Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Informatiksteuerungsorgan des Bundes ISB

Dezember 2020

Bericht zur Bedarfsabklärung für eine «Swiss Cloud»

Inhaltsverzeichnis

Management Summary

Public Cloud-Leistungen werden heute weltweit sowie auch in der Schweiz breit genutzt. Sie ermöglichen Innovation, Flexibilität und Skalierbarkeit. Gleichzeitig stellen sich aber auch Fragen und Herausforderungen bezüglich Datensouveränität und der Abhängigkeit von Anbietern im Ausland, da Clouddienste keine Territorialgrenzen kennen. Die Verfügbarkeit, die Nutzung und die Bedingungen von Public Cloud Leistungen wird somit auch zur Standortfrage. Daher hat der Bundesrat am 6. April 2020 das Informatiksteuerungsorgan des Bundes ISB beauftragt, in Zusammenarbeit mit den Departementen, der Bundeskanzlei, den Kantonen sowie mit Wirtschaft und Wissenschaft zu prüfen, ob die Schweiz mit einer «Swiss Cloud» eine eigene Cloud- und Dateninfrastruktur anstreben soll. Gleichzeitig soll der Handlungsbedarf zur Verbesserung der Datensouveränität und zur Minimierung der Abhängigkeit von internationalen Public Cloud-Providern aufgezeigt werden.

Im vorliegenden Bericht werden die Erkenntnisse im Zusammenhang mit dem Cloud-Bedarf in der Schweiz aufgezeigt. Die Erkenntnisse der Studie beruhen auf über 200 Stellungnahmen aus einer Online-Umfrage, auf mehr als 30 Fachgesprächen mit Experten aus Organisation aller Grössen und Branchen sowie auf mehreren Workshops mit Vertretern aus Wirtschaft, Wissenschaft, Einsatzorganisationen und der öffentlichen Verwaltung.

Fazit

i) Bedarfsträger

Folgende Bereiche haben konkreten Bedarf angemeldet:

1. IT und Telekommunikation,
2. Finanzindustrie und Versicherungen,
3. weitere Bedarfsgruppen der Wirtschaft,
4. öffentliche Hand,
5. Bildung, Gesundheitswesen und Blaulicht-Organisationen,
6. Forschung,
7. krisenresistente und durchhaltefähige Organisationen sowie
8. internationale Organisationen.

ii) Bedarf

Die Nutzung von Cloud-Leistungen ist ein gemeinsames Bedürfnis der befragten Organisationen in der Schweiz. Dabei zeichnet sich ein klarer Paradigmenwechsel hin zu «Cloud First» Strategien ab, wonach IKT-Leistungen nur bei Vorliegen spezifischer Gründe auf Basis eigener Infrastrukturen erbracht werden.

Für den Einsatz von Cloud-Leistungen bedarf es geklärter und ggf. angepasster rechtlicher und regulatorischen Rahmenbedingungen.

Sorge bereitet den Befragten insbesondere das Risiko von nicht autorisierten Datenzugriffen, z. B. im Zusammenhang von nachrichtendienstlichen Ermittlungen. Die Annahme, dass eigene IT-Infrastrukturen grundsätzlich sicherer seien, ist allerdings trügerisch. Vielmehr ist die Anwendung angemessener Schutzkonzepte erforderlich.

Viele Organisation fordern Orientierungshilfen im Umgang mit Cloud-Technologien. Mögliche Mittel können z. B. im Bereitstellen von Best Practices, Normen zur Zertifizierung sowie standardisierten Service-Güteklassen bestehen oder darin, Hilfestellungen zu erhalten, um die Risiken realistisch abschätzen zu können.

Lediglich eine Minderheit der Befragten sieht Bedarf an einer schweizerischen oder durch den Bund kontrollierten Cloud-Infrastruktur, nämlich insbesondere für krisenresistente Infrastrukturen und im Bereich gemeinsamer Lösungen der öffentlichen Hand.

Die Mehrheit der Bedarfsträger bevorzugt kommerzielle Cloud-Leistungen, soweit den oben genannten Punkten geeignet Rechnung getragen wird.

Diese Erkenntnisse legen folgende Schlussfolgerungen nahe:

- Der Bedarf an einer «Swiss Cloud» in Gestalt einer öffentlich-rechtlichen Infrastruktur und als Erfolgsfaktor für den Standort Schweiz ist nicht ausgewiesen.
- Eine «Swiss Cloud» wird als Label in Form von geeigneten Rahmenbedingungen und Leitlinien für eine kompetente und sichere Nutzung von Cloud-Leistungen stark gefordert.

iii) Souveränitätskriterien für Leistungen, die in der Schweiz erbracht werden müssen

Unabhängig von der Frage, ob es eine Schweizer Cloud-Infrastruktur braucht, ist die Studie der Frage nachgegangen, welche Souveränitätskriterien ein solches Angebot erfüllen müsste. Für solche Cloud-Leistungen mit gegebenem Schutzbedarf, müssen beim Provider folgende Eigenschaften sichergestellt sein, die über die ganze Lebensdauer erfüllt sein müssen:

1. Trägerschaft ist in Schweizer Mehrheitsbesitz und ist wirtschaftlich nicht abhängig von anderen Ländern, in denen sie geschäftlich tätig ist;
2. Die Datenbearbeitung erfolgt ausschliesslich in der Schweiz;
3. Es besteht keine Datenherausgabepflicht an Dritte ausser derjenigen der Schweizer Justiz mit Rechtsschutz;
4. Die Organisation untersteht Schweizer Recht mit Gerichtsstand in der Schweiz.

iv) Weiteres Vorgehen

Daraus ergeben sich folgende nächste Schritte:

1. Zertifizierungssystem für Cloud-Leistungen prüfen und konkretisieren;
2. Rechtliche und regulatorische Fragestellungen zur Cloud-Nutzung klären und beantworten;
3. Die internationale Vernetzung und den Einbezug der Schweiz in europäischen Initiativen wie GAIA-X prüfen;
4. Im Rahmen des Aufbaus der Digitalen Verwaltung Schweiz (DVS) die institutionellen Grundlagen der Schweizer Verwaltung zur Nutzung von gemeinsamen Cloud-Leistungen entwickeln;
5. Die (völker-) rechtlichen Rahmenbedingungen für die Gewährleistung der Immunität von Daten in Public Clouds für internationale Organisationen prüfen.

Weitere Massnahmen für einzelne Bedarfsträger sind:

- Dialog mit den Branchen zur Entwicklung von Hilfsinstrumenten zur chancen- und risikobewussten Nutzung von Cloud Diensten führen;
- Bedarf und Weiterentwicklung von krisenresistenten Leistungen für Betreiber kritischer Infrastrukturen klären und konkretisieren.

1 Ausgangslage und Studiendesign

Public Cloud-Leistungen werden heute weltweit sowie auch in der Schweiz breit genutzt. Sie ermöglichen Innovation, Flexibilität und Skalierbarkeit. Gleichzeitig stellen sich aber auch Fragen und Herausforderungen bezüglich Datensouveränität und der Abhängigkeit von Anbietern im Ausland, da Clouddienste keine Territorialgrenzen kennen.

In den letzten Jahren zeichneten sich zwei Cloud-Entwicklungen ab:

1. Das Angebot wurde auf wenigen global verfügbaren Cloud-Plattformen **konsolidiert**.
2. Die Plattformen mit ihren verbundenen Dienstleistungen werden zunehmend voneinander **entkoppelt**.

Die Konsolidierung fand dabei meist um die technologisch innovativsten Plattformen (zum Cloud-Computing Kontext vgl. Anhang, Kapitel 9) statt, insbesondere wenn auch wirtschaftlich günstige Rahmenbedingungen vorhanden waren. Die Entkoppelung von bereits etablierten und global genutzten Plattformen und Ökosystemen findet dabei einerseits auf der technologischen und wirtschaftlichen Ebene statt, andererseits ist oft auch die politische Ebene daran beteiligt.

Mit steigender Verbreitung von Cloud-Leistungen angeboten durch die internationalen Public Cloud-Provider (sogenannte «Hyperscaler») nimmt auch das allgemeine Bewusstsein im Hinblick auf deren Umgang mit den ihnen anvertrauten Daten zu. Ob und vor allem auch welche Daten in der Cloud gespeichert werden dürfen, stehen aus diesem Grund zusehends im Zentrum von Abklärungen. Die mediale Präsenz rund um den amerikanischen CLOUD Act[1], die internationale Vereinbarung «Privacy Shield»[2] zwischen der EU und den USA, sowie die europäische Datenschutz-Grundverordnung (EU-DSGVO)[3] trägt ebenfalls zu diesem gesteigerten Bewusstsein bei.

Einhergehend mit der technologischen Konsolidierung auf den jeweils innovativsten Plattformen ist eine erhebliche Abhängigkeit bei der Nutzung der entsprechenden Cloud-Leistungen entstanden. Sie birgt nicht nur technologische und wirtschaftliche Konsequenzen, sondern hat das Potenzial, (geo-) politischer Machtfaktor zu werden.

Vor diesem Hintergrund stellt sich für viele Organisationen in der Schweiz, inklusive der öffentlichen Hand, die Frage, wie der geeignete Umgang mit Cloud-Leistungen ist. Der Bundesrat hat daher an seiner Sitzung vom 6. April 2020 das Informatiksteuerungsorgan des Bundes ISB beauftragt, in Zusammenarbeit mit den Departementen, der Bundeskanzlei, den Kantonen sowie mit Wirtschaft und Wissenschaft vertieft zu prüfen, ob die Schweiz mit einer «Swiss Cloud» eine eigene Cloud- und Dateninfrastruktur anstreben soll.

Diesen Auftrag etwas weiter gefasst geht es um das Anliegen, die Souveränität über die eigenen Daten sicherzustellen, also über die (vollständige) Kontrolle über gespeicherte und verarbeitete Daten zu verfügen sowie über die unabhängige Entscheidung, wer darauf zugreifen darf. Nicht nur die Bundesverwaltung und die Behörden aller Staatsebenen sehen sich mit diesen Abhängigkeiten und der Frage der «Datensouveränität» konfrontiert, sondern auch Bürgerinnen und Bürger, Wirtschaft und Forschung

---

[1] Vgl. https://www.congress.gov/bill/115th-congress/house-bill/4943, zuletzt aufgerufen am 27. November 2020.

[2] Vgl. https://www.europarl.europa.eu/RegData/etudes/IDAN/2018/625151/EPRS_IDA(2018)625151_EN.pdf, zuletzt aufgerufen am 27. November 2020.

[3] Vgl. https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en, zuletzt aufgerufen am 27. November 2020.

sowie internationale Organisationen. Dieses Thema wird auch in anderen Ländern rege diskutiert (vgl. Kapitel 2).

Daraus ergeben sich die folgenden drei Fragen:

1. In welchen Bereichen besteht für wen welcher Handlungsbedarf?
2. Wie kann die Datensouveränität verbessert werden?
3. Wie kann besser mit dem Risiko umgegangen werden, von grossen globalen Cloud-Providern abhängig zu sein?

Diese Fragen werden im Rahmen der vom ISB durchgeführten Machbarkeitsstudie beantwortet, indem der mittel- bis langfristige Bedarf ermittelt sowie mögliche Ausgestaltungen und deren Machbarkeit geprüft werden. Diese Arbeiten erfolgen in zwei Etappen.

Während der ersten Etappe, die Ende Oktober 2020 abgeschlossen wurde, lag der Fokus auf den Aspekten Bedarf und Notwendigkeit. Dafür hat das ISB im Zeitraum von Mitte Juli bis Mitte September 2020 eine Bedarfserhebung durchgeführt. Diese ist Gegenstand des vorliegenden Berichts. In der zweiten Etappe werden die Aspekte zur Ausgestaltung und Machbarkeit untersucht.

1.1 Ziele

Für die Bedarfserhebung wurden folgende Ziele definiert:

1. Die Erhebung muss breit abgestützt sein und Stakeholder aus der öffentlichen Hand (alle föderalen Ebenen), Wirtschaft und Wissenschaft berücksichtigen.
2. Ausgewählte Vertreter von Bund, Kantonen, Wirtschaft und Wissenschaft sind bei der Bedarfserhebung einzubinden.
3. Die Bedarfserhebung soll die Machbarkeitsstudie und die Erarbeitung möglicher Umsetzungsvarianten einer Swiss Cloud bestmöglich unterstützen.
4. Die Erhebung soll zeitnah und mit einem Zwischenbericht z. H. des Bundesrats bis Oktober 2020 erfolgen.

1.2 Vorgehen

Abbildung 1: High-level Vorgehen

Der Bedarf bezüglich einer «Swiss Cloud» wurde mit Experten aus den Stakeholdergruppen «Öffentliche Hand», «Wirtschaft» und «Wissenschaft» erhoben (siehe Abbildung 1).

Branchenexperten formulierten Hypothesen auf Basis eines Vergleichs von Cloud-Initiativen anderer Länder und Organisationen. Die Grundlage bildeten fünf Zukunftsbilder (siehe Abs. 1.3) und eine Kategorisierung, die die Beschreibung des aktuellen und künftigen Bedarfs zu strukturieren halfen.

Im Projektteam und in Vorgesprächen mit Branchenvertretern wurden die Zukunftsbilder überprüft. Mit dieser Grundlage wurde eine breit angelegte, mehrsprachige, quantitativ angelegte Online-Umfrage (Details im Anhang, Kapitel 11) durchgeführt. Die quantitativen Ergebnisse wurden in qualitativen Stakeholder-Gesprächen und drei Gruppen-Workshops vertieft.

Abbildung 2: Vorgehen (Fokus Umfrage und Vertiefung)

Die Teilnahme an der Online-Umfrage stand grundsätzlich allen interessierten Kreisen offen. Darüber hinaus wurden systematisch verschiedene Gruppen angesprochen und zur Teilnahme eingeladen:

- Im Bereich der öffentlichen Hand (einschliesslich Einsatzorganisationen) sind verschiedene Bundesstellen und – teilweise über die Schweizerische Informatikkonferenz SIK – mehrere Kantone und Gemeinden einbezogen worden.
- Für den Wirtschaftsbereich erfolgte der Einbezug entlang der allgemeinen Systematik der Wirtschaftszweige (NOGA 2008) des BFS[4]. Mehrere Dachorganisationen bzw. -verbände wurden eingeladen, ihre Mitglieder in die Umfrage einzubinden; zudem wurden verschiedene NGOs und NPOs direkt angeschrieben.
- Im Bereich Wissenschaft wurden die Bildung, die Forschung und mehrere Hochschulen und Universitäten angesprochen.

Aufgrund dessen, dass der Fokus der Studie zunächst auf die Bedarfsabklärung gerichtet war, standen Anbieter von Cloud-Dienstleistungen nicht im Vordergrund. Diese waren jedoch eingeladen, ihre Erfahrungen und Erkenntnisse zu teilen und konnten sich im Rahmen der Workshops einbringen.

[4] Siehe https://www.bfs.admin.ch/bfs/de/home/statistiken/industrie-dienstleistungen/nomenklaturen/noga.assetdetail.415633.html, zuletzt aufgerufen am 27. November 2020.

1.3 Mögliche Bausteine einer «Swiss Cloud»

Um den Lösungsraum für künftige Cloud-Nutzungsszenarien in der Schweiz zu strukturieren und den Begriff «Swiss Cloud» zu operationalisieren, wurden fünf sogenannte «Bausteine» (siehe Anhang, Abs. 11.2) entwickelt. Dabei wurden systematisch die relevanten Aspekte und Ausprägungen berücksichtigt:

- Bedürfnisse der Schweizer Akteure,
- Angebot der Cloud-Provider,
- Rolle des Staates,
- organisatorische Varianten,
- mögliche Fertigungstiefen,
- notwendige Rahmenbedingungen für die Nutzung von Cloud-Leistungen.

Die Bausteine sind unabhängige Ideen für mögliche Stossrichtungen. Sie sind kombinierbar und müssen nicht zwingend aufeinander aufbauen.

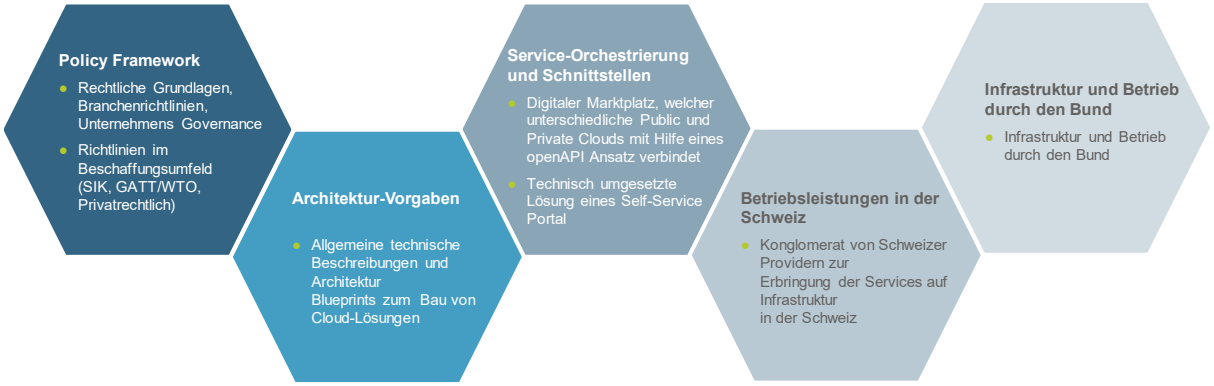

Abbildung 3: Konkretisierung künftiger Cloud-Nutzungsszenarien mittels fünf Bausteinen

Baustein 1: Policy Framework

Dieser Baustein schafft einheitliche, verständliche rechtliche und regulatorische Rahmenbedingungen, welche es Organisationen ermöglichen, belastbare Entscheidungen zu treffen, wann welche Cloud-Leistungen in welcher Form genutzt werden.

Baustein 2: Architektur-Vorgaben

Mit diesem Baustein werden technische Ziel-Architekturen und Blueprints zur Nutzung von Cloud-Lösungen definiert. Sie dienen dazu, einerseits die Leistungsbezüger als Anwender technologisch zu befähigen und anderseits den Cloud-Providern einen Orientierungsrahmen für deren Ausgestaltung der Cloud-Leistungen zu bieten.

Baustein 3: Service-Orchestrierung und Schnittstellen

Dieser Baustein schafft einen Marktplatz für Cloud-Leistungen, der Cloud-Leistungen verschiedener Service-Provider technisch integriert und damit für die Leistungsbezüger einfach beziehbar macht. Durch den Einsatz von offenen Schnittstellen («open API») können Leistungen verschiedener Anbieter kombiniert oder durcheinander substituiert werden.

