VISCHER

Datenschutzrechtliche Anforderungen.

Was dies für eine Beschaffung von Cloud-Lösungen bedeutet

David Rosenthal, Partner, VISCHER AG
22. August 2023

2022 gingen die Wogen etwas hoch

Quellen: Republik.ch, Inside-IT, Netzwoche

Stimmungslage im Datenschutz

https://www.datenschutz.ch

https://www.heise.de

- Der **US CLOUD Act** bewegt noch immer die Gemüter
  - Worum geht es wirklich? Müssen Daten vor US-Behörden besser geschützt sein als vor russischen Hackern?
  - Für einige ist die Cloud *per se* riskanter als alle anderen Lösungen, weshalb sie sie mit anderer Elle messen
- In der Praxis noch immer eine **"heisse Kartoffel"**
  - Organe müssen mit negativen Stellungnahmen rechnen, aber bisher nicht mit Interventionen; sie sind oft auf sich gestellt
  - Strengere Dossier-Prüfung sorgt durchaus für höhere Qualität
- Am Ende eine Entscheidung des jeweiligen **Leitungsorgans**
  - Mehrheit erlaubt sensible Daten in der Cloud auch ohne "E2EE"

E2EE = End-to-End-Encryption

Verlagert sich der Fokus weg vom Lawful Access?

privatim hat im Februar 2022 ein «Merkblatt Cloud-spezifische Risiken und Massnahmen» publiziert, das den öffentlichen Organen insbesondere auch die Beurteilung des Einsatze M365 ermöglichen soll. Der Entscheid des Regierungsrates des Kantons Zürich bedeutet für die öffentlichen Organe grundsätzlich nicht, dass sie vom Inhalt und dem empfohlenen Vorgehen in diesem Me privatim si den Kanto

Richtig!

Beim ausländischen ***Lawful Access*** handelt es sich um einen kleinen Teilaspekt in der Risikoanalyse, der über die zu treffenden technischen und organisatorischen Massnahmen oder – sofern diese nicht genügen – einen Verzicht auf die Auslagerung entscheiden kann.

Auf jeden Fall können die Ausführungen zum ausländischen ***Lawful Access*** nicht die anfangs erwähnten Schritte wie Rechtsgrundlagenanalyse, Schutzbedarfsanalyse sowie Risikoanalyse mit den Restrisiken und den Massnahmenplan ersetzen.

