Überprüfung des Ergebnisses im konkreten Fall ist der Staatsanwaltschaft indes nicht möglich, da dieses letztlich von den Einschätzungen der einzelnen Berechnungsfaktoren abhängt. Diese können von aussen nicht überprüft werden.

Auszug aus: Schreiben der Staatsanwaltschaft Basel-Stadt nach einem Workshop zur Berechnung des Risikos eines ausländischen Behördenzugriffs im Kontext eines Cloud-Projekts des Basler USB/UKBB

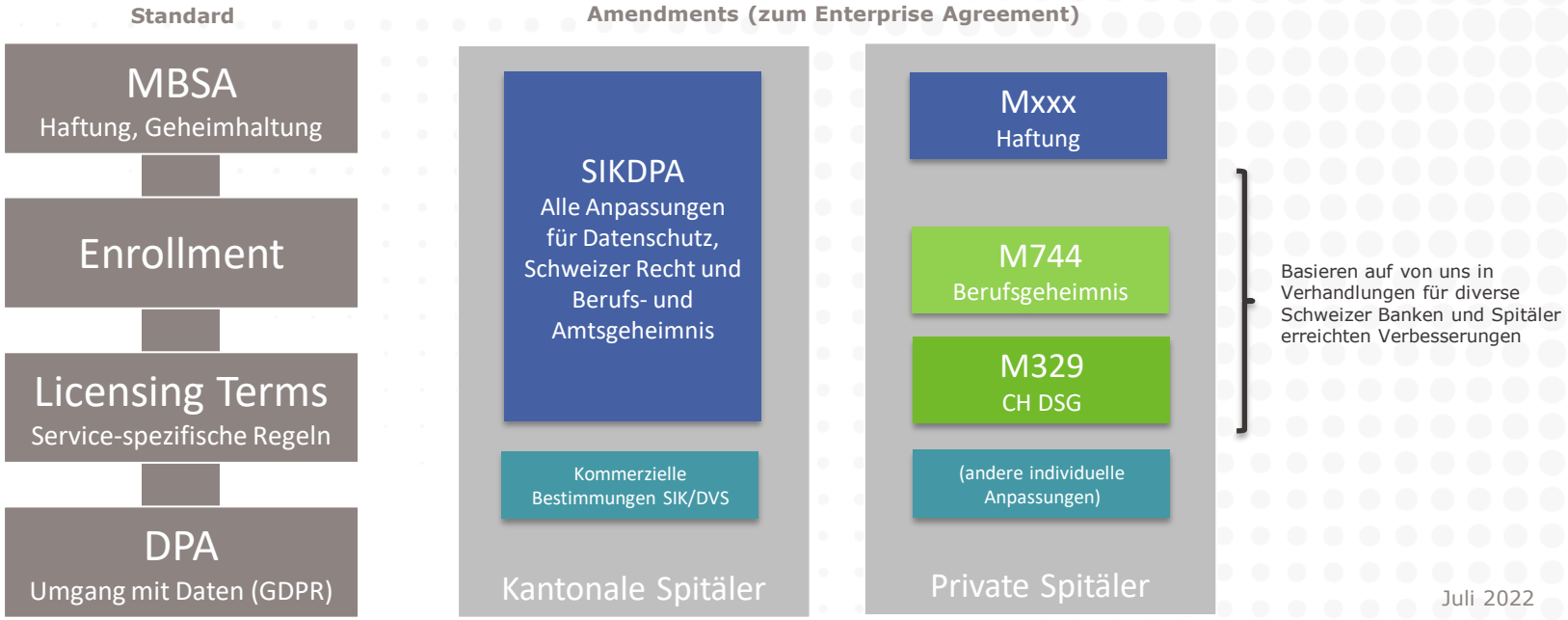
Welche Massnahmen treffen?

- **Berufsgeheimnis und Datenschutz**
  - Europäische Gegenpartei (Microsoft Ireland Operations Ltd.)
  - Datenlagerung in der Schweiz
  - Verschlüsselung von Daten (aber kein "bring-your-own-key")
  - Manuelle Provider-Zugriffe einschränken ("Lockbox" – teuer)
  - Vertraulichkeitsverpflichtung, Defend-your-data-Klausel
  - Schutzmassnahmen für Personendaten gelten für alle Inhalte
  - Einschränkung der Bearbeitung für eigene Providerzwecke
- **Weitere Massnahmen**
  - Konfiguration und Steuerung, Prüfrechte & Einbindung ins IKS, Backups & BCM, Exit-Konzept, Schweizer Recht/Gerichtsstand