Baustein 4: Betriebsleistungen in der Schweiz

Mit diesem Baustein gibt es ein Konglomerat von Schweizer Providern, die Cloud-Leistungen auf Infrastruktur innerhalb der Schweiz erbringen. Die Aufteilung der technischen Komponenten und Fähigkeiten unter den Providern zur Erbringung der Cloud-

Leistungen müsste in einer weiteren Konkretisierung des Bausteins weitergehend betrachtet und ausgestaltet werden.

Baustein 5: Infrastruktur und Betrieb durch den Bund

Mit diesem Baustein besitzt die Bundesverwaltung eine eigene Cloud-Plattform, die sie auch vollständig selbst betreibt. Das genaue Leistungsportfolio sowie die angestrebten Leistungsbezüger der entsprechenden Cloud-Leistungen müsste in einer weiteren Konkretisierung des Bausteins weitergehend betrachtet und ausgestaltet werden.

1.4 Datenbasis und methodische Einordnung

Ziel der Abklärungen war eine breit abgestützte, nicht jedoch repräsentative Bedarfserhebung. Die Umfrage stand allen interessierten Personen zur Teilnahme offen. Angesprochen wurden spezifisch Expertinnen und Experten von Organisationen aller Branchen, Grössen und Sprachregionen in der Schweiz. Insgesamt 332 Personen haben sich für die Teilnahme registriert; davon haben 243 Personen an der Umfrage teilgenommen, wovon 203 Personen die Umfrage vollständig beantwortet haben. Dabei waren alle Sektorgruppen vertreten (siehe Abbildung 4, Details im Anhang, Kapitel 11):

- Die öffentliche Hand wurde vor allem durch Vertreter aus den Reihen der Kantone und der Bundesverwaltung gut abgedeckt, wogegen von Gemeindeebene keine Vertreter an der Umfrage bzw. den Gesprächen und Workshops vertreten waren.
- Die Wirtschaft war gut über viele NOGA-Sektoren vertreten. Wichtige Sektoren, die an der Studie nicht teilgenommen haben, umfassen die Pharma- und Chemieindustrie, das Baugewerbe, das Grundstück- und Wohnungswesen sowie die Kunst- und Kulturbranche. Verlässliche Aussagen basierend auf der Umfrage können spezifisch nur für den IT- und Telekommunikationssektor sowie den Finanz- und Versicherungssektor getroffen werden. Die weiteren Sektoren wurden in Interviews und Workshops beleuchtet, repräsentieren jedoch keine breite Abdeckung, sondern nur Einzelmeinungen und -bedürfnisse.
- Der Rücklauf der Umfrage für die Sektoren Bildung, Gesundheitswesen und Blaulicht-Organisationen war nicht signifikant, wodurch das Meinungsbild und der Bedarf sich hauptsächlich auf Einzelaussagen und Meinungen aus Interviews, Hintergrundgesprächen und Workshops stützt.

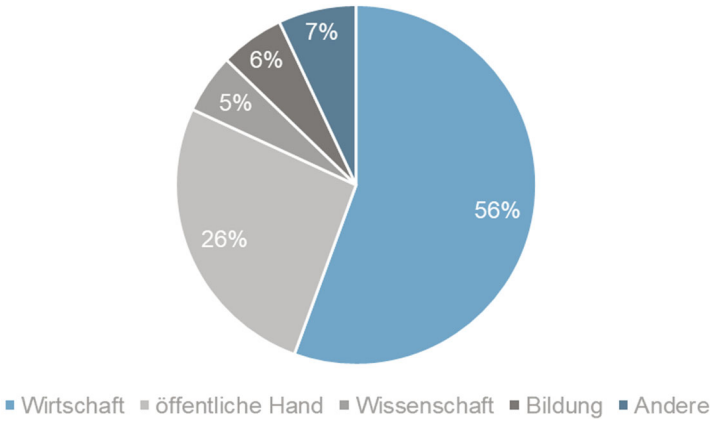

Abbildung 4: Verteilung der Umfrage-Teilnehmenden nach Sektorgruppen

Der Datensatz mit 18’965 Datenpunkten wurde auf Anomalien überprüft. Dafür wurden zuvor definierte Kontrollfragen und Erkenntnisse aus Gesprächen genutzt. Weil sich die Umfrage insbesondere an Experten richtete, war ein Experten-Bias vermutet (Cloud-Experten, die z. B. das vorhandene Knowhow oder Probleme anders einschätzen als die Mehrheit der restlichen Personen). Zudem haben während des Studienzeitraums verschiedene IKT-nahe Wirtschaftsverbände und Anbieter über ihre Kanäle zur Teilnahme aufgerufen und mit eigenen Informationsanlässen und Unterlagen die Meinungsbildung begleitet bzw. beeinflusst. So hat die Bedarfsgruppe «IT- und Telekommunikation» an der Studie ein grosses Interesse und viel Präsenz gezeigt. Ihre Rolle als Anbieterin und Konsumentin lässt sich nur bedingt unterscheiden. Entsprechend sind die Umfrageresultate für diese Gruppe aufgrund der Interessenslagen mit Sorgfalt zu interpretieren. Insgesamt konnte eine systematische Verzerrung nicht nachgewiesen werden; die hier dargelegten, zusammengefassten Umfragebefunde werden als robust und als übereinstimmend mit den Aussagen aus den Gesprächen und Workshops eingeschätzt.

2 Cloud-Initiativen anderer Länder

Viele andere Länder und Staatenverbünde haben in den letzten rund zehn Jahren Cloud-Initiativen gestartet. Deswegen positioniert bereits der Auftrag des Bundesrats diese Studie im Kontext ähnlich gelagerter Initiativen. Grund genug, einen Blick über die Landesgrenzen hinaus zu werfen.

Der primäre Treiber für länderspezifische Cloud-Initiativen bestand historisch darin, die Beschaffung von Cloud-Leistungen, gerade im öffentlichen Sektor, zu vereinfachen und zu standardisieren. Das Ziel war, Risiken insbesondere in den Bereichen der Informationssicherheit zu minimieren.[5] Mit der Zeit haben sich die Projekte weiterentwickelt. Vier ausgewählte Initiativen werden nachfolgend dargestellt.

2.1 Europäische Cloud-Initiativen

In Europa werden verschiedene strategische Initiativen für sichere Cloud-Leistungen zur Erhöhung der digitalen Souveränität und Unabhängigkeit Europas gegenüber externer Technologie gefördert, insbesondere:

1) ENISA

Die Agentur der Europäischen Union für Cybersicherheit (engl. European Network and Information Security Agency, ENISA) ging aus der 2004 gegründeten Agentur für Netz- und Informations-Sicherheit hervor und hat ein gemeinsames Risiko-Management-Framework und einen Beschaffungsleitfaden für Cloud-Leistungen entwickelt. Darin werden die relevanten Sicherheitsaspekte im Rahmen der Beschaffung und des Einsatzes von Cloud-Leistungen in öffentlichen Organisationen adressiert sowie Empfehlungen zum Umgang mit entsprechenden Risiken aufgezeigt.

[5] Vgl. hierzu exemplarisch die Publikationen der ENISA, https://www.enisa.europa.eu/, zuletzt aufgerufen am 27. November 2020.

2) GAIA-X

Das 2019 vorgestellte Projekt GAIA-X wird in einem Public-Private-Partnership-Modell insbesondere durch Deutschland und Frankreich vorangetrieben und ist seit 2020 Teil der gemeinnützigen Gaia-X Foundation mit Sitz in Brüssel.[6] Die offizielle Webseite des deutschen Bundesministeriums für Wirtschaft und Energie (BMWI)[7] beschreibt die Zielsetzung wie folgt:

> *«Ziel ist eine sichere und vernetzte Dateninfrastruktur, die den höchsten Ansprüchen an digitale Souveränität genügt und Innovationen fördert. In einem offenen und transparenten digitalen Ökosystem sollen Daten und Dienste verfügbar gemacht, zusammengeführt und vertrauensvoll geteilt werden können. […] Zum aktuellen Zeitpunkt sind bereits Vertreter aus sieben europäischen Ländern aktiv am Projektgeschehen beteiligt. […]*
>
> *Europa tätigt umfangreiche Investitionen in digitale Technologien und innovative Geschäftsmodelle. Dabei sollen diejenigen, die Innovationen vorantreiben, auch ökonomisch davon profitieren. So werden Wertschöpfung und Beschäftigung in Europa gesichert.*
>
> *Damit Unternehmen und Geschäftsmodelle aus Europa heraus weltweit wettbewerbsfähig sein können, braucht es ein offenes digitales Ökosystem. Dieses sollte sowohl die digitale Souveränität der Nutzer von Cloud-Leistungen als auch die Skalierungsfähigkeit europäischer Cloud-Anbieter ermöglichen.»*

Diese Zielsetzung soll durch einen umfassenden Architekturansatz (vgl. Abbildung 5) umgesetzt werden, der z. B. den Einsatz offener Technologien, Sicherheit auf Netzebene, gemeinsame Standards und Regulierungen sowie einen einheitlichen Daten- und Serviceraum vorsieht.

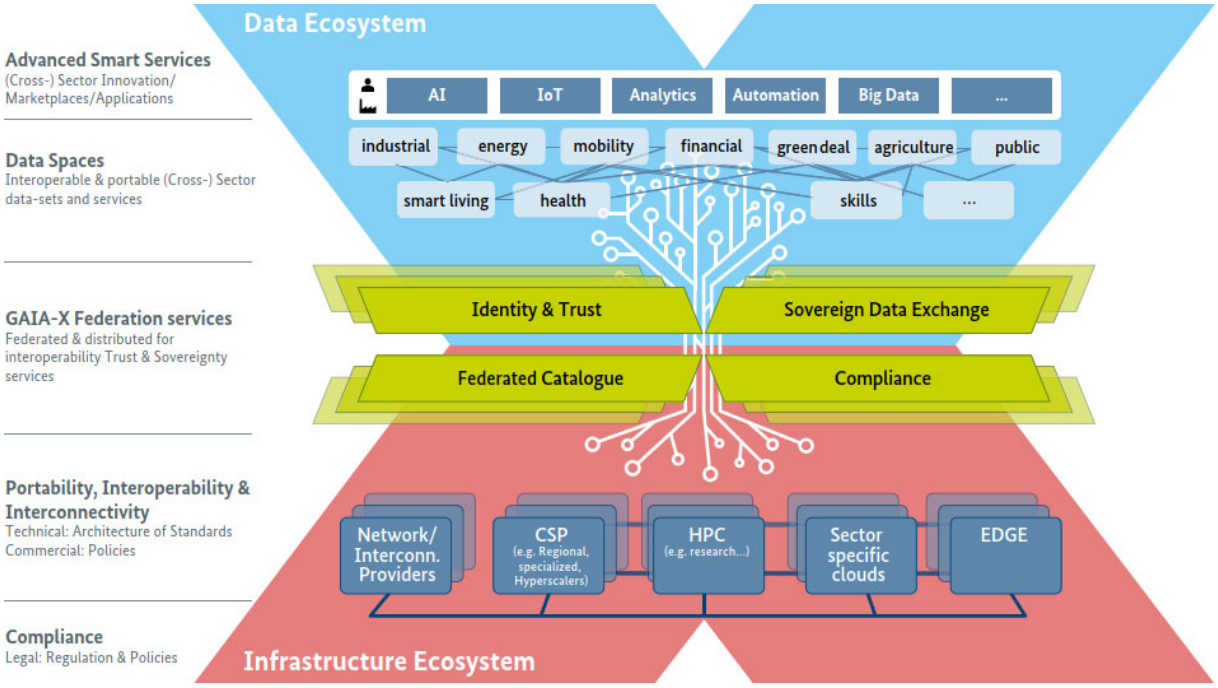

Abbildung 5: Architekturansatz von GAIA-X (Quelle BMWi)

[6] Vgl. https://www.bmwi.de/Redaktion/EN/Publikationen/gaia-x-the-european-project-kicks-of-the-next-phase.pdf?__blob=publicationFile&v=7, zuletzt aufgerufen am 27. November 2020.

[7] Vgl. https://www.bmwi.de/Redaktion/DE/Dossier/gaia-x.html, zuletzt aufgerufen am 27. November 2020.

3) Gemeinsame Cloud Erklärung

Die EU will auf Basis der gemeinsamen Erklärung der Mitgliedstaaten zur Cloud vom 15. Oktober 2020[8] in den folgenden drei Handlungsfeldern ihre Aktivitäten verstärken:

- Erhöhen von privaten, nationalen und europäischen Investitionen in wettbewerbsfähige, nachhaltige und sichere Cloud Infrastrukturen und Leistungen im Rahmen der neu gegründeten European Alliance on Industrial Data and Cloud
- Definieren eines gemeinsamen Ansatzes zum europaweiten Föderieren von Cloud Fähigkeiten und Leistungen
- Fördern von noch sichereren, interoperablen und energie-effizienten Rechenzentren und Cloud-Leistungen

2.2 UK Government G-Cloud

Die UK Government Cloud (G-Cloud) ist eine Initiative der britischen Regierung zur Erleichterung der öffentlichen Beschaffung von Cloud-Leistungen durch Regierungsstellen und zur Förderung der regierungsweiten Einführung von Cloud-Computing. G-Cloud umfasst eine Reihe von Rahmenvereinbarungen mit Anbietern von Cloud-Leistungen wie Amazon, Google oder Microsoft und eine Auflistung ihrer Leistungen in einem Online-Shop – dem sogenannten Digital Marketplace. Dieser ermöglicht es Organisationen des öffentlichen Sektors, die Leistungen zu vergleichen und zu beschaffen, ohne einen eigenen vollständigen Marktanalyse- und Beschaffungsprozess durchführen zu müssen. Die Aufnahme in den digitalen Marktplatz erfordert eine Selbstbestätigung der Einhaltung der Vorschriften, gefolgt von einer Überprüfung, die von der Digitalisierungsbehörde Government Digital Service (GDS) nach eigenem Ermessen durchgeführt wird.

2.3 FedRAMP der US-Regierung

Das Federal Risk and Authorization Management Program (FedRAMP)[9] ist ein Programm der US-Regierung, das einen standardisierten Ansatz für die Sicherheitsbewertung, Autorisierung und kontinuierliche Überwachung von Cloud-Produkten und -Leistungen bietet.

Die Aufgabe des FedRAMP besteht darin, die Einführung sicherer Cloud-Leistungen in der gesamten Regierung durch die Bereitstellung eines standardisierten Ansatzes zur Sicherheits- und Risikobewertung zu fördern.

Anbieter von Cloud-Dienstleistungen können ihre Lösungen durch das FedRAMP einer Zertifizierung unterziehen und werden, nach erfolgreichem Bestehen, in den FedRAMP-Marktplatz aufgenommen und dürfen dann von den unterschiedlichen Bundesbehörden nach festgelegten Richtlinien, verwendet werden. Dafür bieten mehrere grosse Cloud-Provider spezifische Cloud-Lösungen in geschützten Umgebungen in ihren Rechenzentren und teils in exklusiv für die Regierung vorgesehenen Zonen an.

Für klassifizierte Informationen und für militärische Zwecke betreiben die USA eine Reihe von Verwaltungs-Clouds, u. a. will das Verteidigungsministerium mit der Joint

[8] Joint Declaration «Building the next generation cloud for businesses and the public sector in the EU» vom 15. Oktober 2020, vgl. https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe, zuletzt aufgerufen am 27. November 2020.

[9] Vgl. https://www.fedramp.gov/, zuletzt aufgerufen am 27. November 2020.

Enterprise Defense Infrastructure (JEDI) eine gemeinsame genutzte Cloud beschaffen.[10]

2.4 Australien (cloud.gov.au)

Australien hat unter der Federführung der dortigen Digitalisierungsbehörde Digital Transformation Agency (DTA) eine Cloud-Strategie erarbeitet, die vorsieht, dass IKT-Leistungen grundsätzlich Cloud-tauglich konzipiert werden und aus einer Cloud bezogen werden.[11] Für klassifizierte Informationen und um internes Cloud-Knowhow aufzubauen und weiterzuverbreiten, gibt es eine eigene Verwaltungs-Cloud für australische Verwaltungseinheiten.

2.5 Fazit

Cloud-Initiativen wurden in verschiedenen Ländern als Infrastruktur- und Plattform-Vorhaben gestartet und haben sich im Laufe der Zeit zu einem Policy-Framework weiterentwickelt. Dabei ist die Ausgangslage der Länder nicht dieselbe. Der amerikanische Ansatz ist aufgrund der Tatsache, dass mehrere der grossen Public Cloud-Provider amerikanische Firmen unter amerikanischen Recht sind und damit der amerikanische Staat de facto Cloud-Zugriffe kontrollieren kann, nicht direkt auf andere Länder ohne «eigene» Cloud-Provider übertragbar. Wie sich GAIA-X entwickeln wird, wird sich erst noch zeigen. Aktuell ist noch unklar, ob aus der primär deutsch-französischen Initiative ein europaweites Vorhaben wird und ob tatsächlich eine eigene Infrastruktur aufgebaut werden wird oder die Ziele mittels eines Policy-Frameworks erreicht werden.

Zusammenfassend lässt sich feststellen, dass in vielen Ländern eine Kombination der folgenden vier Lösungsansätze zum Einsatz kommt:

1. Bündeln der Cloud-Initiativen unter einem Dach durch eine legitimierte Verwaltungsstelle.
2. Erarbeiten einer gemeinsamen Cloud-Strategie mit einem «Cloud First» Grundsatz
3. Erarbeiten eines Policy-Frameworks für den Bezug von Cloud-Leistungen
4. Bereitstellen einer Verwaltungs-Cloud für besonders schützenswerte Daten

Interessant ist, was im Rahmen dieser nationalen Cloud-Initiativen nicht getan wurde: Es wurden keine nationale Cloud-Infrastrukturen für einen allgemeinen Einsatz aufgebaut. Zudem beschränken sich Befähigungsprogramme auf die Verwaltung selbst bzw. sind integriert in die Bildungspolitik.

3 Kontroversen und «Missverständnisse»

Die Gespräche und Workshops der Studie förderten einige Kontroversen und «Missverständnisse» zu Tage, die bekannt sind aus den Cloud-Diskussionen anderer Län-

[10] Vgl. https://www.cloud.mil/JEDI-Cloud/, zuletzt aufgerufen am 27. November 2020.

[11] Vgl. https://www.dta.gov.au/our-projects/secure-cloud-strategy, zuletzt aufgerufen 27. November 2020.

der.[12] Im weiteren Prozess, insbesondere für den politischen und öffentlichen Dialog, gilt es diese Punkte zu berücksichtigen.