Quelle: Privatim

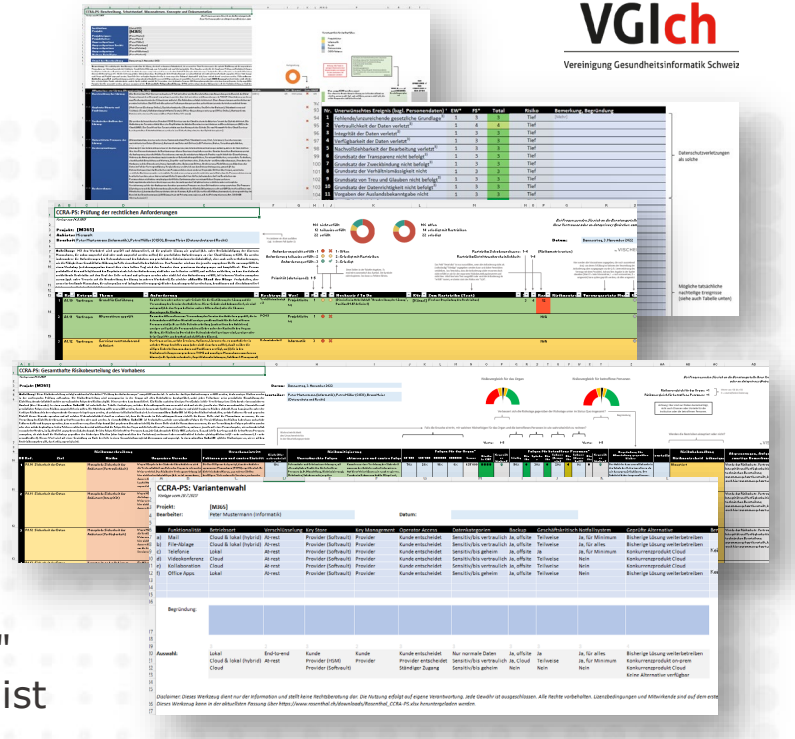
Was erarbeitet werden muss

- **Beschreibung**, was geplant ist (auch aus Datensicht)
- Schutzbedarf beurteilen, Risiken der Informationssicherheit und des Datenschutzes einschätzen und **Massnahmen** definieren
  - "ISDS-Konzept", "DSFA", "FLARA"-Beurteilung, InfoSec-Analyse
  - Div. weitere Konzepte (z.B. zu Einführung, IAM, Nutzung, Exit)
- Prüfung der **rechtlichen Anforderungen**
  - Rechtsgrundlagen-Analyse
  - Beurteilung Anforderungen Datenschutz, Amts- und Berufsgeheimnis, spezialgesetzliche Vorgaben, "Gute Cloud-Praxis"
  - Vertragsprüfung
- Gesamthafte Beurteilung der **Restrisiken**

Abkürzungen:
ISDS = Informationssicherheit und Datenschutz
DSFA = Datenschutz-Folgenabschätzung
FLARA = Foreign Lawful Access Risk Assessment
IAM = Identity and Access Management

Hilfsmittel: CCRA-PS

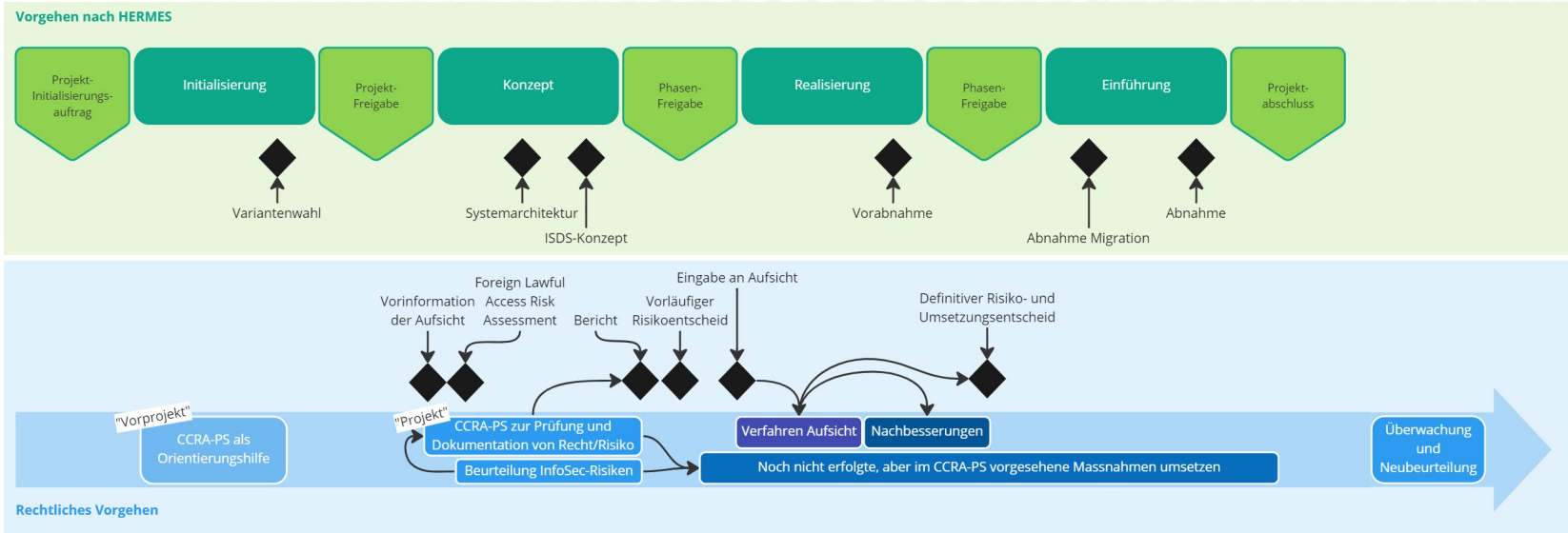
- **Prüfmethode** für (heikle) Cloud-Projekte
  - Projektbeschreibung
  - Rechtliche Anforderungen, "GCP"
  - DSFA, Gesamtrisikobeurteilung
- **Open Source** für die öffentliche Hand und Spitäler (d.h. kostenlos)*
  - Lanciert im November 2022
  - Bereits in zehn Kantonen im Einsatz
  - Nicht verwechseln mit "Methode Rosenthal I" betr. Lawful Access, die ebenfalls im Einsatz ist