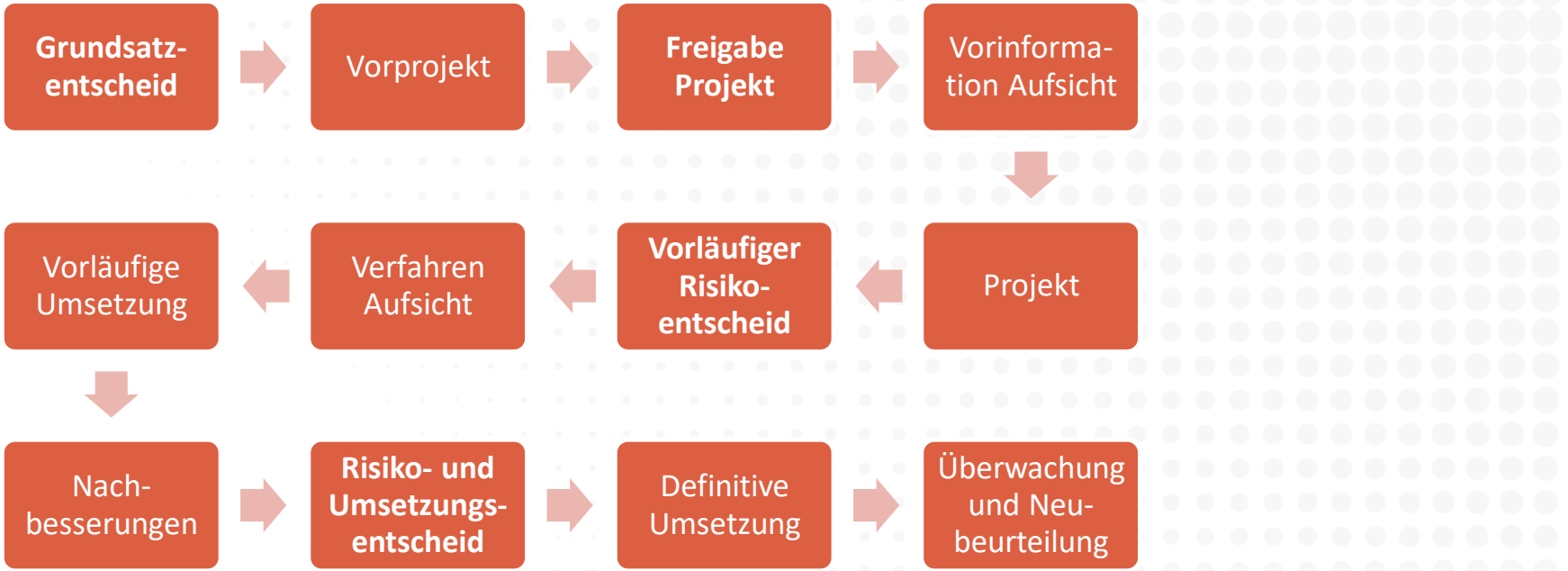
Wie Daten in der Cloud geschützt werden



Microsoft-Verträge: Heutige Vertragszusätze



Ein typischer Ablauf eines Cloud-Projekts



	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

Mehrere Streams,
mehrere Stakeholder

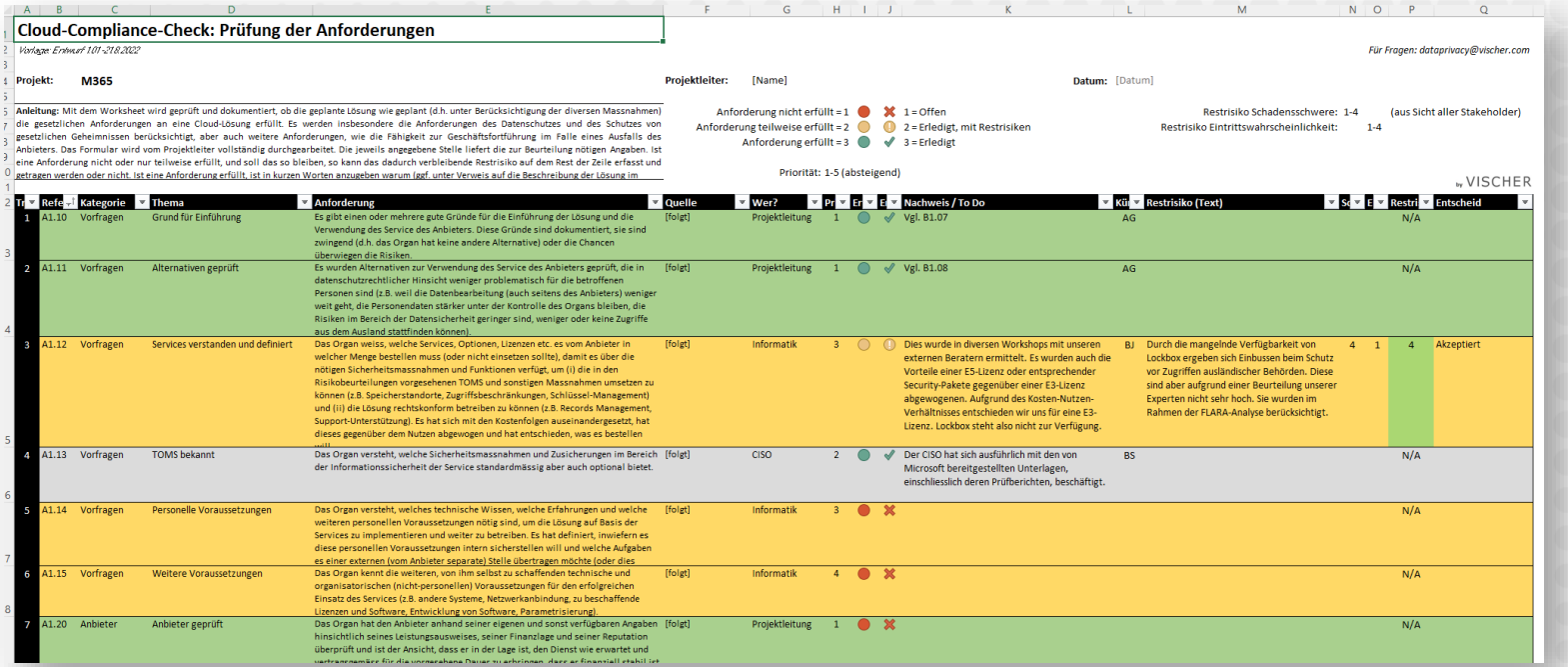
Dossier für Aufsicht und Spitalleitung

- **Projektbeschreibung**
- Risikobeurteilung **Informationssicherheit** inklusive BCM
- Risikobeurteilung **ausländischer Behördenzugriff**
- Beurteilung der **rechtlichen Vorgaben**
  - Prüfung Datenschutz (Datenbearbeitungen als solche, deren Auslagerung und eigenverantwortliche Bearbeitung des Providers), Datenschutz-Folgenabschätzung (DSFA)
  - Prüfung Berufs- und Amtsgeheimnis
  - Weitere aufsichtsrechtliche Vorgaben, "Gute Cloud-Praxis"
- **Vertrag** mit Zusätzen
- Beurteilung der **weiteren Risiken**

ISDS-Konzept

VISCHER

Tool zur Compliance- und Risikobeurteilung



Cloud-Compliance-Check: Prüfung der Anforderungen

Vorlage: Entwurf 1.01-27.8.2022

Für Fragen: dataprivacy@vischer.com

Projekt: M365 **Projektleiter:** [Name] **Datum:** [Datum]