3.1 Abhängigkeit von Cloud-Providern

«Wenn man die Leistungen aus einer Cloud nutze, dann sei man dem Provider auf Gedeih und Verderb ausgeliefert. Mit einseitigen vertraglichen Anpassungen sei zu rechnen und man büsse die Fähigkeit, den Anbieter zu wechseln sowie seine organisatorische Unabhängigkeit ein.»

Grundsätzlich sind die sich aus der Cloud-Nutzung ergebenden Abhängigkeiten vergleichbar mit bekannten Formen von Lieferantenabhängigkeiten, bei denen eine Organisation eine genutzte Leistung nicht mehr ohne Weiteres durch die eine andere Lieferantin substituieren kann. Das liegt meist an der Verwendung proprietärer Technologien, die inkompatibel mit jenen der Mitbewerber sind. Allerdings können auch ineffiziente Prozesse oder vertragliche Beschränkungen dazu führen.

Mit der Cloud-Nutzung geht typischerweise auch eine Verringerung der eigenen Wertschöpfungstiefe bei der Produktion von IKT-Leistungen einher, wodurch die Thematik der Auslagerung von betrieblichen Tätigkeiten (Outsourcing) hinzukommt.

Solche Abhängigkeiten bzw. die daraus entstehenden Risiken sind damit nicht neuartig und spezifisch für die Cloud-Nutzung. Entsprechend kann auf bewährte Ansätze zum Umgang mit Technologien und Lieferantenabhängigkeiten abgestützt werden:

1. Technologie-Management und Lebenszyklus-Management-Fähigkeiten der Organisation weiterentwickeln.
2. Lieferantenabhängigkeiten als Teil des Risikomanagements positionieren und Best Practices zum Umgang mit Lieferantenabhängigkeiten umsetzen.[13]

3.2 «Cloud ist unsicher»

Für die einen ist ihre lokale Infrastruktur sicherer als die Cloud, für die anderen geht das Sicherheitsdispositiv eines Cloud-Providers weit über das hinaus, was man früher selbst zu leisten im Stande war.

Der spezifische in der IKT verwendete Begriff der «Sicherheit» umfasst bekanntermassen die drei Aspekte «Vertraulichkeit», «Integrität» und «Verfügbarkeit», die unterschieden werden sollten. Aus einer Risikomanagement-Perspektive gilt dabei grundsätzlich, dass dieselben Risiken für alle mit dem Internet verbundenen Geräte bestehen, ob diese nun im eigenen Rechenzentrum oder bei einem Cloud-Provider betrieben werden. Diese Risiken können mit gängigen Massnahmen angegangen werden. Es besteht dabei kein Grund anzunehmen, dass Cloud-Provider in diesen Aspekten schlechter abschneiden, da sie über besser gemanagte Systeme mit einer weitergehenden Automatisierung (und daher tendenzielle entsprechend weniger manueller

[12] Vgl. Australien: «Myth: The Cloud is not as secure as on premise services» in der «Secure Cloud Strategy», https://www.dta.gov.au/our-projects/secure-cloud-strategy. Bei GAIA-X wird auch ein «Lobbygerangel» erwartet, siehe https://www.handelsblatt.com/politik/international/cloud-projekt-gaia-x-wird-europaeisch-immer-mehr-staaten-und-firmen-schliessen-sich-altmaiers-cloud-an/26210232.html, beide zuletzt aufgerufen am 27. November 2020.

[13] Vgl. auch den Bericht «Abhängigkeit von Herstellern und Wege zur Risikominderung bei IT-Beschaffungen» vom 9. August 2019» in Erfüllung des Postulates 16.3515 Weibel vom 16. Juni 2016, https://www.isb.admin.ch/dam/isb/de/dokumente/Dokumentation/berichte/Bericht_Postulat_Weibel_16-3515_Abhaengigkeit_Herstellern_Wege_Risikominderung_IT-Beschaffungen.pdf.download.pdf/Bericht_Postulat_Weibel_16-3515_Abhaengigkeit_Herstellern_Wege_Risikominderung_IT-Beschaffungen.pdf, zuletzt aufgerufen am 27. November 2020.

Fehler) verfügen, was unter dem Strich bessere Sicherheitseigenschaften und eine effektivere IT-Kontrolle (im Sinne sogenannter «IT general controls») im Rahmen des internen Kontrollsystems (IKS) ermöglicht.

Hinsichtlich hochverfügbaren Leistungen, die Teil eines Business Continuity Managements sind, gibt es in vielen Szenarien (Ausfälle, Störungen, Manipulation) keine relevanten Unterschiede, da der «end-to-end» Betrieb eines kompletten Service bis zum Anwender meist nicht autonom möglich ist. Ausnahmen bestehen für (landes-) kritische Leistungen von Organisationen, die krisenresistent oder durchhaltefähig sein müssen (siehe auch Abs. 6.7).

Hinsichtlich Vertraulichkeit gehen die Meinungen auseinander. Konsultierte Experten schliessen mit grosser Wahrscheinlichkeit aus, dass Cloud-Provider die Vertraulichkeit im Betrieb oder während der Übertragung verletzen. Vielmehr steht die Frage im Raum, ob andere Staaten aufgrund ihrer nachrichtendienstlichen Fähigkeiten oder aufgrund ihrer (teils geheimen) Gesetze ohne Erlaubnis auf die Daten von Organisationen zugreifen können. Im Zweifelsfall muss diese Frage bejaht werden bzw. ist abhängig von den verfügbaren und eingesetzten technologischen Möglichkeiten, wie starke Verschlüsselung der Daten. Ob sie für eine eigene Infrastruktur anders zu beantworten ist, ist im Einzelfall zu prüfen und entsprechend sind geeignete Ansätze zu entwickeln.

3.3 Positionierung des Datenschutzes

Von einigen für diese Studie konsultierten Experten wurde die Wahrnehmung geäussert, dass der Datenschutz und die damit beauftragten Stellen die Innovation zuweilen behindern. Andere machten eher geltend, der Datenschutz sei auch als Chance für den Standort Schweiz zu positionieren. So oder so drang der Wunsch durch, dass der Datenschutz als «Ermöglicher» in die Projekte integriert werden könne.

Die Materie ist komplex. In der Schweiz sind die Kantone für die Kontrolle der Einhaltung der kantonalen Datenschutzgesetze (für die öffentliche Hand) zuständig; der eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) beaufsichtigt die Bundesstellen und ist für die Unternehmen zuständig. Er nimmt eine nationale Beratungsfunktion wahr. Es gibt somit eine heterogene Rechtslage und das Potential, dass die vielen Verantwortlichen den gesetzlichen Rahmen unterschiedlich auslegen.

Zudem scheint in verschiedenen Organisationen nicht ausreichend geklärt zu sein, wer die datenschutzrechtlichen Konsequenzen von Geschäftsentscheiden zu tragen hat, wer diese dann ad personam trägt und wie mit Restrisiken und Unsicherheiten umzugehen ist.

Daraus ergeben sich für die weitere Bearbeitung von Cloud-Themen in Organisationen die folgenden drei Stossrichtungen:

1. Laufende Auseinandersetzung mit neuen Technologien und gezielte Cloud-Befähigung der Akteure, insbesondere der Personen, die solche Entscheide vorbereiten, treffen oder umsetzen. Dabei empfiehlt es sich, bereits früh in gemischten Teams an solchen Themen zu arbeiten und eine multidisziplinäre Perspektive zu entwickeln.
2. Cloud-Lösungsmuster für den eigenen Bedarf sind zu entwickeln bzw. zu beschaffen.
3. Der Umgang mit neuen Themen und Innovationen ist zu klären und auszuhandeln, insbesondere hinsichtlich der Rollenerwartungen der beteiligten Akteure. Hilfreich ist dabei ein günstiges Framing von solchen Fragestellungen («Was müssten wir tun, um X möglich zu machen»), um neue Lösungswege zu finden.

3.4 Die Rolle des Bundes in der Cloud-Nutzung

Cloud-Provider werben seit mehreren Jahren insbesondere bei besonders regulierten Organisationen wie Banken und der Bundesverwaltung, um sie für ihre Leistungen zu gewinnen. Umgekehrt wünschen sich Vertreter aus der Wirtschaft und kantonalen Verwaltungen, dass die Bundesverwaltung eine Vorreiterrolle übernimmt: Sie solle deutlich auf Cloud-Leistungen setzen und dies auch aktiv kommunizieren.

Abgesehen von nachvollziehbaren wirtschaftlichen Interessen der beteiligten Akteure, wird dabei nicht klar, weshalb die Bundesverwaltung eine Vorreiterrolle in der Cloud-Nutzung einnehmen sollte. Insbesondere muss die der Überlegung zugrundeliegende Annahme, dass wenn die Bundesverwaltung in die Cloud geht, dies auch für andere Organisationen zulässig und zweckmässig sei, als problematisch eingestuft werden. Cloud-Leistungen bergen Risiken, die professionell bewirtschaftet werden müssen. Jedoch sind nicht alle Organisationen ohne weiteres in der Lage, die Risiken angemessen zu erkennen, zu bewerten und die erforderlichen Massnahmen umzusetzen.

Es ist davon auszugehen, dass Organisationen in der Schweiz die Cloud-Nutzung des Bundes verfolgen und das Verhalten der Bundesverwaltung eine Signalwirkung haben kann. In diesem Zusammenhang könnte die Strategische Initiative SI-4 «Hybrid Multi-Cloud», die ein Umsetzungselement der IKT-Strategie des Bundes 2020-2023 ist,[14] unter besonderer Aufmerksamkeit stehen.

3.5 Fazit

Cloud-Mythen sind weit verbreitet und prägen die Wahrnehmung und das Entscheidverhalten. Für den weiteren politischen und öffentlichen Dialog empfiehlt sich deshalb, diese Einschätzungen rasch professionell anhand von legitimierten Interessen und Zielen zu versachlichen, damit der Prozess medial nicht «entgleist». Entsprechend sind die in diesem Kapitel erwähnten Empfehlungen Teil der Handlungsfelder (siehe Kapitel 7).

4 Treiber, Hindernisse und Cloud-Nutzungstrends

Ein wesentlicher Teil der Studie bestand darin, die ausschlaggebenden Gründe für und die Hindernisse der Cloud-Nutzung von Organisationen in der Schweiz in Erfahrung zu bringen. Die Umfrage gab dazu klare Indikationen, die in den Gesprächen und Workshops bestätigt und vertieft werden konnten.

4.1 Treiber

Einfachen Zugang zu neuen Technologien und ein umfassendes Angebots- und Dienstleistungsportfolio sind die beiden wichtigsten Treiber für den Einsatz von Cloud-Leistungen. Ersteres erlaubt es Organisationen, neue Technologien wie beispielsweise IoT, Big Data oder Blockchain einfach zu nutzen und ermöglicht so neue Geschäftsmodelle bzw. Arbeitsweisen. Dies trägt laut den Teilnehmenden zu ihrer Wettbewerbsfähigkeit und Innovationskraft bei.

[14] Vgl. Anhang B: Masterplan zur «IKT-Strategie des Bundes 2020-2023 – Ausgabe 2020», https://www.newsd.admin.ch/newsd/message/attachments/60845.pdf, zuletzt aufgerufen am 27. November 2020.

Das umfassende Angebots- und Dienstleistungsportfolio von Cloud-Providern erlaubt den Organisationen oft eine viel schnellere und zielgerichtetere Bereitstellung von Services, als sie selbst dazu in der Lage wären. Ein Bild, das sich auch in den wichtigsten Cloud-Fähigkeiten zeigt (siehe Abbildung 6).

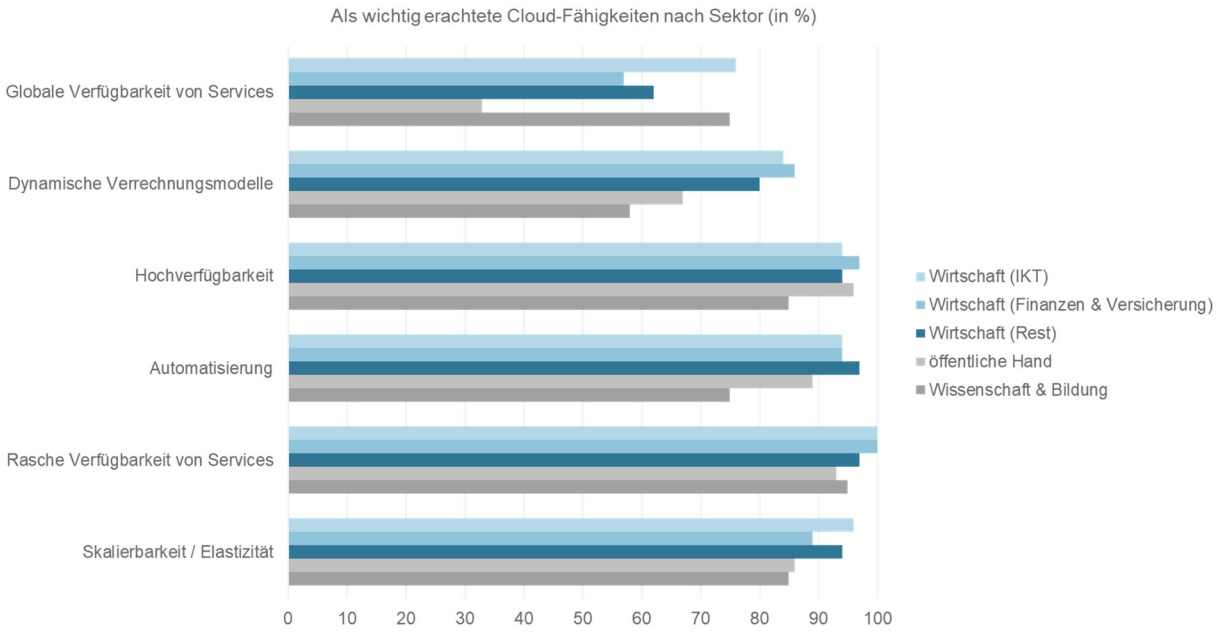

Abbildung 6: Als wichtig erachtete Cloud-Fähigkeiten nach Sektor

Wie erwartet wird die globale Verfügbarkeit der Cloud-Leistungen von der öffentlichen Hand als weniger wichtig beurteilt; ansonsten gibt es keine relevanten sektorspezifischen Unterschiede.

4.2 Hindernisse

Die Mehrheit der Organisationen beurteilt die aus der Cloud-Nutzung entstehenden Abhängigkeiten als einen kritischen Hinderungsgrund (siehe auch Abs. 3.1). Nicht behindernd seien die Betriebskosten oder die Leistungsversprechen der Cloud-Provider. Spezifisch bei der öffentlichen Hand gibt es Hinderungsgründe, die andere Sektoren nicht in vergleichbarem Ausmass betreffen, nämlich das Datenabfluss-Risiko, nichtakzeptable Vertragsbedingungen und fehlendes Knowhow (siehe Abbildung 7). Im Gespräch erwähnen auch Vertreter anderer Sektoren diese Herausforderungen als behindernd, gewichten sie aber, bis auf das Knowhow, verhältnismässig tiefer.

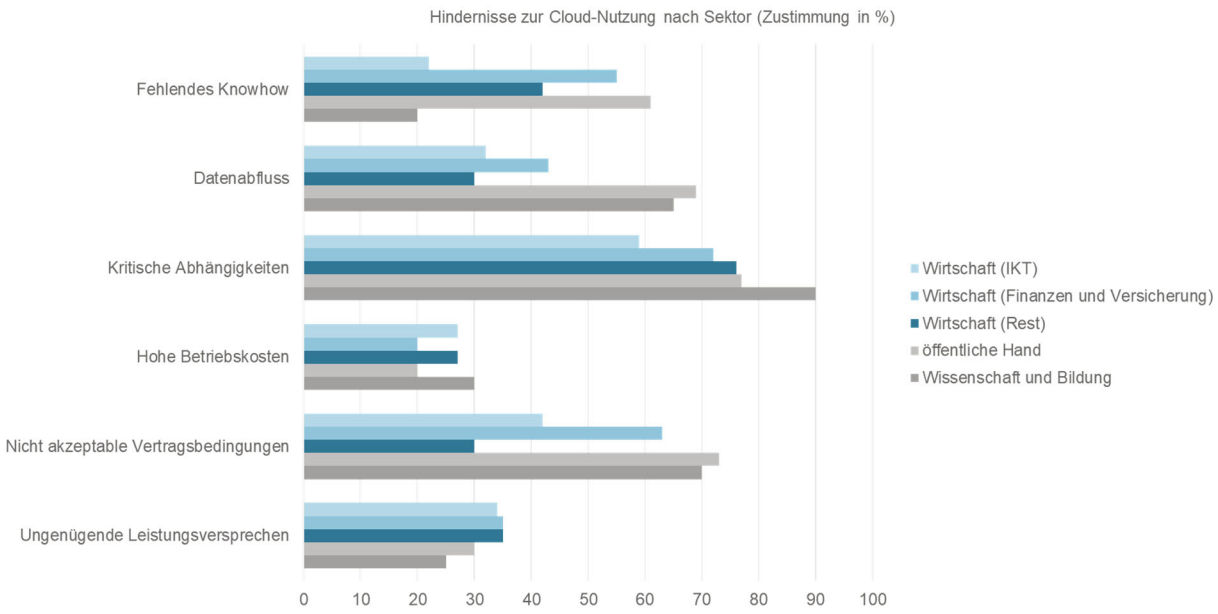

Abbildung 7: Hindernisse zur Cloud- Nutzung nach Sektor

Die Interviews und Workshops förderten zudem weitere Themen zu Tage, welche die Organisationen in ihrer Cloud-Nutzung einschränken:

- Rechtliche Grundlagen für eine Nutzung von Cloud-Leistungen werden als unklar wahrgenommen.
- Viele unterschiedliche Stellen innerhalb der Organisation sind einzubeziehen (zusätzlicher Aufwand, Prozesse und Personen zu organisieren).
- Spezifisch fehle das Zusammenspiel der IT und der Rechtsabteilung.
- Der Datenschutz und die damit beauftragten Stellen behindern bisweilen die Innovation (siehe auch Abs. 3.3).
- Die eigene Organisation wird als träge wahrgenommen.
- Der Beschaffungsweg für solche Leistungen ist nicht definiert (was in kleineren Fällen teils in Käufen mit Geschäftskreditkarte mündet).
- Die eigene IT-Organisation reagiert mit Angst vor Kompetenzverlust.