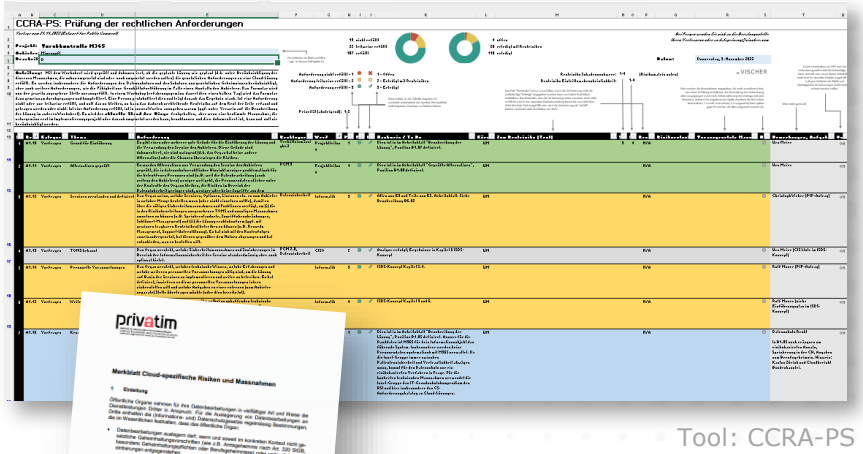
* https://www.rosenthal.ch/downloads/Rosenthal_CCRA-PS.xlsx
https://www.rosenthal.ch/downloads/VISCHER-Leitfaden-Public-Sector-Cloud.pdf