Anleitung: Mit dem Worksheet wird geprüft und dokumentiert, ob die geplante Lösung wie geplant (d.h. unter Berücksichtigung der diversen Massnahmen) die gesetzlichen Anforderungen an eine Cloud-Lösung erfüllt. Es werden insbesondere die Anforderungen des Datenschutzes und des Schutzes von gesetzlichen Geheimnissen berücksichtigt, aber auch weitere Anforderungen, wie die Fähigkeit zur Geschäftsfortführung im Falle eines Ausfalls des Anbieters. Das Formular wird vom Projektleiter vollständig durchgearbeitet. Die jeweils angegebene Stelle liefert die zur Beurteilung nötigen Angaben. Ist eine Anforderung nicht oder nur teilweise erfüllt, und soll das so bleiben, so kann das dadurch verbleibende Restrisiko auf dem Rest der Zeile erfasst und getragen werden oder nicht. Ist eine Anforderung erfüllt, ist in kurzen Worten anzugeben warum (ggf. unter Verweis auf die Beschreibung der Lösung im

Anforderung nicht erfüllt = 1 — 1 = Offen
Anforderung teilweise erfüllt = 2 — 2 = Erledigt, mit Restrisiken
Anforderung erfüllt = 3 — 3 = Erledigt

Priorität: 1-5 (absteigend)

Restrisiko Schadensschwere: 1-4 (aus Sicht aller Stakeholder)
Restrisiko Eintrittswahrscheinlichkeit: 1-4