Diese Liste ist nicht abschliessend, lässt aber zusammen mit den Themen aus der Umfrage erkennen, dass die Hindernisse vermutlich zwei Bereichen geschuldet sind:

- Ungenügende Rahmenbedingungen und Wissen in der Organisation, um Cloud-Leistungen nutzen zu können.
- Mangelnde Klarheit, Cloud-Leistungen sicher und juristisch angemessen einzusetzen.

4.3 Aktuelle Nutzung und künftiger Bedarf

Die Wirtschaft, insbesondere der IKT-Sektor selbst, nutzen aktuell am meisten Cloud-Leistungen (siehe Abbildung 8). Während in anderen Branchen die Cloud-Durchdringung heute noch nicht durchgängig ist, zeichnet sich ab, dass alle Sektoren mehr Cloud-Leistungen nutzen wollen (siehe Abbildung 9). Beeindruckend ist dabei, dass der Trend nach mehr Leistungsbezug aus der Cloud grundsätzlich für alle Anwendungsfälle gilt. Damit scheint sich ein «Cloud First» Paradigmenwechsel abzuzeichnen, IKT-Leistungen nur noch dann lokal zu erbringen, wenn es spezifische Gründe dafür gibt – was entsprechend hybride Cloud-Ansätze zur Folge hat.

In den Gesprächen wurde punktuell auch der Bedarf eines schweizweiten Daten Hubs[15] eingebracht, der eine Datenwirtschaft mit klarer Daten-Governance ermöglichen würde. Zudem wurde auch ein Bedarf an sicherer lokaler Infrastruktur für Daten Recovery genannt.

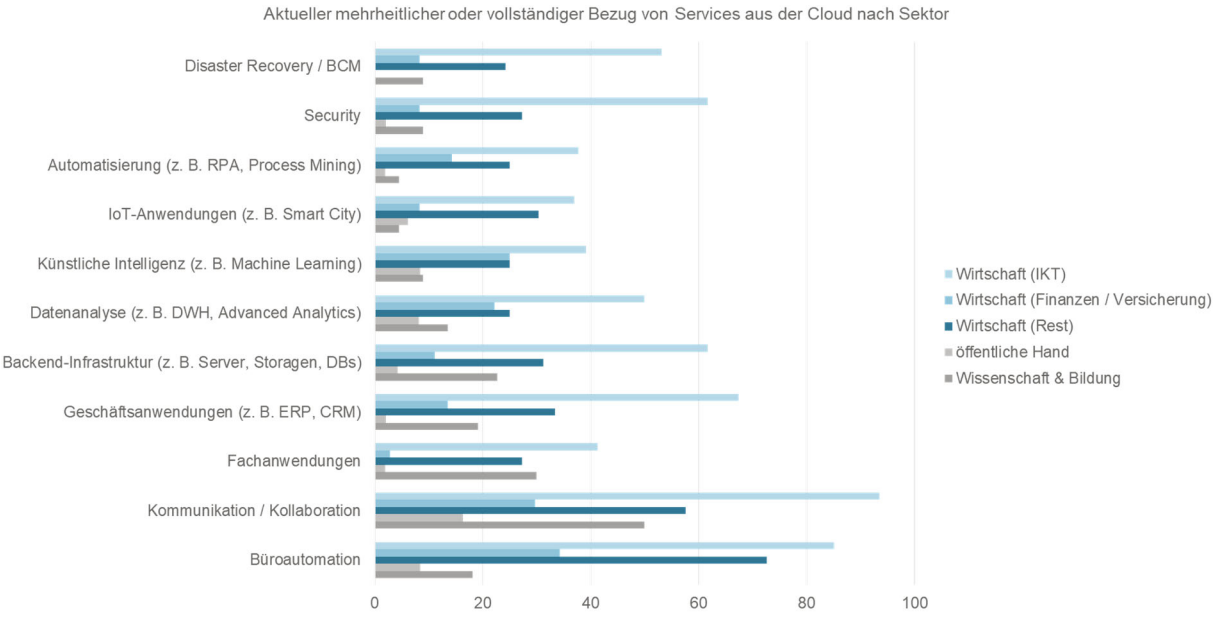

Abbildung 8: Aktueller Bezug von Services aus der Cloud nach Sektor

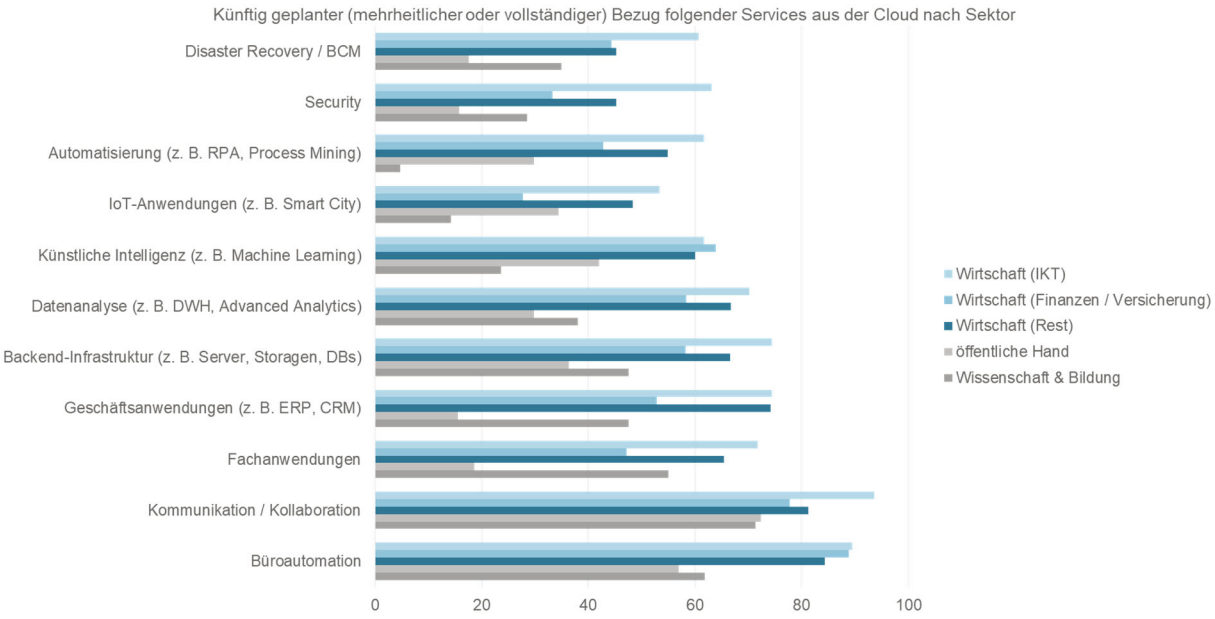

Abbildung 9: Künftiger Bezug von Services aus der Cloud nach Sektor

[15] Vgl. dazu auch Mo. 204260: «Zukunftsfähige Daten-Infrastruktur und Daten-Governance in der Bundesverwaltung», https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20204260, zuletzt aufgerufen am 27. November 2020.

4.4 Fazit

Trotz teilweiser Rechtsunsicherheit sowie in gewissen Bereichen fehlender Expertise und Erfahrung besteht eine grundsätzliche Einigkeit, künftig mehr Cloud-Leistungen zu nutzen. Der naheliegende Schluss ist, dass die Vorteile – insbesondere der einfache Zugang zu neuen Technologien und ein umfassendes Angebots- und Dienstleistungsportfolio – die Nachteile in der heutigen Bewertung überwiegen. Die Diskussionen fördern eine differenzierte Sicht zu Tage, die sich am Informationsschutz- und Autonomie-Bedarf orientiert und risikobasierte Lösungsansätze offenbart (z. B. hybride Cloud-Architektur).

5 Warum eine «Swiss Cloud»?

Warum braucht es eine Swiss Cloud? Im Rahmen der Studie ergaben sich hierzu zwei Narrative:

1. als Standortfaktor für den Wirtschaftsstandort Schweiz;
2. als Schutzmassnahme im Zusammenhang nachrichtendienstlicher Ermittlungen.

Als Standortfaktor wurde die Swiss Cloud mit einer nationalen Infrastruktur wie der NEAT verglichen. Das Land, das über keine relevanten Bodenschätze verfügt, könnte eine moderne, sichere Cloud-Infrastruktur als Alleinstellungsmerkmal im internationalen Standortwettbewerb anbieten.

Die Umfrageresultate lassen mit einer Zustimmung von 41% für eine schweizerisch betriebene Cloud bzw. 24% für eine durch den Bund betriebene Cloud jedoch keinen generellen Bedarf an einer Swiss Cloud erkennen (siehe Abbildung 10). Vom Bund gefordert wird vielmehr von über 80% der konsultierten Experten, dass er bessere rechtliche Rahmenbedingungen sowie die Rechtssicherheit erhöht. Im Gespräch war es den Experten dabei gleichermassen wichtig zu betonen, dass diese Einschätzung nicht als Ruf nach mehr Regulierung verstanden werden soll.

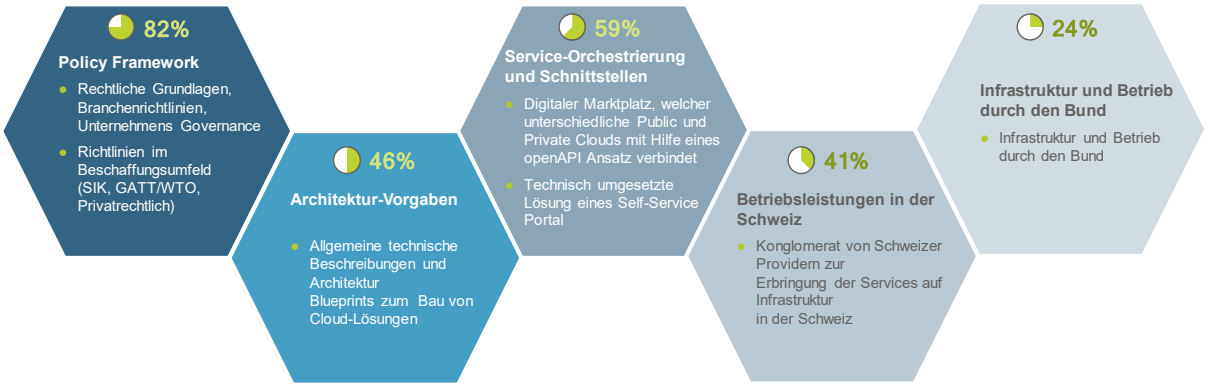

Abbildung 10: Staatliche Aufgabe gemäss Umfrage

Dabei ist der Bedarf an nationaler Infrastruktur je Sektor verschieden. Für die öffentliche Hand, durchhaltefähige Organisationen und Betreiber von kritischen Infrastrukturen (vgl. Abs. 6.7) ist der Bedarf einer eigenen Infrastruktur gegeben. Diese für den Eigengebrauch bestimmte Infrastruktur spielt dann aber nicht eine Rolle als Standortfaktor.

Als Schutzmassnahme verstanden knüpft das zweite Narrativ an den öffentlichen Meinungs- und Bewusstseinswandel nach den Snowden-Enthüllungen an: Als staatlicher

oder nichtstaatlicher Wirtschaftsakteur muss davon ausgegangen werden, dass Informationen auch beschafft werden, wenn sie genügend wertvoll sind – seien es z. B. Verhandlungsstrategien, Rüstungsinformationen oder intellektuelles Eigentum in der Hochtechnologie und im Forschungsbereich. Dieser Betrachtung folgend, stellt sich die Frage, welche Massnahmen geeignet sind, um das Risiko des (unerwünschten) Datenabflusses zu reduzieren.

Die Umfrage-Teilnehmenden sehen dabei die Absenz einer Datenherausgabepflicht an Dritte und die Unterstellung unter Schweizer Recht als die beiden am höchsten gewichteten Anforderungen (siehe Abbildung 11).

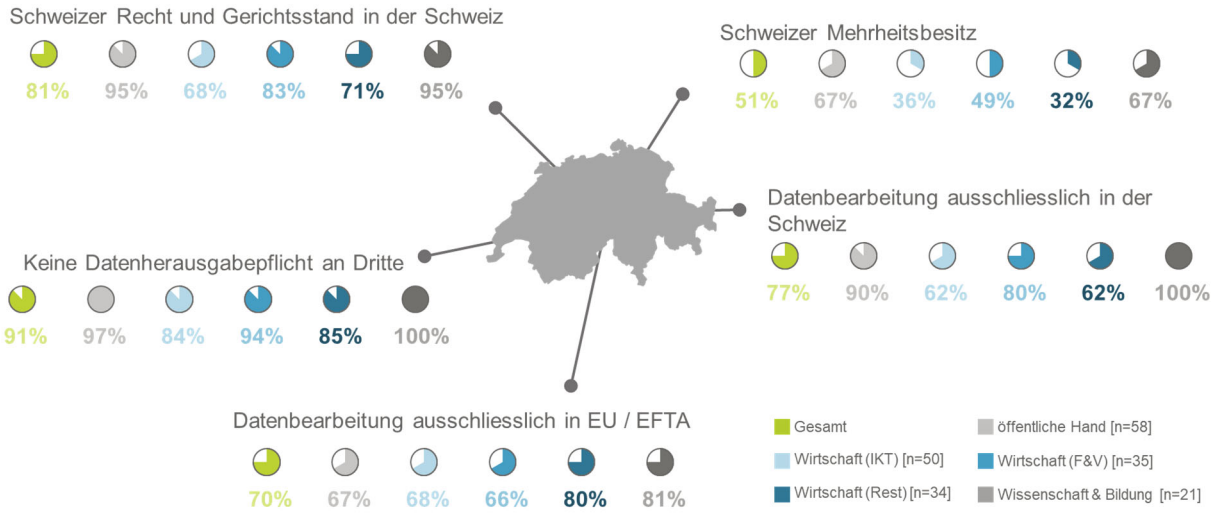

Abbildung 11: Relevante Souveränitätskriterien

Informiert durch Schutzüberlegungen der Bundesverwaltung (als Teil des sogenannten P041 - RINA-Prozesses[16]) fordern Experten bei gegebenem Schutzbedarf die folgenden Eigenschaften, die über die ganze Lebensdauer erfüllt sein müssen:

1. Die Trägerschaft ist in Schweizer Mehrheitsbesitz und ist wirtschaftlich nicht abhängig von anderen Ländern, in denen sie geschäftlich tätig ist.
2. Die Datenbearbeitung erfolgt ausschliesslich in der Schweiz.
3. Es besteht keine Datenherausgabepflicht an Dritte ausser derjenigen der Schweizer Justiz mit Rechtsschutz.
4. Die Organisation untersteht Schweizer Recht mit Gerichtsstand in der Schweiz

Nutzer solcher Leistungen sind primär staatliche Stellen mit streng vertraulicher Information[17], daneben wurden in Rahmen der Studie zwei weitere Bedarfsträger identifiziert: 1. Internationale Organisationen wie das IKRK oder die UN (siehe auch Abs. 6.8) sowie Wirtschaftsakteure, die über besonders wertvolles intellektuelles Eigentum verfügen.

Für diese Nutzer kommen – im heutigen rechtlichen Rahmen und nach Einschätzung der konsultierten Experten – internationale Anbieter nicht in Frage und zwar selbst

[16] Die Unterlagen sind nicht öffentlich zugänglich; siehe intranet.isb.admin.ch → IKT-Vorgaben → Prozesse und Methoden → P041 - Schutzbedarfsanalyse (Schuban) → P041 - Hi02: Anleitung zum Prüfprozess RINA (Risikomanagementmethode zur Reduktion nachrichtendienstlicher Ausspähung)

[17] D. h. Informationen, die als VERTRAULICH oder GEHEIM im Sinne der Informationsschutzverordnung ISchV, SR 510.411, gelten.

dann nicht, wenn diese ihre Leistungen in der Schweiz auf eigener Infrastruktur erbringen würden. Entsprechend bräuchte es einen schweizerischen Provider für solche Leistungen.

6 Identifizierte Bedarfsträger

Nachfolgend werden die Bedarfe der identifizierten Bedarfsträger beschrieben, die folgende Eigenschaften erfüllen: i) ein spezifischer Bedarf liegt vor, der mit ausgewählten Vertretern der Stakeholder-Gruppen vertieft und validiert (siehe auch Abs. 1.4 dazu) werden konnte und ii) die Träger verfügen über eine volkswirtschaftlich relevante aggregierte Wirtschaftskraft. Die Ergebnisse sind in Tabelle 1 zusammengefasst. Potenzielle Bedarfsträger, die nicht an der Studie teilgenommen haben, sind nicht erfasst und können blinde Flecken für den tatsächlichen Bedarf darstellen (vgl. dazu Abs. 1.4).

Bedarfsträger / *Bedarf*	IT und Telekommunikation	Finanzindustrie und Versicherungen	Weitere Bedarfsgruppen der Wirtschaft	Öffentliche Hand (ohne Spezialbedarfe)	Bildung, Gesundheitswesen, Blaulicht-Organisationen	Forschung	Krisenresistente und durchhaltefähige Organisationen	Internationale Organisationen
Baustein 1: Policy Framework								
Baustein 2: Architektur-Vorgaben								
Baustein 3: Service-Orchestrierung und Schnittstellen								
Baustein 4: Betriebsleistungen in der Schweiz								
Baustein 5: Infrastruktur und Betrieb durch den Bund								
Förderung, Befähigung, Beratung								
Souveräne Cloud-Angebote mit besonderen Garantien								
Schutz besonders schützenswerter Daten								
Zugang zu Innovation								

Tabelle 1: Zusammenfassung des Bedarfs (grün = gefordert; orange = nicht erwünscht; grau = nicht gefordert)

6.1 IT und Telekommunikation

Die Bedarfsgruppe «IT- und Telekommunikation» hat an der Studie ein grosses Interesse und viel Präsenz gezeigt. Ihre Rolle als Anbieterin und Konsumentin lässt sich nur bedingt unterscheiden. Entsprechend sind die Umfrageresultate für diese Gruppe aufgrund der Interessenslagen mit Sorgfalt zu interpretieren.

Der Sektor verfolgt seit je den Ansatz, die Wertschöpfungstiefe aktiv zu gestalten und alles, was zum Gebrauchsgut («commodity») wird, einzukaufen. Wenig überraschend nutzt der Sektor bereits viele Cloud-Leistungen, verfügt über eine vergleichsweise

hohe Maturität und sieht in der Cloud viele Treiber. Hindernisse werden vor allem in der Abhängigkeit und den Vertragsbedingungen erkannt.