GCP = Gute-Cloud-Praxis
DSFA = Datenschutz-Folgenabschätzung

Zeitlicher Ablauf im Projekt



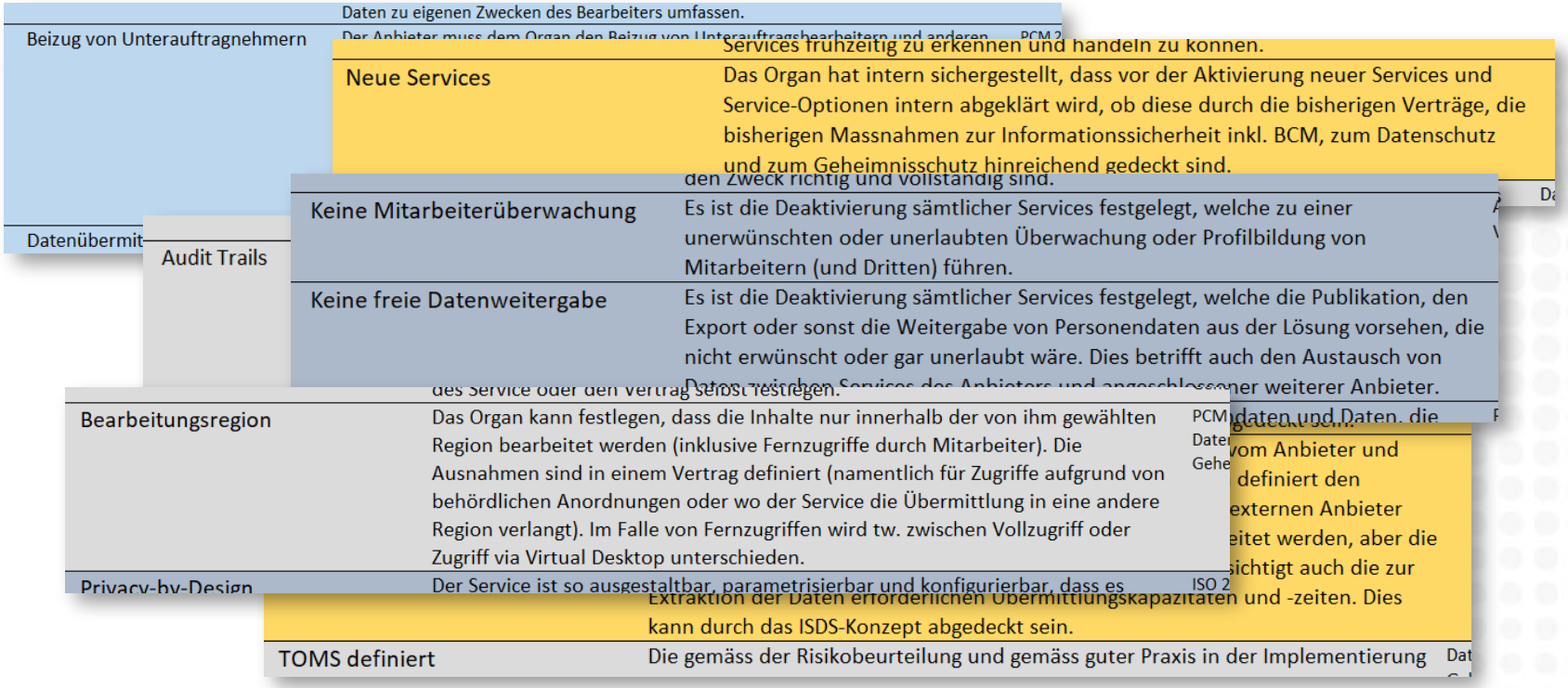
140 Anforderungen für Cloud-Projekte



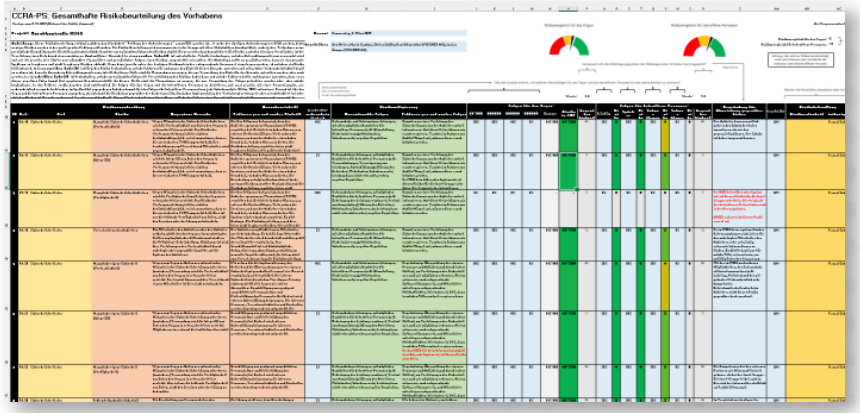
Tool: CCRA-PS

Wird typischerweise von den Fachstellen abgearbeitet und dokumentiert und dann in Workshops besprochen und finalisiert

- Wir sehen in den Workshops regelmässig dieselben **Defizite**
  - Rechtsgrundlagen, Gründe für den Wechsel und Alternativen zuwenig geklärt bzw. erläutert
  - Zu geringes Verständnis für das, was der Provider und seine Lösung wirklich tut/kann/hat
  - Zu oberflächliche Konzepte oder "es wird einfach gemacht"
  - Fehlende Prozesse für Provider- und Lösungs-Management
  - Exit-Planung/BCM mangelhaft


Daten zu eigenen Zwecken des Bearbeiters umfassen.
Beizug von Unterauftragnehmern
Der Anbieter muss dem Organ den Beizug von Unterauftragsbearbeitern und anderen
PCM 2
Services frühzeitig zu erkennen und handeln zu können.
Neue Services
Das Organ hat intern sichergestellt, dass vor der Aktivierung neuer Services und Service-Optionen intern abgeklärt wird, ob diese durch die bisherigen Verträge, die bisherigen Massnahmen zur Informationssicherheit inkl. BCM, zum Datenschutz und zum Geheimnisschutz hinreichend gedeckt sind.
den Zweck richtig und vollständig sind.
Datenübermit
Audit Trails
Keine Mitarbeiterüberwachung
Es ist die Deaktivierung sämtlicher Services festgelegt, welche zu einer unerwünschten oder unerlaubten Überwachung oder Profilbildung von Mitarbeitern (und Dritten) führen.
Keine freie Datenweitergabe
Es ist die Deaktivierung sämtlicher Services festgelegt, welche die Publikation, den Export oder sonst die Weitergabe von Personendaten aus der Lösung vorsehen, die nicht erwünscht oder gar unerlaubt wäre. Dies betrifft auch den Austausch von
des Service oder den Vertrag selbst festlegen.
ner weiterer Anbieter.
Bearbeitungsregion
Das Organ kann festlegen, dass die Inhalte nur innerhalb der von ihm gewählten Region bearbeitet werden (inklusive Fernzugriffe durch Mitarbeiter). Die Ausnahmen sind in einem Vertrag definiert (namentlich für Zugriffe aufgrund von behördlichen Anordnungen oder wo der Service die Übermittlung in eine andere Region verlangt). Im Falle von Fernzugriffen wird tw. zwischen Vollzugriff oder Zugriff via Virtual Desktop unterschieden.
PCM
Daten
Gehe
daten und Daten, die
vom Anbieter und
definiert den
externen Anbieter
eitet werden, aber die
sichtigt auch die zur
Privacy-by-Design
Der Service ist so ausgestaltbar, parametrisierbar und konfigurierbar, dass es
ISO 2
Extraktion der Daten erforderlichen Übermittlungskapazitäten und -zeiten. Dies kann durch das ISDS-Konzept abgedeckt sein.
TOMS definiert
Die gemäss der Risikobeurteilung und gemäss guter Praxis in der Implementierung
Dat