by VISCHER

Tr	Refe…	Kategorie	Thema	Anforderung	Quelle	Wer?	Pr	Er	E	Nachweis / To Do	Kü	Restrisiko (Text)	Sc	E	Restri	Entscheid
1	A1.10	Vorfragen	Grund für Einführung	Es gibt einen oder mehrere gute Gründe für die Einführung der Lösung und die Verwendung des Service des Anbieters. Diese Gründe sind dokumentiert, sie sind zwingend (d.h. das Organ hat keine andere Alternative) oder die Chancen überwiegen die Risiken.	[folgt]	Projektleitung	1			Vgl. B1.07	AG				N/A	
2	A1.11	Vorfragen	Alternativen geprüft	Es wurden Alternativen zur Verwendung des Service des Anbieters geprüft, die in datenschutzrechtlicher Hinsicht weniger problematisch für die betroffenen Personen sind (z.B. weil die Datenbearbeitung (auch seitens des Anbieters) weniger weit geht, die Personendaten stärker unter der Kontrolle des Organs bleiben, die Risiken im Bereich der Datensicherheit geringer sind, weniger oder keine Zugriffe aus dem Ausland stattfinden können).	[folgt]	Projektleitung	1			Vgl. B1.08	AG				N/A	
3	A1.12	Vorfragen	Services verstanden und definiert	Das Organ weiss, welche Services, Optionen, Lizenzen etc. es vom Anbieter in welcher Menge bestellen muss (oder nicht einsetzen sollte), damit es über die nötigen Sicherheitsmassnahmen und Funktionen verfügt, um (i) die in den Risikobeurteilungen vorgesehenen TOMS und sonstigen Massnahmen umsetzen zu können (z.B. Speicherstandorte, Zugriffsbeschränkungen, Schlüssel-Management) und (ii) die Lösung rechtskonform betreiben zu können (z.B. Records Management, Support-Unterstützung). Es hat sich mit den Kostenfolgen auseinandergesetzt, hat dieses gegenüber dem Nutzen abgewogen und hat entschieden, was es bestellen will.	[folgt]	Informatik	3			Dies wurde in diversen Workshops mit unseren externen Beratern ermittelt. Es wurden auch die Vorteile einer E5-Lizenz oder entsprechender Security-Pakete gegenüber einer E3-Lizenz abgewogenen. Aufgrund des Kosten-Nutzen-Verhältnisses entschieden wir uns für eine E3-Lizenz. Lockbox steht also nicht zur Verfügung.	BJ	Durch die mangelnde Verfügbarkeit von Lockbox ergeben sich Einbussen beim Schutz vor Zugriffen ausländischer Behörden. Diese sind aber aufgrund einer Beurteilung unserer Experten nicht sehr hoch. Sie wurden im Rahmen der FLARA-Analyse berücksichtigt.	4	1	4	Akzeptiert
4	A1.13	Vorfragen	TOMS bekannt	Das Organ versteht, welche Sicherheitsmassnahmen und Zusicherungen im Bereich der Informationssicherheit der Service standardmässig aber auch optional bietet.	[folgt]	CISO	2			Der CISO hat sich ausführlich mit den von Microsoft bereitgestellten Unterlagen, einschliesslich deren Prüfberichten, beschäftigt.	BS				N/A	
5	A1.14	Vorfragen	Personelle Voraussetzungen	Das Organ versteht, welches technische Wissen, welche Erfahrungen und welche weiteren personellen Voraussetzungen nötig sind, um die Lösung auf Basis der Services zu implementieren und weiter zu betreiben. Es hat definiert, inwiefern es diese personellen Voraussetzungen intern sicherstellen will und welche Aufgaben es einer externen (vom Anbieter separate) Stelle übertragen möchte (oder dies	[folgt]	Informatik	3								N/A	
6	A1.15	Vorfragen	Weitere Voraussetzungen	Das Organ kennt die weiteren, von ihm selbst zu schaffenden technische und organisatorischen (nicht-personellen) Voraussetzungen für den erfolgreichen Einsatz des Services (z.B. andere Systeme, Netzwerkanbindung, zu beschaffende Lizenzen und Software, Entwicklung von Software, Parametrisierung).	[folgt]	Informatik	4								N/A	
7	A1.20	Anbieter	Anbieter geprüft	Das Organ hat den Anbieter anhand seiner eigenen und sonst verfügbaren Angaben hinsichtlich seines Leistungsausweises, seiner Finanzlage und seiner Reputation überprüft und ist der Ansicht, dass er in der Lage ist, den Dienst wie erwartet und vertragsgemäss für die vorgesehene Dauer zu erbringen, dass er finanziell stabil ist	[folgt]	Projektleitung	1								N/A	

Die fünf Cloud-Fragen der Spitalleitung …

	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 Berufsgeheimnisses 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 Berufsgeheimnis 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 Spital haben können, richtig einschätzen, steuern und in Bezug zu den Restrisiken stellen, die wir sonst bzw. sowieso haben?	Welche weiteren Bedrohungen, welche für das Spital 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?

VISCHER

Fragen & Diskussion

drosenthal@vischer.com

Zürich
Schützengasse 1
Postfach
8021 Zürich, Schweiz
T +41 58 211 34 00

Basel
Aeschenvorstadt 4
Postfach
4010 Basel, Schweiz
T +41 58 211 33 00

Genf
Rue du Cloître 2-4
Postfach
1211 Genf 3, Schweiz
T +41 58 211 35 00

www.vischer.com