Der gemeinsame Tenor in der Branche ist, dass weder Baustein 4 – eine Schweizer Infrastruktur noch Baustein 5 – eine Bundes-Cloud-Infrastruktur als zielführend beurteilt wird, da das Angebot an Cloud-Lösungen in der Schweiz in der jetzigen Form ausreichend sei. Vielmehr bestünde ein Bedarf an Befähigung, insbesondere von Unternehmen sowie kleineren IT-Unternehmen, welche KMUs und Microunternehmen in ihrer (geografischen) Nähe beraten und unterstützen. Diese Forderung geht weiter als nur Beratung in spezifischen Themen wie Cybersicherheit, sondern umfasst generelle Befähigungen im Sinne von Sensibilisierung, Förderung von branchen- und themenspezifischen Musterlösungen sowie Aus- und Weiterbildungsangeboten.

Insbesondere Provider sehen in weiterer staatlicher Regulierung potenzielle Hindernisse. Erstens würde ein strikter Datenschutz Innovation und «time-to-market» bremsen. Zweitens könnten Gesetze nur selten technologieneutral formuliert werden, wodurch laufende Gesetzesänderungen erforderlich würden, die nicht mit den Entwicklungen Stand halten könnten.

6.2 Finanz- und Versicherungsindustrie

Die Finanz- und Versicherungsindustrie hat in den letzten Jahren viel investiert, um die Vorteile von Cloud-Leistungen zu nutzen, und ist nun daran, die Nutzung weiterauszubauen. Es besteht ein grosser und umfassender Bedarf an Cloud-Leistungen.

Die Finanz- und Versicherungsindustrie untersteht besonderen Regulierungen, welche die Identifizierung und Begrenzung gewisser Risiken in Zusammenhang mit Cloud-Lösungen zum Gegenstand haben (zum Beispiel Outsourcing, Cybersicherheit, Kundendaten, BCM). Banken haben zudem bei der gewählten Kundendatenhaltung den möglichen strafrechtlichen Konsequenzen einer Verletzung von Art. 47 BankG (Bankkundengeheimnis) Rechnung zu tragen. In der aktuellen Ausgangslage ist aus Sicht dieses Sektors noch zu wenig klar geregelt, unter welchen Voraussetzungen eine Cloud-Lösung verwendet werden darf und wann eine Verletzung vorliegt.

Die Schweizerische Bankiervereinigung (SBVg) hat eigene Rechtsgutachten beauftragt und einen Cloud-Leitfaden erarbeiten lassen, der die wesentlichen Themen adressiert.[18] Offen sind dabei insbesondere Datenherausgabepflichten der Cloud-Provider an Dritte, wo insbesondere die amerikanischen Regelungen noch nicht abschliessend beurteilt werden können und eine staatliche Klärung erwünscht ist.

Die Zugehörigkeit eines Finanzinstituts zu einer international tätigen Finanzgruppe bzw. oder zu einem Finanzkonzern hat einen Einfluss auf seine Cloud-Strategie. Inlandorientierte Institute richten sich eher nach den aktuell in der Schweiz vorhandenen Cloud-Lösungen. Grössere und international tätige Finanzinstitute haben komplexere Cloud-Strategien, die teilweise im Mutterhaus entwickelt werden und zusätzliche ausländische regulatorische Vorgaben berücksichtigen müssen. Diese Feststellung unterstreicht die Forderung nach den Bausteinen 1 und 2 – Policy Framework sowie klaren Richtlinien und Grundlagen zur Befähigung (z. B. Lösungsmuster für die Verschlüsselung). Bei den anderen Bausteinen besteht kein Bedarf, insbesondere nicht nach einer Schweizer Infrastruktur im Sinne der Bausteine 4 oder 5.

[18] Vgl. https://www.swissbanking.org/library/richtlinien/cloud-leitfaden-wegweiser-fuer-sicheres-cloud-banking/cloud-leitfaden_de.pdf, zuletzt aufgerufen am 27. November 2020.

6.3 Weitere Bedarfsgruppen der Wirtschaft

Gemeinsam bei allen Wirtschaftssektoren ist der Bedarf an Cloud-Leistungen in unterschiedlichen Formen und unterschiedlicher Ausprägung. Gewisse Sektoren fokussieren sich dabei mehr auf die Nutzung ergänzender IKT-Leistungen aus der Cloud, andere die Nutzung von Cloud-Leistungen für den Betrieb von Kernsystemen.

Viele grössere Unternehmen nutzen Cloud-Fähigkeiten und gewichten diese sehr hoch in Hinblick auf Innovationskraft und time-to-market. Als weniger wichtig werden Skalierbarkeit und der Bedarf an einer Swiss Cloud bewertet. Ein Wechsel auf eine andere Cloud wäre für sie mit hohen Migrationskosten und wenig Nutzen verbunden.

Jedoch sehen sich viele Wirtschaftssektoren mit unsicheren rechtlichen und regulatorischen Rahmenbedingungen konfrontiert, welche durch rechtliche Regelungen geschaffen wurden (z. B. CLOUD Act, Privacy Shield). Um diese Konflikte zu beheben bzw. das Risiko besser einschätzen zu können, entstand der Wunsch nach einem Risiko-Framework oder eines Leitfadens, welcher vom Bund veröffentlicht und gutgeheissen wird.

Entsprechend stimmen die Wirtschaftssektoren in diesem Sinne grundsätzlich Baustein 1 (Policy Framework) und 2 (als Befähigung verstanden) zu. Damit wollen sie die gemeinsamen Bedürfnisse (Rechtsklarheit, Straftatbestände, Risiken verbunden mit kritischen Abhängigkeiten und Datenabfluss, Risiko-Framework usw.) adressieren und Standards zur Orientierung setzen. Dafür könnte den Wirtschaftsvertretern zufolge z. B. «Swiss Cloud» als Label oder Gütesiegel für sichere und geprüfte Cloud-Leistungen positioniert werden. Dies soll vor allem auch KMUs und Mikrounternehmen befähigen und ihnen Vertrauen in Cloud-Dienste geben.

6.4 Öffentliche Hand (ohne Spezialbedarfe)

Die öffentliche Hand hat im Vergleich mit den anderen Sektoren den aktuell geringsten Service-Bezug aus der Public Cloud (vgl. Abs. 4.3). Die rechtlich geprüften und erfolgreichen Cloud-Nutzungen einzelner Verwaltungsstellen, exemplarisch sei hier Geoportal der Swisstopo erwähnt,[19] sind verhältnismässig wenig bekannt bzw. sind noch nicht in den gemeinsamen Erfahrungsschatz der öffentlichen Hand übernommen worden.

Ihre Treiber für einen Gang in die Public Cloud sind die Hochverfügbarkeit, Skalierbarkeit, Automation sowie die rasche Verfügbarkeit der benötigten Services. Einzig die globale Verfügbarkeit der Daten ist weniger relevant.

Herausforderungen in der Cloud-Nutzung liegen einerseits in dem Erfordernis, dass staatliches Handeln formalrechtlich legitimiert sein muss. Eine weitere Herausforderung liegt in der Art der Daten begründet, die die jeweiligen Organisationen bearbeiten, da klassifizierte Informationen anfallen, die besonders strikten Vorschriften der Bearbeitung, Speicherung und Weitergabe unterliegen.[20] Entsprechend wurden aus diesem Sektor die grössten Bedenken im Bereich Datenschutz und Datensicherheit genannt.

---

[19] Siehe http://map.geo.admin.ch, zuletzt aufgerufen am 27. November 2020.

[20] Siehe hierzu für die Bundesverwaltung insbesondere die Informationsschutzverordnung ISchV, SR 510.411, sowie die Weisungen des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung WIsB vom 16. Januar 2019.

Ein Gang in die Cloud wird durch ein Fehlen von klaren rechtlichen Aussagen, welche Clouds für welche Daten genutzt werden dürfen, gehemmt. Die Gefahr einer Amtsgeheimnisverletzung (Art. 320 Abs. 1 StGB) führt gemäss Aussagen dazu, dass die Public Cloud unter Umständen nicht als mögliche Option in Betracht gezogen wird.

Fehlendes Knowhow, die Gefahr eines Datenabflusses und nicht akzeptable Vertragsbedingungen wurden überdies als stärker behindernd eingeschätzt, als dies bei den anderen Sektoren der Fall ist.

Im Hinblick auf die genannten Bedenken wird darum in der Umsetzung von Baustein 1 – Policy Framework klar am meisten Nutzen gesehen. Interessant ist zudem, dass das Baustein 5 – als Verwaltungs-Cloud verstanden – von der Verwaltung, zusammen mit dem Sektor Wissenschaft und Bildung, ebenfalls einen vergleichsweisen hohen Zuspruch erhält.

Zusammenfassend lässt sich feststellen, dass für die Verwaltung vor allem die rechtlichen Rahmenbedingungen geklärt werden müssen. Die diesbezügliche Unklarheit hemmt, neben dem fehlenden Knowhow, eine effiziente Nutzung von Public Services. Eine Art Wegleitung für die Nutzung von Public Cloud Services wird ebenfalls als hilfreich erachtet.

6.5 Bildung, Gesundheitswesen, Blaulicht-Organisationen

Die Sektorgruppen Bildung, Gesundheitswesen und Blaulicht-Organisationen sehen sich auf einer hohen Abstraktionsebene mit vergleichbaren Hindernissen, und dementsprechend auch mit ähnlichem Bedarf an einer Swiss Cloud, konfrontiert. Heute ist die Cloud-Nutzung noch eher gering ausgeprägt.

Das liegt nicht zuletzt daran, dass oftmals besonders schützenswerte (Personen-) Daten vorliegen. Im Gesundheitswesen sind dies etwa Patienten- und Gesundheitsdaten, in der Bildung Personendaten von Minderjährigen, bei Blaulicht-Organisationen Personendaten von potenziellen Verurteilten oder Opfern. Zudem führt die föderale Aufgabenteilung zu einer Fragmentierung mit einem tiefen Standardisierungsgrad. Aufgrund dieser Situation sehen sich viele der befragten Organisationen mit unklaren Rahmenbedingungen konfrontiert und fordern die Erarbeitung von klaren Lösungsmustern, wie mit diesen Daten in Bezug auf Cloud-Lösungen umgegangen werden soll.

Diese Tatsache wird durch das Umfrageresultat unterstützt, dass alle Vertreter aus Wissenschaft und Bildung die Rahmenbedingung «keine Datenherausgabepflicht an Dritte» als wichtigen Aspekt einer Swiss Cloud betrachten. Zusätzlich wird auch von allen Vertretern eine «Datenbearbeitung ausschliesslich in der Schweiz» gefordert (siehe Kapitel 5) und «rechtliche Sicherheit» ist mit Abstand der am stärksten gewichtete Vorteil einer Swiss Cloud. Diese klaren Trends zeigen den dringenden Bedarf nach klarer Rechtslage bzw. nach Befähigung für den Umgang mit besonders schützenswerten Daten auf. Es hat sich aus den Gesprächen und der Umfrage herauskristallisiert, dass die Schaffung dieser Rahmenbedingungen als Aufgabe des Bundes gesehen wird.

Entsprechend werden die Bausteine 1 und 2 – Policy Framework und Beratung bevorzugt. Vereinzelte Vertreter mehrere Organisationen fordern zudem Befähigung und Beratung im Bereich der Cybersicherheit. Hier sehen die Vertreter eine grosse Lücke bei dem vorhandenen Knowhow und es wird grosser Wert auf Unterstützung gelegt.

Zudem kam vor allem aus dem Umfeld der Bildungseinrichtungen, vereinzelt auch von den Blaulicht-Organisationen, der Wunsch nach einer Swiss Cloud im Sinne eines

Standard-Angebots an Sektorlösungen (Software-as-a-Service), welche auf Schweizer Bedürfnisse und Recht zugeschnitten sind, was einem Marktplatz (Baustein 3) entsprechen würde. Dafür bräuchte es aber auf Governance-Ebene erst entsprechende Vorkehrungen, um den Rechtsrahmen, den Bedarf und die Steuerung zu vereinheitlichen.

6.6 Forschung

Im Bereich Forschung liegen kaum spezifisch abweichende Einschätzungen vor. Bezüglich des generellen Einsatzes von Cloud-Leistungen werden das umfassend verfügbare Dienstleistungsangebot sowie der damit verbundene einfache Zugang zu neuen Technologien und zu Innovation sehr geschätzt. Als wichtigste Cloud-Fähigkeiten werden die Skalierbarkeit verbunden mit einer raschen Service-Verfügbarkeit (time-to-market) genannt, gefolgt von deren Hochverfügbarkeit und deren Verfügbarkeit auf globaler Basis.

Die schweizerischen Hochschulen haben eigene Infrastrukturen im Bereich High-performance Computing bzw. Supercomputing aufgebaut.[21] Der Forschungsbereich rechnet für die kommenden Jahre mit einem signifikanten Wachstum der Cloud-Nutzungen, insbesondere für Dienstleistungen im Bereich SaaS (Software-as-a-Service). Bereits in die Wege geleitet wurde die Erarbeitung der strategischen Grundlagen für Open Research Data durch swissuniversitites, beauftragt durch das SBFI.[22]

Für den Forschungsbereich stehen drei Aspekte im Vordergrund: zunächst, dass die Datenbearbeitung in der Schweiz erfolgt; weiter, dass Dritten gegenüber keine Datenherausgabepflicht bestehen dürfe sowie drittens, dass Schweizer Recht und Gerichtsstand massgeblich seien. Vorteile einer Swiss Cloud werden v.a. im Datenschutz und in der Rechtssicherheit gesehen.

Entsprechend verlangt der Forschungsbereich nach einem starken Policy Framework im Sinne des Bausteins 1.

6.7 Krisenresistente und durchhaltefähige Organisationen

Betreiber kritischer Infrastrukturen, insbesondere Energieversorger[23], Organisationen, die auch in einer Krise funktionieren müssen (z. B. staatliche und staatsnahe IKT-Dienstleister, Blaulicht-Organisationen) und die Armee als durchhaltefähige Organisation, nutzen heute noch wenig Cloud-Leistungen. Aufgrund der voranschreitenden Digitalisierung dieser Organisation und da ihre IT für das Funktionieren der Organisation eine kritische Infrastruktur darstellt, besteht für solche Organisationen ein Spezialbedarf an sicheren Infrastrukturen mit Cloud-ähnlichen Eigenschaften.

6.8 Internationale Organisationen

Internationale Organisationen, namentlich das IKRK oder die UN, nutzen heute noch wenig Cloud-Leistungen, haben aber aufgrund ihres Operationsradius einen Bedarf an

[21] Exemplarisch sei hier das Centro Svizzero di Calcolo Scientifico CSCS (https://www.cscs.ch/) erwähnt.

[22] Vgl. https://www.swissuniversities.ch/themen/digitalisierung/open-science, zuletzt aufgerufen am 27. November 2020.

[23] Vgl. SKI-Strategie des BABS, https://www.babs.admin.ch/de/aufgabenbabs/ski/kritisch.html, zuletzt aufgerufen am 27. November 2020.

weltweit verfügbaren Leistungen mit Cloud-Eigenschaften. Marktgängige Cloud-Angebote sind für diese Organisationen aus den folgenden Gründen keine Option:

1. Ein Teil der bearbeiteten Daten ist delikat und besonders schützenswert.
2. Gewisse Personen, die die Angebote nutzen, geniessen aufgrund ihres völkerrechtlichen Status' Immunität.
3. Die Angebote müssen auch in Ländern verfügbar sein, die unter einem Embargo stehen.

Entsprechend besteht der Wunsch nach einem Angebot, bei dem garantiert wird, dass keine Datenherausgabepflichten an Dritte bestehen, und dass das Völkerrecht eingehalten wird, z. B. hinsichtlich Immunität. Organisationen wie das IKRK würden ein Schweizer Angebot im Sinne des Bausteins 4 oder 5 aufgrund der stabilen Schweizer Verhältnisse und der Neutralität begrüssen. Ein internationales Angebot mit entsprechenden Garantien würde die Anforderungen vermutlich auch erfüllen.

7 Schlussfolgerungen und Handlungsfelder

7.1 Schlussfolgerungen

Die Studie gelangt zu folgenden Aussagen:

- Die Nutzung von Cloud-Leistungen ist ein gemeinsames Bedürfnis der befragten Organisationen in der Schweiz. Dabei zeichnet sich ein klarer Paradigmenwechsel hin zu «Cloud First» Strategien ab, wonach IKT-Leistungen nur bei Vorliegen spezifischer Gründe auf Basis eigener Infrastrukturen erbracht werden.
- Für den Einsatz von Cloud-Leistungen bedarf es geklärter und ggf. angepasster rechtlicher und regulatorischen Rahmenbedingungen.
- Sorge bereitet den Befragten insbesondere das Risiko von nicht autorisierten Datenzugriffen, z. B. im Zusammenhang von nachrichtendienstlichen Ermittlungen. Die Annahme, dass eigene IT-Infrastrukturen grundsätzlich sicherer seien, ist allerdings trügerisch. Vielmehr ist die Anwendung angemessener Schutzkonzepte erforderlich.
- Viele Organisation fordern Orientierungshilfen im Umgang mit Cloud-Technologien. Mögliche Mittel können z. B. im Bereitstellen von Best Practices, Normen zur Zertifizierung sowie standardisierten Service-Güteklassen bestehen oder darin, Hilfestellungen zu erhalten, um die Risiken realistisch abschätzen zu können.
- Lediglich eine Minderheit der Befragten sieht Bedarf an einer schweizerischen oder durch den Bund kontrollierten Cloud-Infrastruktur, nämlich insbesondere für krisenresistente Infrastrukturen und im Bereich gemeinsamer Lösungen der öffentlichen Hand.
- Die Mehrheit der Bedarfsträger bevorzugt kommerzielle Cloud-Leistungen, soweit den oben genannten Punkten geeignet Rechnung getragen wird.

Dies legt folgende Schlussfolgerungen nahe:

- Der Bedarf an einer «Swiss Cloud» in Gestalt einer öffentlich-rechtlichen Infrastruktur und als Erfolgsfaktor für den Standort Schweiz ist nicht ausgewiesen.
- Hingegen wird eine «Swiss Cloud» als Label in Form geeigneter Rahmenbedingungen und Leitlinien für eine kompetente und sichere Nutzung von Cloud-Leistungen stark gefordert.