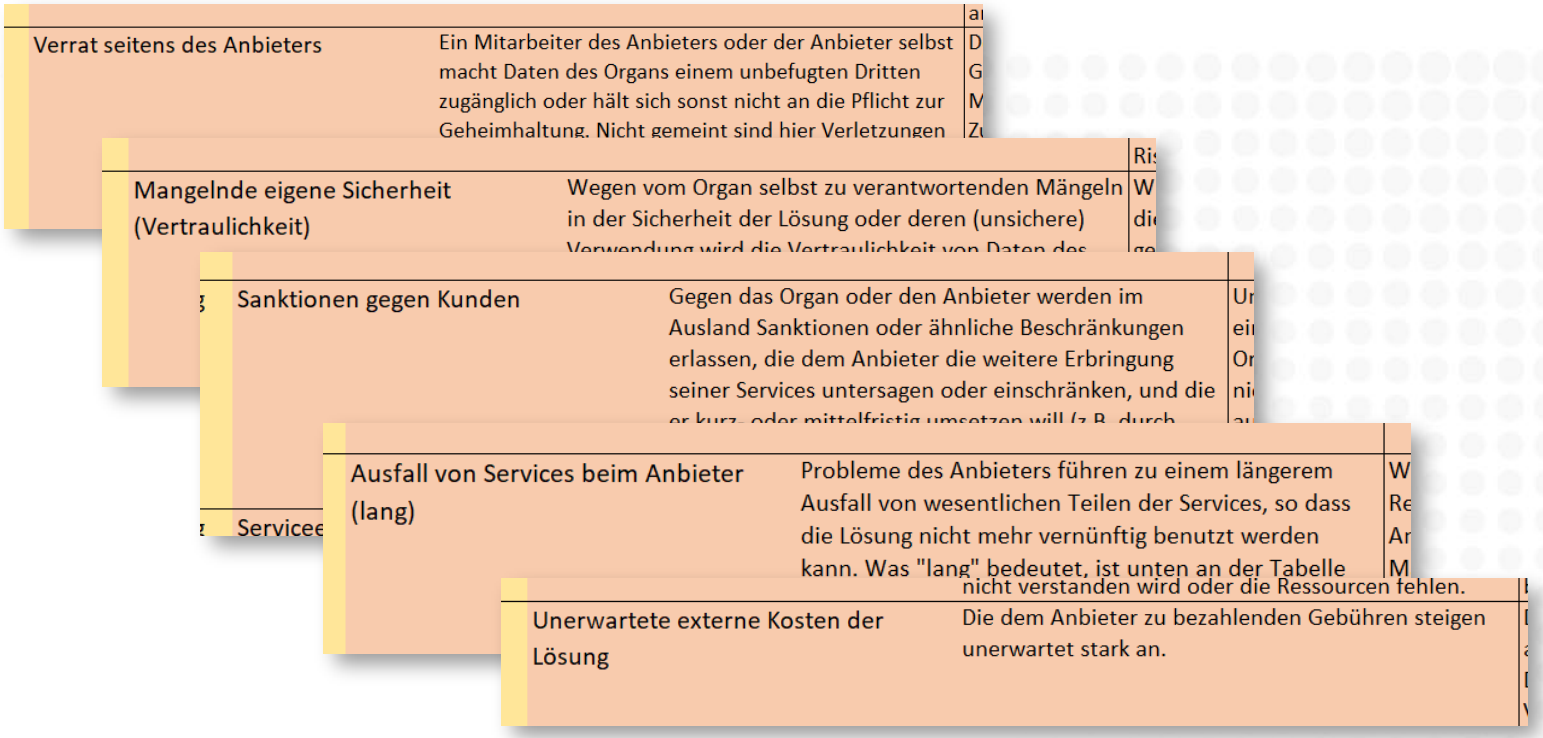
60 Risiken von Cloud-Projekten



Tool: CCRA-PS

Die Risikobeurteilung wird in Workshops von den Fachstellen (inkl. Nutzervertreter) interdisziplinär zusammen vorgenommen und danach den Risikoträgern mit den Massnahmen zur Mitigierung, damit diese darüber entscheiden