Entsprechend ergeben sich daraus die folgenden fünf Handlungsfelder:

1. Zertifizierungssystem für Cloud-Leistungen prüfen und konkretisieren;
2. Rechtliche und regulatorische Fragestellungen zur Cloud-Nutzung klären und beantworten;
3. Die internationale Vernetzung und den Einbezug der Schweiz in europäischen Initiativen wie GAIA-X prüfen;
4. Im Rahmen des Aufbaus der Digitalen Verwaltung Schweiz (DVS) die institutionellen Grundlagen der Schweizer Verwaltung zur Nutzung von gemeinsamen Cloud-Leistungen entwickeln;
5. Die (völker-) rechtlichen Rahmenbedingungen für die Gewährleistung der Immunität von Daten in Public Clouds für internationale Organisationen prüfen.

Weitere Massnahmen für einzelne Bedarfsträger sind:

- Dialog mit den Branchen zur Entwicklung von Hilfsinstrumenten zur chancen- und risikobewussten Nutzung von Cloud Diensten führen;
- Bedarf und Weiterentwicklung von krisenresistenten Leistungen für Betreiber kritischer Infrastrukturen klären und konkretisieren.

Diese Handlungsfelder und Massnahmen erfüllen den in den Gesprächen und Workshops mit den Experten identifizierten und validierten Bedarf.

7.2 Handlungsfeld 1: Zertifizierungssystem

Zertifizierungssystem für Cloud-Leistungen prüfen und konkretisieren

Ausgangslage

- Datensicherheit spielt bei der Nutzung von Cloud Leistungen eine wichtige Rolle; Nutzer sollen auf diesbezüglich vertrauenswürde Dienstleister abstützen können. Fremdstaatliche Zugriffsrechte und Cloud-Sicherheitsvorfälle belasten zunehmend wirtschaftliche Akteure; die entsprechenden Risiken hemmen die Nutzung von neuen Technologien.
- Technische Sicherheit der IKT und der Cloud-Nutzung sowie der Umgang mit Lieferantenabhängigkeiten sind bedeutsam; dafür braucht es gemeinsame Standards und ein Risiko-Management-Framework.
- Begrifflichkeiten sind heute noch zu wenig geklärt, was den Dialog erschwert; neben technischen Aspekten gehören dazu auch «Datensouveränität», «technologische Souveränität», «wirtschaftliche Souveränität» und «digitale Selbstbestimmung» im Zusammenhang mit der Cloud.

Zielsetzung

- Service-Güteklassen und Risiko-Management-Framework für IKT- und Cloud-Nutzung schaffen und Organisationen in der Anwendung befähigen. Dabei gilt, wann immer möglich, sich an bereits bestehenden Standards zu orientieren.
- Relevante IKT- und Cloud-Begriffe werden definiert und publiziert.
- Einhaltung von IKT- und Cloud-Standards auditierbar gestalten.

Massnahmen

- IKT- und Cloud-Lösungen, die den Service-Güteklassen (bezüglich Amtsgeheimnis, Informationsschutz, Datenschutz, Verfügbarkeit etc.) entsprechen, werden in einem öffentlichen Verzeichnis aufgeführt.
- Publikation eines Cloud-Glossars, der die Terminologie vereinheitlicht.

7.3 Handlungsfeld 2: Recht und Regulation

Rechtliche und regulatorische Fragestellungen zur Cloud-Nutzung klären und beantworten

Ausgangslage

- Unter Spezialisten gilt als offene Frage, unter welchen Umständen durch StGB-Tatbestände geschützte Daten in die Cloud gegeben werden dürfen (z. B. Bankgeheimnis nach Art. 47 BankG, Amtsgeheimnis nach Art. 320 StGB, Berufsgeheimnis nach Art. 321 und 321bis StGB)
- Einen Aspekt bilden Datenherausgabepflichten von Providern aus Drittstaaten, die hinsichtlich ihrer Rechtsfolgen und wirtschaftlichen Implikationen ungeklärt sind (vgl. US CLOUD Act).
- Es stellen sich (völker-) rechtliche Fragen, namentlich im Bereich der staatlichen Jurisdiktion, der Menschenrechte und des Datenschutzrechtes an den Schnittstellen verschiedener Rechtsordnungen.

Zielsetzung

- (Völker-) rechtlicher Rahmen ist geklärt, insbesondere im Bereich Datenschutz, Informationsschutz, Geheimnisschutz.
- Widersprüchliche Rechtsnormen sind aufgelöst bzw. mit Empfehlungen zum Umgang damit adressiert.

Massnahmen

- Eine departementsübergreifende Arbeitsgruppe für Rechts- und Regulationsfragen zum Cloud-Einsatz wird eingesetzt, die die Problemfelder juristisch aufarbeitet und Empfehlungen erarbeitet – insbesondere an den Gesetzgeber (vgl. Anhang C: Aufgeworfene Rechtsfragen).

7.4 Handlungsfeld 3: Internationale Vernetzung

Die internationale Vernetzung und den Einbezug der Schweiz in europäischen Initiativen wie GAIA-X prüfen

Ausgangslage

- In anderen Staaten wurden Cloud-Projekte rasch als politisches Thema besetzt, was anstelle eines pragmatischen Vorgehens mit zeitnahen Lösungen zu längeren Debatten führte.
- Solche Projekte, insbesondere auch GAIA-X der EU schaffen Chancen und Risiken für die Schweiz. Die EU investiert in solche Projekte auch, um ihre digitale Souveränität und Unabhängigkeit gegenüber externer Technologie zu erhöhen.
- Die durch die Experten benannten Cloud-Bedürfnisse von Schweizer Akteuren weisen eine hohe Dringlichkeit auf:

Innerhalb weniger Jahre sollen die Grundlagen für gewisse Nutzungsszenarien geschaffen und die Umsetzung realisiert werden.

- Die sich stellenden Fragen rund um Datensouveränität, technologische und wirtschaftliche Souveränität im Zusammenhang mit der Cloud werden noch nicht hinreichend verstanden.

Zielsetzung

- Der öffentliche und politische Dialog wird als Veränderungsprozess verstanden und gestaltet.
- Dabei werden die sich stellenden Fragen rund um Datensouveränität, politische, technologische und wirtschaftliche Souveränität im Zusammenhang mit der Cloud klar und sachlich positioniert.
- Die Legitimation des staatlichen Handelns mit Blick auf die Swiss Cloud ist validiert, d. h. staatliches Handeln ist hinsichtlich seiner Grundlage, Notwendigkeit und Zielsetzung geklärt und so auch klar kommuniziert.
- International mit Cloud-Initiativen anderer Länder, insbesondere der EU vernetzen, Chancen nutzen und Risiken minimieren, beispielsweise durch Beteiligung.

Massnahmen

- Regelmässige zeitnahe und transparente Berichte und Informationen zum Thema Cloud
- Schulungskampagne für Schlüsselpersonen.
- Informationsanlässe für Journalisten und politische Entscheidträger.
- Nach Möglichkeit international mit Cloud-Initiativen anderer Länder vernetzen.

7.5 Handlungsfeld 4: Digitale Verwaltung Schweiz

Im Rahmen des Aufbaus der Digitalen Verwaltung Schweiz (DVS) die institutionellen Grundlagen der Schweizer Verwaltung zur Nutzung von gemeinsamen Cloud-Leistungen entwickeln

Ausgangslage

- Die öffentliche Hand ist daran, neue Technologien für die Digitalisierung nutzbar zu machen und dafür die Voraussetzungen zu schaffen (vgl. z. B. betreffend die Bundesverwaltung die Strategische Initiative SI-4 «Hybrid Multi-Cloud» sowie die SI-5 «neue Technologien», die Teil der IKT-Strategie 2020-2023 des Bundes sind.
- Entsprechend besteht ein grosser Befähigungsbedarf (Knowhow-Aufbau, Teilen von Best Practices)
- Auch besteht eine potenzielle Nachfrage für gemeinsame Service-Angebote im Rahmen der Initiative Digitale Verwaltung Schweiz. Die Nachfrage kann u. a. über eOperations AG gebündelt werden.

Zielsetzung

- Die öffentliche Verwaltung kennt und ist befähigt, neue Technologien, insbesondere Cloud-Leistungen angemessen und nutzenstiftend einzusetzen. Dafür braucht es auch eine

vorausschauende Exploration und eine Vernetzung von Experten.

- Die rechtlichen und technischen Kompetenzen auf Ebene Kanton bzw. Bund werden weiter harmonisiert und wo sinnvoll zusammengeführt.
- Gemeinsame Bedarfe an Service-Angeboten sind identifiziert und Lösungen für deren Befriedigung beauftragt.

Massnahmen

- Bestehende IKT-Harmonisierungsvorhaben und Strategische Initiativen werden beschleunigt.
- Die Initiative Digitale Verwaltung Schweiz prüft den Bedarf an Befähigung und gemeinsamer Service Angebote und definiert die nächsten Schritte.

7.6 Handlungsfeld 5: Völkerrechtlicher Rahmen

Die (völker-) rechtlichen Rahmenbedingungen für die Gewährleistung der Immunität von Daten in Public Clouds für internationale Organisationen prüfen

Ausgangslage

- Internationale Organisationen (z. B. IKRK oder die UN), aber auch das EDA, haben einen Bedarf an weltweit verfügbaren Leistungen mit Cloud-Eigenschaften.
- Es braucht für diese Art Nutzung jedoch die Garantie, dass keine Datenherausgabepflichten an Dritte bestehen, sowie die Garantie, dass das Völkerrecht eingehalten wird, z. B. hinsichtlich Immunität.

Zielsetzung

- Für Daten dieser Organisationen, die Immunität geniessen, braucht es eine klare und durchsetzbare Regelung der Immunität auch bei Nutzung von Cloud Leistungen.
- Das EDA überprüft die Anwendung des Schweizer Rechts bezüglich der Immunität solcher Datenhaltung.

Massnahmen

- Das EDA initiiert internationale Vorstösse, um für internationale Organisationen nutzbare Cloud-Angebote zu ermöglichen.

7.7 Ergänzende Massnahmen für einzelne Bedarfsträger

Dialog mit den Branchen zur Entwicklung von Hilfsinstrumenten zur chancen- und risikobewussten Nutzung von Cloud Diensten führen

Ausgangslage

- Das Wissen um die IKT- und Cloud-Nutzung ist noch zu wenig breit in der Wirtschaft und der Verwaltung vorhanden, um die Chancen neuer IKT- und Cloud-Technologien vollständig und risikoadäquat zu realisieren: Dies betrifft insb. gewisse KMU, Entscheider im Fach, Datenschützer, Vertragsjuristen und Einkäufer.
- Es fehlen geprüfte und branchenspezifische Lösungsmuster («Kochbuchrezepte»).

Zielsetzung

- Bedürfnisse und Ansätze zur Befähigung für neue Technologien und Cloud mit Industriepartnern sind geklärt, um die Beurteilungsfähigkeit auf allen Stufen zu verbessen.

- Fördern von geprüften und branchen- bzw. themenspezifischen Lösungsmustern für die IKT- und Cloud-Nutzung (z. B. Cloud-Nutzung im Gesundheitswesen, Verschlüsselungsansätze).

Massnahmen

- Branchendialog mit Industriepartnern führen, damit marktgerechte Weiterbildungsmassnahmen entstehen (insb. für KMU bzw. deren IT-Dienstleister, Entscheidern im Fach, Datenschützer, Vertragsjuristen und Einkäufern), z. B. durch branchen- und themenspezifische Musterlösungen (Business Cases, Verträgen, Pflichtenheftern, Operating Model-, Betriebs-, Controlling- und Risk-Management-Konzepte usw.)

Bedarf und Weiterentwicklung von krisenresistenten Leistungen für Betreiber kritischer Infrastrukturen klären und konkretisieren

Ausgangslage

- Für krisenresistente und durchhaltefähige Organisationen werden Infrastrukturen mit Cloud-ähnlichen Eigenschaften benötigt.

Zielsetzung

- Das Vorgehen für krisenresistente Infrastrukturen ist definiert.

Massnahmen

- Mit krisenresistenten und durchhaltefähigen Organisationen den Bedarf an krisenresistenten Infrastrukturen mit Cloud-ähnlichen Eigenschaften ermitteln, Lösungsansätze erarbeiten und Synergien identifizieren, um ein Folgevorgehen festzulegen.

8 Anhang A: Glossar

AI	Künstliche Intelligenz (Artificial Intelligence)
BankG	Bundesgesetz über die Banken und Sparkassen, SR 952.0
BCM	Betriebliches Kontinuitätsmanagement (Business Continuity Management)
BFS	Bundesamt für Statistik
Big Data	Datenmengen, welche beispielsweise zu gross, zu komplex, zu schnelllebig oder zu schwach strukturiert sind, um sie mit manuellen und herkömmlichen Methoden der Datenverarbeitung auszuwerten
CISO	Chief Information Security Officer
BFS	Bundesamt für Statistik
CLOUD Act	Claryfying Lawful Overseas use of Data Act, US-Gesetz zum Zugriff der US-Behörden auf gespeicherte Daten im Internet
Cloud Computing	Eine IT-Infrastruktur, die beispielsweise über das Internet verfügbar gemacht wird (siehe Anhang B, Kapitel 9)
Cloud-Leistung	IKT-Leistungen, welche durch Cloud-Computing erbracht werden
Cloud-Provider	Anbieter von IKT-Leistungen mittels einer Cloud Computing-Infrastruktur (siehe Anhang B, Kapitel 9)
Commodity	Gebrauchsgut; oft in Verbindung mit eingekaufter Leistung im IT- und Telekommunikationssektor
CRM	Kundenbeziehungsmanagement (Customer Relationship Management)
DB	Datenbank
Digital Marketplace	Eine Auflistung der Cloud-Leistungen von Cloud-Providern in einem Online-Shop
DSG	Bundesgesetz über den Datenschutz, SR 253.1
DWH	Datenlager (Data Warehouse)
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragte
EDK	Schweizerische Konferenz der kantonalen Erziehungsdirektoren
ERP	Integriertes IT-System zur Unternehmensplanung und Geschäftsabwicklung (Enterprise Resource Planning)
EU-DSGVO	Europäische Datenschutz-Grundverordnung
FINMA	Eidgenössische Finanzmarktaufsicht
GAIA-X	Eine europäische Cloud-Initiative, die insbesondere durch Deutschland und Frankreich vorangetrieben wird
GATT	Allgemeines Zoll- und Handelsabkommen (General Agreement on Tariffs and Trade)
Hybrid Cloud	Siehe Anhang B, Kapitel 9, Tabelle 4
Hyperscaler	Ein globaler Cloud-Provider, der über weltweite Präsenz von Rechenzentren verfügt

IaaS	Infrastructure-as-a-Service (Siehe Anhang B, Kapitel 9, Tabelle 3)
IKRK	Internationales Komitee vom Roten Kreuz
IKT	Informations- und Kommunikationstechnik
IoT	Internet of Things
ISB	Informatiksteuerungsorgan des Bundes
ISchV	Informationsschutzverordnung, SR 510.411
IT	Informationstechnik
KMU	Kleine und mittlere Unternehmen
Multi Cloud	Siehe Anhang B, Kapitel 9, Tabelle 4
NEAT	Neue Eisenbahn-Alpentransversale
NGO	Nichtregierungsorganisation (non-governmental organization)
NOGA	Allgemeine Systematik der Wirtschaftszweige (Nomenclature générale des activités économiques)
NPO	Nicht-gewinnorientierte Organisation (non-profit organization)
openAPI	Offene Schnittstellen
Outsourcing	Auslagerung; oft in Verbindung mit betrieblichen Tätigkeiten, die IT involvieren
PaaS	Platform-as-a-Service (Siehe Anhang B, Kapitel 9, Tabelle 3)
Privacy Shield	Eine informelle Absprache auf dem Gebiet des Datenschutzrechts zwischen der EU und den USA
Private Cloud	Siehe Anhang B, Kapitel 9, Tabelle 4
Process Mining	Rekonstruktion und Auswertung von Geschäftsprozessen auf Basis digitaler Spuren in IT-Systemen
Public Cloud	Siehe Anhang B, Kapitel 9, Tabelle 4
RINA-Prozess	Risikomanagementmethode der schweizerischen Bundesverwaltung zur Reduktion der nachrichtendienstlichen Ausspähung
RPA	Robotergesteuerte Prozessautomatisierung (Robotic Process Automation)
SaaS	Software-as-a-Service (Siehe Anhang B, Kapitel 9, Tabelle 3)
SBFI	Staatssekretariat für Bildung, Forschung und Innovation
SBVg	Schweizerische Bankiervereinigung
Schrems II	Ein Gerichtsurteil des Europäischen Gerichtshofes in Bezug auf das Privacy Shield Abkommen
Sektorgruppe	Einordnung der Bedarfsgruppen nach öffentlicher Hand, Wirtschaft, Wissenschaft, Gesundheitswesen, etc.
Service-Provider	Anbieter von einer IKT-Leistung, welche einem Service entspricht
SIK	Schweizerische Informatikkonferenz
StGB	Schweizerisches Strafgesetzbuch, SR 311.0
Swisstopo	Bundesamt für Landestopografie
time-to-market	Dauer von Produktentwicklung bis zur Platzierung am Markt
UN	Vereinigte Nationen (United Nations)

WIsB	Weisungen des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung
WTO	Welthandelsorganisation (World Trade Organization)

9 Anhang B: Kontext «Cloud Computing»

Cloud Computing hat sich in den letzten 10 Jahren zu einem wichtigen Rückgrat unserer Gesellschaft entwickelt, gleichermassen im Privaten wie im Geschäftlichen. Der dadurch initiierte gesellschaftliche wie auch der wirtschaftliche Wandel durch diese «Cloudifizierung» von Dienstleistungen ist vergleichbar mit der «Elektrifizierung» im 19. Jahrhundert. Cloud Computing findet sich mittlerweile in jedem Bereich unseres Lebens. Elektrische Zahnbürsten übermitteln via App unser Putzverhalten an den Hersteller. Autos berechnen die optimale Route mit aktuellen Verkehrsdaten in Sekundenschnelle neu. Zeitungen, Bücher und Filme können jederzeit und von (beinahe) jedem Ort der Welt bezogen und betrachtet werden.

Diese Beispiele illustrieren wesentliche Elemente der gängigen Definition von «Cloud Computing» des European Network and Information Security Agency (ENISA):

> *«Cloud Computing ist ein Modell der Datenverarbeitung, mit dem bei Bedarf, jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste)* zugegriffen werden kann*. Diese können schnell und mit minimalem Verwaltungsaufwand bzw. geringer Serviceprovider-Interaktion zur Verfügung gestellt werden.»*[24]

Diese Definition beruht auf den fünf essenziellen Charakteristiken des amerikanischen National Institute of Standard and Technology (NIST):

Servicemodelle	Eigenschaften
On-Demand Self Service	Die Provisionierung der Ressourcen (z. B. Rechenleistung, Storage) läuft automatisch ohne Interaktion mit dem Service-Provider ab.
Broad Network Access	Die Services sind mit Standard-Mechanismen über das Netz verfügbar und nicht an einen bestimmten Client gebunden.
Ressource Pooling	Die Ressourcen des Service-Providers liegen in einem Pool vor, aus dem sich viele Anwender bedienen können (Mandantenfähigkeit oder multi-tenant Modell), die Anwender wissen dabei nicht zwingend, wo sich die Ressourcen befinden.
Rapid Elasticity	Die Services können schnell und elastisch[25] zur Verfügung gestellt werden, in manchen Fällen auch automatisch. Aus Anwendersicht scheinen die Ressourcen daher unendlich zu sein.
Measured Services	Die Ressourcennutzung kann gemessen und überwacht werden und entsprechend bemessen auch den Cloud-Anwendern zur Verfügung gestellt werden.

Tabelle 2: Cloud Computing Charakteristiken nach NIST

Cloud-Service- und Bereitstellungsmodelle

Im Cloud Computing wird zwischen Cloud-Servicemodell und Cloud-Bereitstellungsmodell unterschieden. Das Servicemodell bezieht sich dabei auf die technische Fertigungstiefe einer Cloud-Leistung und das Bereitstellungsmodell auf die Art und Weise, wie eine Leistung bereitgestellt wird.

---

[24] Vgl. Cloud-Computing Studie des europäischen Parlaments, 2012, IP/A/IMCO/ST/2011-18, PE 475.104.

[25] Bezieht sich auf die Fähigkeit eines Cloud-Dienstes, dynamisch und automatisiert bei Bedarf Ressourcen hinzuzufügen/wegzunehmen, wenn die Nachfrage steigt oder sinkt.

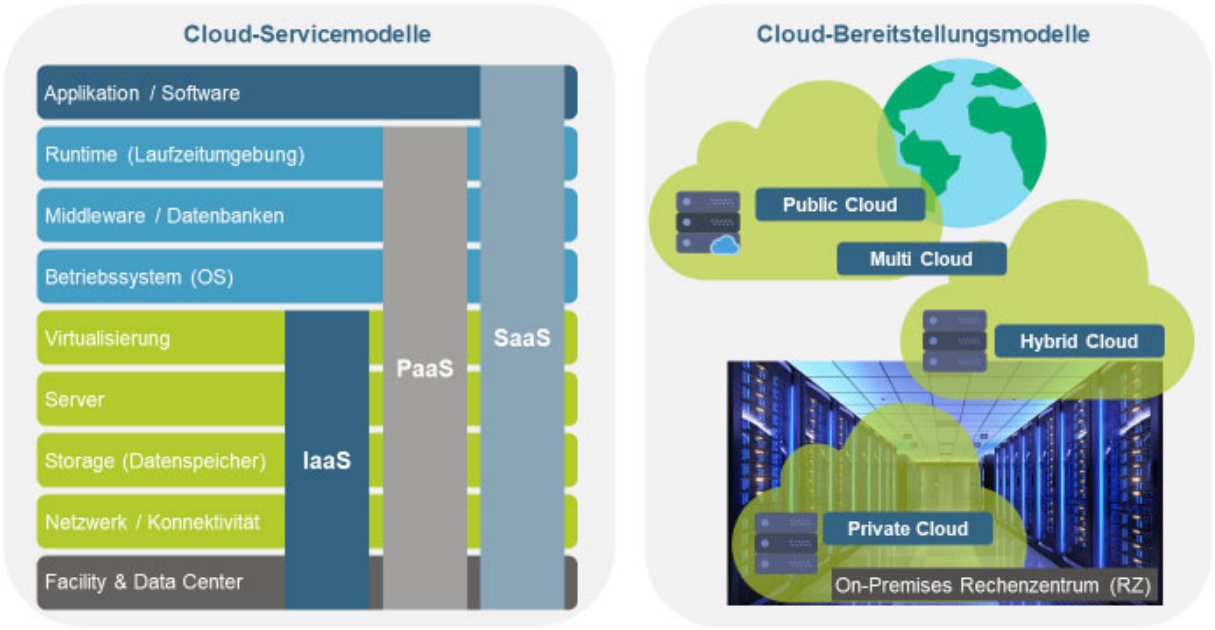

Abbildung 12: Begriffsklärung Cloud-Varianten

Das Cloud-Servicemodell wird üblicherweise in drei Bereiche unterteilt, denen drei aufeinander aufbauenden Architekturschichten entsprechen (siehe Abbildung 12):

- «**Infrastructure as a Service**» **(IaaS)** bildet dabei die Basis aller Servicemodelle und fokussiert sich auf den Infrastrukturbereich.
- «**Plattform as a Service**» **(PaaS)** baut auf IaaS auf, stellt aber Cloudnutzern nicht nur Infrastruktur bereit, sondern umfasst auch zusätzliche Komponenten, welche für das Funktionieren einer Anwendung notwendig sind.
- «**Software as a Service**» **(SaaS)** beinhaltet alle vorangegangenen Architekturschichten und stellt eine konsumfertige Lösung bereit (siehe Tabelle 3).

Servicemodelle	Eigenschaften
IaaS	Virtuelle **Infrastruktur-Instanzen** mit entsprechender Rechenleistung, Datenspeicher und Konnektivität
PaaS	Bereitgestellte Software-Entwicklungs- und **Laufzeit-Umgebung** mit darunterliegender Rechenleistung, Datenspeicher und Konnektivität
SaaS	Vollständige **Software-Lösung** oder Anwendungsprogramme, welche über das Netzwerk zugreifbar sind

Tabelle 3: Eigenschaften Cloud-Servicemodelle

Diese Cloud-Servicemodelle können auf unterschiedliche Weise bereitgestellt werden: In einer «**Private Cloud**» werden die Services nur einer einzigen Institution angeboten und entweder von dieser selbst oder durch Dritte betrieben.

Servicemodelle, welche einer breiten Gruppe oder einer ganzen Branche zur Verfügung gestellt werden, erhalten diese hauptsächlich aus einer «**Public Cloud**».

Da es unterschiedliche Anbieter von Public Cloud Lösungen gibt (Microsoft, Amazon, Google, Alibaba usw.), und diese beliebig kombiniert werden können, wird bei deren kombinierter Anwendung von sogenannten **«Multi Clouds»** gesprochen.

Eine sogenannte «**Hybrid Cloud**» kombiniert schliesslich eine Private Cloud und Public Cloud-Leistungen. Organisationen nutzen dieses Modell, um bestehende Lösungen mit Cloud-Lösungen zu verbinden (siehe Tabelle 4).

Bereitstellungs-modelle	Eigenschaften
Public Cloud	Mandantenfähige, **öffentlich** zugängliche Cloud-Ressourcen mit praktisch «unbegrenzter» Skalierbarkeit
Private Cloud	Cloud-Umgebung, die ausschliesslich **für eine Organisation** betrieben wird
Hybrid Cloud	**Gleichzeitiger Einsatz** von Public und Private Cloud-Services innerhalb derselben Systemarchitektur
Multi Cloud	**Mehrere Cloud-Services**, die in einer heterogenen Systemarchitektur gleichzeitig genutzt werden

Tabelle 4: Eigenschaften Cloud- Bereitstellungsmodelle

Weniger verbreitete Begriffe bei den Bereitstellungsmodellen sind Community Cloud, Government Cloud oder Healthcare Cloud. Hierbei handelt es sich mehrheitlich um Marketingbegriffe grosser Hersteller, welche die Servicemodelle für den gezielten Einsatz und unter Berücksichtigung der jeweiligen spezifischen Anforderungen, für gewisse Branchen bündeln.

10 Anhang C: Aufgeworfene Rechtsfragen

- Unter welchen Voraussetzungen findet in der Cloud eine Verletzung des Berufs-, Banken- oder Amtsgeheimnisses statt?
- Inwiefern können in einer Cloud Personendaten von nicht-personenbezogenen Daten sinnvoll unterschieden und entkoppelt werden? Wie ist rechtlich damit umzugehen, wenn unterschiedliche normative Standards auf unterschiedliche Daten in einer Cloud Anwendung finden (Differenzierungsmöglichkeit)?
- Ist der Straftatbestand bei Anwendungsfällen in der Cloud ausreichend definiert und gesetzlich geregelt?
- Unter welchen Voraussetzungen wird das Dienstgeheimnis im Militär verletzt?
- Unter welchen Voraussetzungen dürfen ausländische Behörden auf (Personen)daten in der Cloud zugreifen (Stichwort «Lawful Access» und CLOUD Act)?
- Inwiefern gelten die datenschutzrechtlichen Regeln zum internationalen Datenverkehr im Zusammenhang mit Herausgabeansprüchen bei einer Cloud (vgl. Art. 6 CH-DSG und Art. 45-46 EU-DSGVO)?
- Folgt ein Schweizer Gericht denselben Richtlinien wie der EuGH in dem Urteil, dass alle Exporte von Personendaten aus der EU in die USA der EU Datenschutz-Grundverordnung (DSGVO) unterliegen (oder analog in der Schweiz dem DSG)? Vgl. hierzu Schrems II[26]
- Wird ein «Executive Agreement» von der Schweiz benötigt, um bessere Rechtssicherheit zu schaffen und Datenschutz zu gewährleisten in Hinblick auf den CLOUD Act der USA?
- Ist ein «Executive Agreement» zum CLOUD Act förderlich in Hinblick auf Datenschutz und den rechtlichen Bedürfnissen der Organisationen in der Schweiz?
- Wie können die Daten von Personen, welche diplomatischer Immunitäten und Privilegien unterliegen, in der Cloud speziell geschützt werden?
- Ist es zulässig Cloud-Provider zu nutzen, welche Rechenzentren in Ländern unter Embargo haben?

[26] Vgl. z. B. https://www.lw.com/thoughtLeadership/Das-schrems-II-Urteil-des-EuGH-was-m%C3%BCssen-unternehmen-bei-internationalen-datentransfers-%C3%A4ndern, zuletzt aufgerufen am 27. November 2020.

11 Anhang D: Umfrage

11.1 Methodik

Im Rahmen der Bedarfserhebung wurde eine Expertenbefragung durchgeführt. Dabei wurde eine Klassierung entlang der allgemeinen Systematik der Wirtschaftszweige (NOGA) des Bundesamts für Statistik vorgenommen (vgl. Abs 1.4). Expertinnen innerhalb der Wirtschaftszweige wurden über Branchenverbände und Dachorganisationen identifiziert und zur Registrierung für die Teilnahme aufgefordert.

Insgesamt wurden 332 Personen zur Teilnahme eingeladen. Die Umfrage wurde am 20. Juli 2020 geöffnet und bis am 24. August offengehalten. Die neu registrierten Teilnehmerinnen wurden fortlaufend eingeladen, um jeder Teilnehmerin einen möglichst langen Zeitraum zur Beantwortung der Umfrage zu gewährleisten. Der letzte Versand von Einladungen erfolgte am 18. August 2020. Zudem wurden mit Ausnahme der letzten Versandgruppe sämtliche Teilnehmerinnen, die die Umfrage noch nicht ausgefüllt haben, mindestens einmal mittels Erinnerungsmail erinnert.

Zum Zeitpunkt der Schliessung der Umfrage haben 243 Teilnehmerinnen mindestens eine Frage beantwortet und 203 Teilnehmerinnen den Fragebogen vollständig ausgefüllt.

11.2 Thesen für die Bedarfserhebung

Wie in Abs. 1.2 erwähnt, wurden für die Bedarfserhebung Hypothesen entwickelt, welche sowohl bei der Entwicklung der Bausteine als auch bei der Ausarbeitung der Umfrage und der Interviews eine Rolle spielten.

Die Hypothesen wurden entlang von fünf Cloud Dimensionen formuliert (vgl. Abbildung 13 und Tabelle 5) und unterlagen zwei Rahmenbedingungen, damit die Bedarfserhebung Bezug nehmen konnte auf ein plausibilisiertes Szenario:

- Würde der Entscheid für eine «Swiss Cloud»-Infrastruktur getroffen, stünde in den nächsten fünf Jahren zur Verfügung.
- Die Swiss Cloud käme mit einer garantierten Betriebstätigkeit von mindestens zehn Jahren nach Betriebsaufnahme.

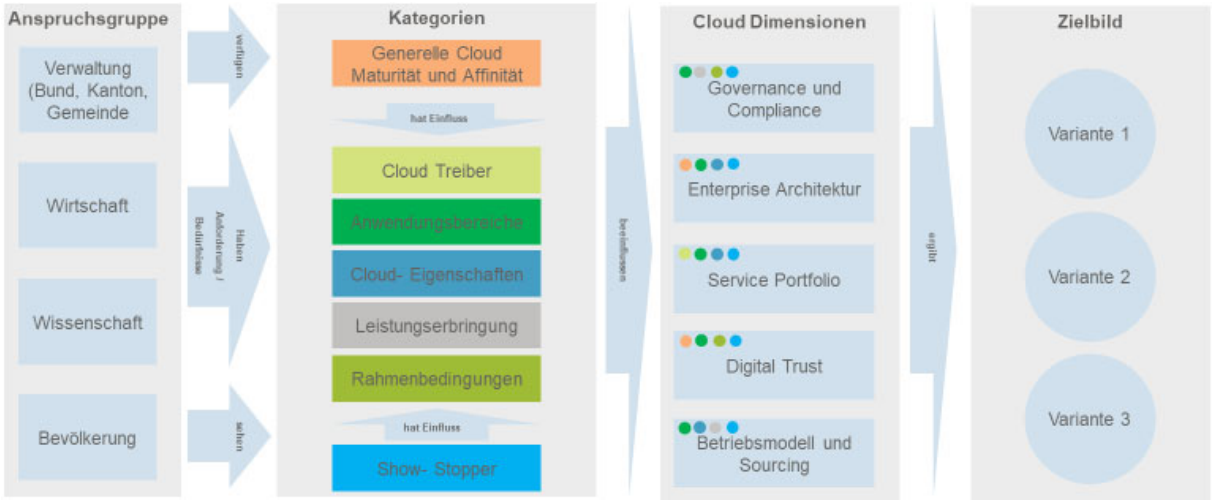

Abbildung 13: Frage-Kategorien, Anspruchsgruppen, Cloud-Dimensionen und deren Zusammenspiel

Cloud Dimension	Thesen
Governance und Compliance	• In vielen Bereichen, jedoch nicht flächendeckend, bestehen heute erst teilweise und branchenabhängig die notwendigen und umsetzbaren Richtlinien und Empfehlungen für die sichere und produktive Nutzung von Public Cloud Dienstleistungen von schweizerischen wie auch internationalen Providern. • Es besteht kein Anpassungsbedarf an den aktuellen rechtlichen Grundlagen und deren Anwendung ist für alle Unternehmen/Organisationen klar.[27]
Enterprise Architektur	• Die Nutzung von Public Cloud Services internationaler Provider nimmt in allen Bereichen in den nächsten 5 Jahren noch markant zu (z. B. > 30% des aktuellen IT-Workloads). • Den Unternehmen/Organisationen in den Bereichen fehlt es vielfach an Knowhow und/oder Ressourcen, um aktiv die IT- wie auch Geschäftstransformation im Rahmen der notwendigen Digitalisierungsvorhaben voranzutreiben.
Service-Portfolio	• Der Bedarf an innovativen und einfach zugänglichen Technologien und Services (IoT, Data Analytics, Big Data, AI usw.) wird sich in den nächsten 5 Jahren in allen Bereichen weiter verstärken. • Die Bereiche sehen eine erhöhte Abhängigkeit (Vendor Lock-in) von internationalen Cloud-Providern durch die zunehmende Verschiebung, Transformation und Weiterentwicklung von Lösungen in die Cloud sowie die Zunahme der Nutzung höherwertiger Cloud-Servicemodelle (IaaS → PaaS → SaaS). • Die hohe Wachstumsdynamik des Cloud-Marktes bringt eine rasante Weiterentwicklung von Serviceangeboten mit hoher Qualität, Professionalität und Innovationskraft.
Digital Trust (Informationssicherheit und Datenschutz)	• Alle Bereiche sehen in der Verfügbarkeit von Cloud-Leistungen (Datenverarbeitung und –Nutzung) aus der Schweiz eine Steigerung der Standortattraktivität und Wirtschaftlichkeit. • Dienstleistungen aus dem Bereich E-Government werden von der Bevölkerung eher akzeptiert, wenn die zugrundeliegende Datenverarbeitung und Speicherung durch den Bund, ein bundesnahes Unternehmen oder ein Konsortium unter Schweizer Kontrolle sichergestellt wird.
Betriebsmodell und Sourcing	• Die Vertreter aller Bereiche sehen ein erhöhtes Geschäftsrisiko, wenn sie einen substanziellen Anteil ihrer IT-Ressourcen von einem nichtschweizer Provider beziehen. • Die Vertreter aller Bereiche implizieren mit einer Swiss Cloud automatisch eine garantierte (und bei Bedarf vom Bund gestützte) Serviceerbringung (garantierte Betriebstätigkeit) und Datensicherheit. • Die Swiss Cloud muss nicht zwingend eine Infrastruktur mit beinhalten, sondern kann auch lediglich aus einem Set von verbindlichen Regeln bestehen.

Tabelle 5: Cloud-Dimensionen und Thesen für die Bedarfserhebung

11.3 Statistische Eckwerte

Die Umfrage bestand insgesamt aus 61 Fragen (vgl. Abs. 11.4), von denen je nach Antwortverlauf in jedem Fall mindestens 49 Fragen von jedem Teilnehmer abgefragt

[27] Hinweis: Diese These wurde bewusst so formuliert, um den konkreten Bedarf zu eruieren.

wurden. Über alle Teilnehmer und Antwortoptionen hinweg wurden im Umfragezeitraum 18’965 Antworten erfasst (inkl. Tabellenantworten).