- Auch hier sehen wir immer wieder dieselben **Hotspots**
  - Fehlende "Business Impact Analysen" für den Fall eines Ausfalls, fehlende Absicherung
  - Schwieriger Exit aus der Cloud
  - Fehlende(s) Wissen, Personal und Prozesse zur Überwachung und Steuerung des Providers
  - Fehlnutzung durch Anwender
  - Kaum als Risiko empfunden: Politik/Reputation, Bezug zum Ausland, Informationssicherheit


Verrat seitens des Anbieters
Ein Mitarbeiter des Anbieters oder der Anbieter selbst macht Daten des Organs einem unbefugten Dritten zugänglich oder hält sich sonst nicht an die Pflicht zur Geheimhaltung. Nicht gemeint sind hier Verletzungen
Mangelnde eigene Sicherheit (Vertraulichkeit)
Wegen vom Organ selbst zu verantwortenden Mängeln in der Sicherheit der Lösung oder deren (unsichere) Verwendung wird die Vertraulichkeit von Daten des
Sanktionen gegen Kunden
Gegen das Organ oder den Anbieter werden im Ausland Sanktionen oder ähnliche Beschränkungen erlassen, die dem Anbieter die weitere Erbringung seiner Services untersagen oder einschränken, und die
Ausfall von Services beim Anbieter (lang)
Probleme des Anbieters führen zu einem längerem Ausfall von wesentlichen Teilen der Services, so dass die Lösung nicht mehr vernünftig benutzt werden kann. Was "lang" bedeutet, ist unten an der Tabelle
nicht verstanden wird oder die Ressourcen fehlen.
Unerwartete externe Kosten der Lösung
Die dem Anbieter zu bezahlenden Gebühren steigen unerwartet stark an.

Was ist wirklich geplant? Führungsentscheid!

CCRA-PS: Variantenwahl

Vorlage vom [illegible]023

Projekt: [M365]

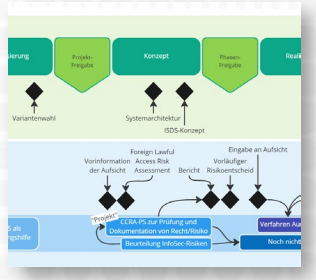
Bearbei Peter Mustermann (Informatik) **Datum:**

	Funktionalität	Betriebsort	Verschlüsselung	Key Store	Key Management	Operator Access	Datenkategorien	Backup	Geschäftskritisch	Notfallsystem	Geprüfte Alternative
a)	Mail	Cloud & lokal (hybrid)	At-rest	Provider (Softvault)	Provider	Kunde entscheidet	Sensitiv/bis vertraulich	Ja, offsite	Teilweise	Ja, für Minimum	Bisherige Lösung weiterbetreiben
b)	File-Ablage	Cloud & lokal (hybrid)	At-rest	Provider (Softvault)	Provider	Kunde entscheidet	Sensitiv/bis vertraulich	Ja, offsite	Teilweise	Ja, für alles	Bisherige Lösung weiterbetreiben
c)	Telefonie	Lokal	At-rest	Provider (Softvault)	Provider	Kunde entscheidet	Sensitiv/bis geheim	Ja, offsite	Ja	Ja, für Minimum	Konkurrenzprodukt Cloud
d)	Videokonferenz	Cloud	At-rest	Provider (Softvault)	Provider	Kunde entscheidet	Sensitiv/bis vertraulich	Ja, offsite	Teilweise	Nein	Konkurrenzprodukt Cloud
e)	Kollaboration	Cloud	At-rest	Provider (Softvault)	Provider	Kunde entscheidet	Sensitiv/bis vertraulich	Ja, offsite	Teilweise	Nein	Konkurrenzprodukt Cloud
f)	Office Apps	Lokal	At-rest	Provider (Softvault)	Provider	Kunde entscheidet	Sensitiv/bis geheim	Ja, offsite	Teilweise	Nein	Bisherige Lösung weiterbetreiben
	Begründung:										
		3	2	3	2	3	3	3	3	3	4
Auswahl:		Lokal	End-to-end	Kunde	Kunde	Kunde entscheidet	Nur normale Daten	Ja, offsite	Ja	Ja, für alles	Bisherige Lösung weiterbetreiben
		Cloud & lokal (hybrid)	At-rest	Provider (HSM)	Provider	Provider entscheidet	Sensitiv/bis vertraulich	Ja, Cloud	Teilweise	Ja, für Minimum	Konkurrenzprodukt on-prem
		Cloud		Provider (Softvault)		Ständiger Zugang	Sensitiv/bis geheim	Nein	Nein	Nein	Konkurrenzprodukt Cloud
											Keine Alternative verfügbar

Tool: CCRA-PS

Die beschaffungsrechtliche Herausforderung

- Compliance-**Prüfung** und Risiko-Beurteilung erfolgt am besten in der **Konzeptphase**, die einige Monate dauern kann
  - Sie muss für eine konkrete Lösung durchgeführt werden und findet daher i.d.R. *nach* der Variantenwahl statt
  - Entscheide über Parameter der Lösung (z.B. Verschlüsselung) und Nutzung (z.B. Datenklassen) sind zu Beginn oft noch offen
  - Die Durchführung erfordert i.d.R. fachliche und personelle Unterstützung von extern



- **Wann** das beschaffungsrechtliche **Verfahren durchführen**?
  - Drei Verfahren: Lösungssuche bzw. Berater für die Konzeptphase, Lösung (d.h. das "Produkt"), Berater für die Implementierung
  - Eine Herausforderung bringt vor allem die "Lösung" mit sich

Ein Zielkonflikt? Nicht unbedingt …

- Das **Beschaffungsrecht** erlaubt das Arbeiten mit
  - Anforderungskriterien (z.B. Kontrolle des Operator Access)
  - Optionen (z.B. betr. Schutzmassnahmen oder Subprovider)
  - Rücktrittsmöglichkeiten (z.B. bei regulatorischen Hindernissen)
  - Nachverhandlung (Essentialia dürfen nicht verändert werden)
  - Change Requests (z.B. Vorbehalte bei Rechtsentwicklungen)
- Will heissen: Bereits die Ausschreibung erfordert ein **sehr konkretes Verständnis** der regulatorischen Anforderungen
  - Profitieren von Erfahrungen und Vorarbeiten anderer
  - Vorsicht vor den Tücken des "Shared Responsibility Model" und vor Versprechungen, die nicht vertraglich festgehalten sind

Risiken schon vor dem Zuschlag beurteilen?

- Risiken der **Datenbearbeitung an sich**
  - Sie sind vom Zuschlag unabhängig
  - Sie können Anpassungen der Lösung erforderlich machen
  - Beispiele: Zu lange Datenspeicherung, zu viele Empfänger
- Risiken aufgrund des **Anbieters** und der Art und Weise, wie er die **Datenbearbeitung betreibt** (Bereitstellungsmodell etc.)
  - Sie können erst nach dem Zuschlag beurteilt werden
  - Beispiele: Datensicherheit, Ausfallrisiko, Telemetrie-Daten
  - Das Risiko erhöhende/senkende Faktoren sind allerdings bekannt
    - Mit Erfahrung vorhersehbar; sie können als Eignungs- oder Zuschlagskriterien abgefragt werden; Einsatz von Optionen

Wohin die Reise gehen muss …

- **Standardisierung** der Vertragsbedingungen auf einem für öffentliche Organe akzeptablen Niveau (mind. bei Hyperscalern)
  - Auch die Anbieter stecken noch in der Entwicklung
- Mehr **Erfahrungsaustausch** und **Lösungsorientierung**
  - Viele Projekte ähneln sich – warum das Rad immer neu erfinden?
  - Aber: Risikobeurteilungen sind subjektiv, erfordern Know-how und Umstände ändern sich – darum ist "copy & paste" heikel
  - Die Diskussion über die Risiken ist noch immer wenig sachlich und wenig konstruktiv – und ist damit kontraproduktiv
- **Austauschbarkeit** der Anbieter – und damit mehr Wettbewerb
  - Der Druck auf die Cloud-Provider muss aufrecht erhalten werden

VISCHER

Danke für Ihre Aufmerksamkeit!

Weitere Infos und Tools (inkl. CCRA-PS): www.rosenthal.ch

Fragen: 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