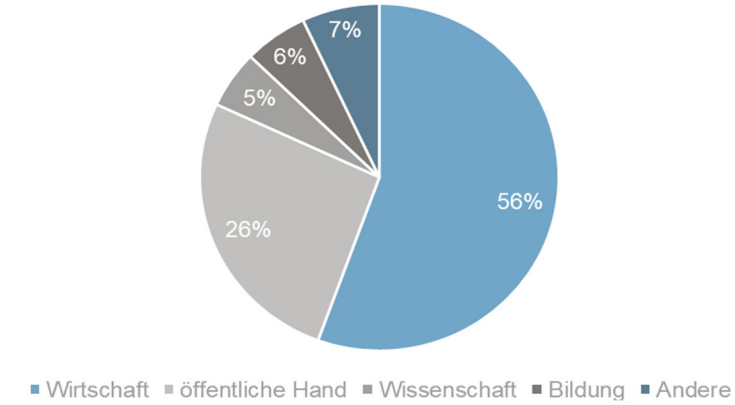

Abbildung 14: Teilnehmer nach Sektor (absoluter Wert und prozentual)

Die Verteilung der Umfrageteilnehmerinnen nach Organisationsgrösse und Bereich ist in Abbildung 15 dargestellt.[28] Dabei ersichtlich ist insbesondere die relativ geringe Repräsentation der Wissenschaft und Bildung in der Umfrage (vgl. Abs 1.4). Der Wirtschaftsbereich und die Öffentlichkeit sind über alle Organisationsgrössen relativ gut und erwartungsgemäss vertreten.

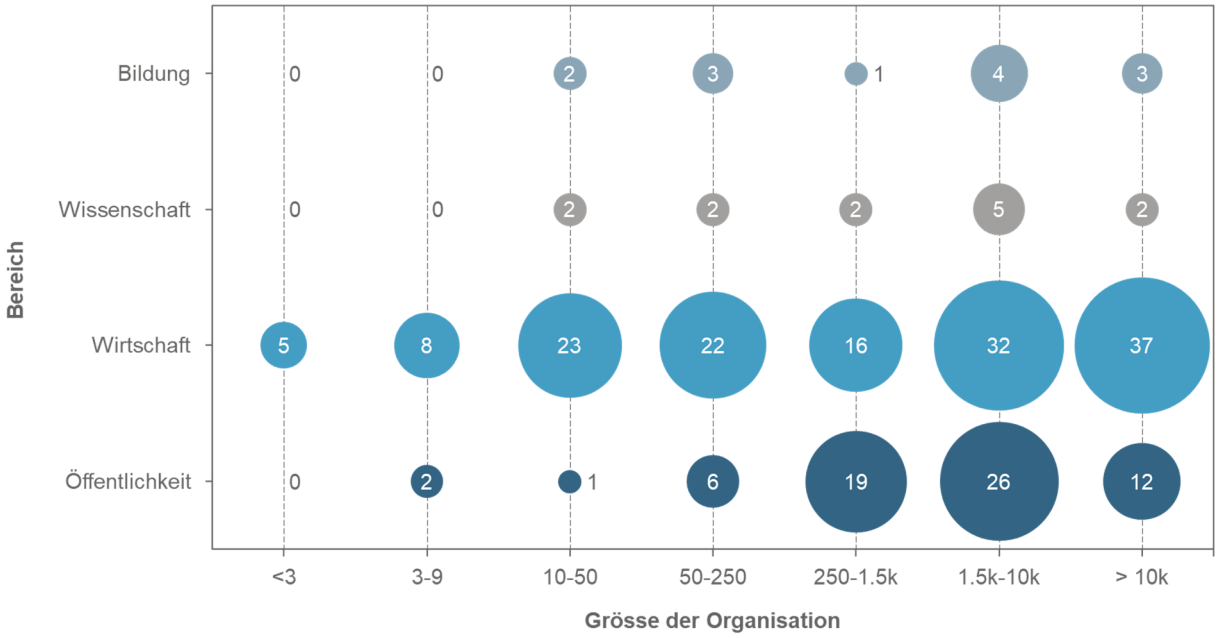

Abbildung 15: Teilnehmerinnen der Umfrage nach Bereich und Organisationsgrösse

[28] Von den 243 Teilnehmerinnen konnte der Bereich aufgrund von uneindeutigen Freitextangaben für sechs Teilnehmer nicht eindeutig zugeordnet werden. Diese Teilnehmer sind in allen Darstellungen nach Bereich nicht enthalten.

11.4 Fragenkatalog

In nachstehender Tabelle ist der Fragenkatalog der Umfrage erfasst.

Nr.	Frage
1.	**Unsere Organisation gehört zu folgendem Bereich:** – Öffentlichkeit – Wirtschaft – Wissenschaft – Bildung – Andere: [Freitextfeld]
2.	*(Frage erscheint, falls bei Frage 1 «Öffentlichkeit» gewählt wurde)* **Unsere Organisation gehört diesem Sektor an:** – Bundesumfeld – Kantonale Ebene – Gemeinde – Blaulicht-Organisation (BORS) – Anderer: [Freitextfeld]
3.	*(Frage erscheint, falls bei Frage 1 «Wirtschaft» gewählt wurde)* **Unsere Organisation gehört diesem Sektor an:** – Land- und Forstwirtschaft, Bergbau, Baugewerbe und Bau – Verarbeitendes Gewerbe – Energie- und Wasserversorgung – Handel, Gastgewerbe und Beherbergung – Verkehr, Transport und Logistik – Information und Kommunikation – Finanz- und Versicherungsdienstleister – Grundstück- und Wohnungswesen – Gesundheits- und Sozialwesen – Kunst, Unterhaltung und Erholung, sonstige Dienstleistungen – Freiberufliche, wissenschaftliche, wirtschaftliche und technische Dienstleistungen – Anderer: [Freitextfeld]
4.	*(Frage erscheint, falls bei Frage 1 «Bildung» gewählt wurde)* **Unsere Organisation gehört diesem Sektor an:** – Obligatorische Schule – Sekundarstufe – Tertiärstufe / Hochschule – Anderer: [Freitextfeld]
5.	**Die Grösse unserer gesamten Organisation umfasst:** – Weniger als 3 Beschäftigte – 3-9 Beschäftigte – 10-49 Beschäftigte – 50-249 Beschäftigte – 250-1'499 Beschäftigte – 1'500-9'999 Beschäftigte – 10'000 oder mehr Beschäftigte

Nr.	Frage
6.	**Das jährliche IT-Budget unserer Organisation beträgt schätzungsweise:** – Unter 300'000 CHF – Zwischen 300'000 CHF und 1 Mio. CHF – Zwischen 1 und 3 Mio. CHF – Zwischen 3 und 10 Mio. CHF – Zwischen 10 und 100 Mio. CHF – Zwischen 100 Mio. CHF und 1 Mia. CHF – Über 1 Mia. CHF – Keine Angabe
7.	**Ich würde mich am ehesten dem folgenden Bereich in meiner Organisation zuordnen:** – Geschäftsführung – IT – Vertrieb – Einkauf – Finanzen – Produktentwicklung / Forschung – Anderer: [Freitextfeld]
8.	**Meine Position in meiner Organisation entspricht am ehesten der Folgenden:** – Oberes Management / C-Level – Mittleres Management – Unteres Management – Fachspezialist/in (ohne Führungsfunktion) – Andere: [Freitextfeld]
9.	**Ich bin ein Cloud-Anbieter oder biete Beratungstätigkeiten bei der Implementierung von Cloud-Services an.** – Ja – Nein
10.	**Folgende IT-Betriebsmodelle werden in unserer Organisation genutzt:** *(Mehrfachantwort möglich)* – Interner IT-Betrieb – Teil-Outsourcing / Outtasking der IT(-Infrastruktur) – Outsourcing der gesamten IT(-Infrastruktur) – Andere: [Freitextfeld]
11.	**Unsere Organisation nutzt aktuell bereits Cloud-Services.** – Ja – Nein
12.	**In unserer Organisation gibt es Anwendungsbereiche, in denen bewusst auf den Einsatz einer Cloud verzichtet wird.** – Nein – Ja, nämlich: [Freitextfeld]

Nr.	Frage
13.	*(Frage erscheint, falls bei Frage 11 «Ja» gewählt wurde, d. h. Cloud-Services sind bereits im Einsatz)* **Die Cloud-Nutzung in unserer Organisation entspricht am ehesten dem folgenden Reifegrad:**[29] – Level 1: Bedarf an Cloud wurde erkannt, vereinzelte Cloud-Lösungen sind im Einsatz. Eine laufende Evaluation weiterer Services, die in die Cloud migriert werden könnten, findet statt. Eine Cloud-Strategie ist jedoch noch nicht festgelegt. – Level 2: Umfassende Cloud-Lösungen sind bereits in Betrieb und eine Cloud-Strategie ist definiert. Die Cloud als Treiber von Digitalisierung, Innovation und Agilität ist aber noch nicht klar wahrnehmbar. – Level 3: Eine «Cloud First»-Strategie ist festgelegt. Die konsequente Transformation des Unternehmens hinsichtlich Cloud-Nutzung findet gegenwärtig statt. – Level 4: Konsequente Integration der Cloud ins Business ist erfolgt. Innovation und Agilität werden gelebt, der aktuelle Fokus liegt auf weiteren Optimierungen.
14.	*(Frage erscheint, falls bei Frage 11 «Ja» gewählt wurde, d. h. Cloud-Services sind bereits im Einsatz)* **Die Nutzung von Cloud-Services in unserer Organisation ist weit fortgeschritten.** – Stimme völlig zu – Stimme eher zu – Stimme eher nicht zu – Stimme überhaupt nicht zu
15.	*(Frage erscheint, falls bei Frage 11 «Ja» gewählt wurde, d. h. Cloud-Services sind bereits im Einsatz)* **Der aktuelle Fortschritt der Cloud-Nutzung in unserer Organisation ist zufriedenstellend.** – Stimme völlig zu – Stimme eher zu – Stimme eher nicht zu – Stimme überhaupt nicht zu
16.	*(Frage erscheint, falls bei Frage 11 «Ja» gewählt wurde, d. h. Cloud-Services sind bereits im Einsatz)* **Heute nutzt unsere Organisation mehrheitlich das folgende Cloud-Bereitstellungsmodell:** – Private Cloud (eine eigene Cloud-Infrastruktur für unsere Organisation) – Public Cloud (unsere Organisation teilt sich die Cloud-Infrastruktur mit anderen Organisationen) – Hybrid Cloud (Kombination aus Public Cloud und Private Cloud / On-premise Infrastruktur) – Multi Cloud (Verwendung mehrerer Private und Public Clouds) – Anderes Cloud-Modell: – Keine Angabe
17.	*(Frage erscheint, falls bei Frage 11 «Ja» gewählt wurde, d. h. Cloud-Services sind bereits im Einsatz)* **Heute beträgt der Anteil an Public Cloud Services (im Verhältnis zum gesamten IT-Anwendungsbereich) in unserer Organisation:** – Weniger als 15% (punktuelle Cloud-Lösungen im Einsatz, z. B. für Bewerbermanagement) – Zwischen 15-50% (erste grössere Cloud-Lösungen in verschiedenen Prozessen im Einsatz) – Über 50% (Leistungen werden mehrheitlich aus der Cloud bezogen) – Keine Angabe

[29] Das Reifegradmodell basiert auf dem FHNW Maturity Model for Cloud and Enterprise IT (https://link.springer.com/chapter/10.1007/978-3-319-74322-6_9), zuletzt aufgerufen am 27. November 2020.

Nr.	Frage
18.	*(Frage erscheint, falls bei Frage 11 «Ja» gewählt wurde, d. h. Cloud-Services sind bereits im Einsatz)* **Wir nutzen folgende Cloud-Provider:** *(Mehrfachantwort möglich)* – Alibaba Cloud – AWS (Amazon Web Services) – Google Cloud Platform – IBM Cloud – Microsoft Azure – Oracle – SAP – Schweizer Cloud Provider – Andere(r) Provider
19.	*(Frage erscheint, falls bei Frage 11 «Ja» gewählt wurde, d. h. Cloud-Services sind bereits im Einsatz)* **Heute ist für unsere Organisation das relevanteste Cloud-Servicemodell:** – Infrastructure as a Service (IaaS): Virtuelle Infrastruktur-Instanzen mit entsprechender Rechenleistung, Storage und Konnektivität – Platform as a Service (PaaS): Bereitgestellte Software-Entwicklungs- und Laufzeit-Umgebung mit darunterliegender Rechenleistung, Storage und Konnektivität – Software as a Service (SaaS): Vollständige Software-Lösungen oder Anwendungsprogramme, die über das Netzwerk zugreifbar sind – Keine Angabe
20.	*(Frage erscheint, falls bei Frage 11 «Ja» gewählt wurde, d. h. Cloud-Services sind bereits im Einsatz)* **Unsere Organisation bezieht aktuell Services in den folgenden Anwendungsbereichen aus der Cloud:** *(Bewertung jeder Option entlang folgender Skala: Gar nicht, Teilweise, Mehrheitlich, Vollständig, Weiss nicht)* – Büroautomation (z. B. Arbeitsplatz, Office-Lösung) – Kommunikation / Kollaboration (z. B. Video-Telefonie, Datenaustausch) – Fachanwendungen – Geschäftsanwendungen (z. B. ERP, CRM) – Backend-Infrastruktur (z. B. Server, Storage, Datenbanken) – Daten-Analyse (z. B. BI, Big Data, Data Warehouse, Advanced Analytics) – Künstliche Intelligenz (z. B. Machine Learning, Cognitive Services) – IoT-Anwendungen (z. B. Smart City, Smart Building, Smart Metering) – Automatisierung (z. B. Robotic Process Automation, Process Mining) – Security – Disaster Recovery / BCM – Andere: [Freitextfeld]
21.	**Der Einsatz von Cloud-Services in unserer Organisation wird durch eine Cloud-Governance (Organisation, Prozesse, Weisungen, Richtlinien, Leitfäden etc.) wirksam gesteuert.** – Stimme völlig zu – Stimme eher zu – Stimme eher nicht zu – Stimme überhaupt nicht zu
22.	**Unsere Organisation verfügt über eine Cloud-Strategie (integriert in die IT-Strategie oder losgelöst).** – Stimme völlig zu – Stimme eher zu – Stimme eher nicht zu – Stimme überhaupt nicht zu

Nr.	Frage
23.	**Unsere Organisation hat eine Roadmap, die aufzeigt, welche Anwendungsbereiche in den nächsten 2-3 Jahren aus der Cloud bezogen oder in die Cloud migriert werden sollen.** – Stimme völlig zu – Stimme eher zu – Stimme eher nicht zu – Stimme überhaupt nicht zu
24.	**Unsere Organisation soll künftig Services in den folgenden Anwendungsbereichen aus der Cloud beziehen:** *(Bewertung jeder Option entlang folgender Skala: Gar nicht, Teilweise, Mehrheitlich, Vollständig, Weiss nicht)* – Büroautomation (z. B. Arbeitsplatz, Office-Lösung) – Kommunikation / Kollaboration (z. B. Video-Telefonie, Datenaustausch) – Fachanwendungen – Geschäftsanwendungen (z. B. ERP, CRM) – Backend-Infrastruktur (z. B. Server, Storage, Datenbanken) – Daten-Analyse (z. B. BI, Big Data, Data Warehouse, Advanced Analytics) – Künstliche Intelligenz (z. B. Machine Learning, Cognitive Services) – IoT-Anwendungen (z. B. Smart City, Smart Building, Smart Metering) – Automatisierung (z. B. Robotic Process Automation, Process Mining) – Security – Disaster Recovery / BCM – Andere: [Freitextfeld]
25.	**Der Einsatz von Cloud-Services beeinflusst unsere Aufbau- und Ablauforganisation spürbar.** – Stimme völlig zu – Stimme eher zu – Stimme eher nicht zu – Stimme überhaupt nicht zu
26.	**In den nächsten fünf Jahren steigt der Anteil der Cloud-Anwendungsbereiche in unserer Organisation geschätzt um:** – Gar nicht (Anteil wird sinken) – Gleichbleibend – Weniger als 15% – Zwischen 15-50% – Mehr als 50%
27.	**Künftig ist für unsere Organisation das relevanteste Cloud-Servicemodell:** – Infrastructure as a Service (IaaS): Virtuelle Infrastruktur-Instanzen mit entsprechender Rechenleistung, Storage und Konnektivität – Platform as a Service (PaaS): Bereitgestellte Software-Entwicklungs- und Laufzeit-Umgebung mit darunterliegender Rechenleistung, Storage und Konnektivität – Software as a Service (SaaS): Vollständige Software-Lösungen oder Anwendungsprogramme, die über das Netzwerk zugreifbar sind – Keine Angabe
28.	**Unsere Organisation nutzt die folgenden Cloud-Fähigkeiten noch zu wenig:** *(Mehrfachantwort möglich)* – Skalierbarkeit / Elastizität (herauf- sowie herunterskalieren von Ressourcen) – Rasche Verfügbarkeit von Services – Automatisierung – Hochverfügbarkeit – Dynamische Verrechnungsmodelle – Globale Verfügbarkeit von Services – Andere: – Keine der Antworten

Nr.	Frage
29.	**Die heutigen Angebote der Cloud-Provider sind ausreichend, um unsere Anwendungsfälle abzudecken.** – Stimme völlig zu – Stimme eher zu – Stimme eher nicht zu – Stimme überhaupt nicht zu – Keine Angabe
30.	**Die Anforderungen unserer Organisation in Bezug auf Cloud-Services werden abgedeckt durch den aktuell angebotenen Service...** *(Bewertung jeder Option entlang folgender Skala: Stimme völlig zu, Stimme eher zu, Stimme eher nicht zu, Stimme überhaupt nicht zu)* – … globaler Cloud-Provider. – … europäischer Cloud-Provider (EU/EFTA). – … Schweizer Cloud-Provider.
31.	**Cloud-Services verschiedener Provider lassen sich heute ausreichend kombinieren (Multi Cloud).** – Stimme völlig zu – Stimme eher zu – Stimme eher nicht zu – Stimme überhaupt nicht zu – Keine Angabe
32.	**Die heute von uns verwendeten Architekturstandards sind für die Cloud-Nutzung in unserer Organisation zweckdienlich.** – Stimme völlig zu – Stimme eher zu – Stimme eher nicht zu – Stimme überhaupt nicht zu – Keine Angabe
33.	**Ein möglichst umfassendes Dienstleistungs- und Angebots-Portfolio unserer Cloud-Provider ist ausschlaggebend für den Einsatz von Cloud-Services in unserer Organisation.** – Stimme völlig zu – Stimme eher zu – Stimme eher nicht zu – Stimme überhaupt nicht zu
34.	**Für unsere Organisation ist der rasche und einfache Zugang zu neuen Technologien (z. B. ohne Investitionen in Beschaffung und Aufbau eigener IT-Infrastruktur) ausschlaggebend.** – Stimme völlig zu – Stimme eher zu – Stimme eher nicht zu – Stimme überhaupt nicht zu
35.	**Für unserer Organisation ist das Vorhandensein eines Schweizer Marktplatzes, über den wir integrierte und auf Schweizer Bedürfnisse ausgerichtete Services von verschiedenen Providern beziehen können, ausschlaggebend.** – Stimme völlig zu – Stimme eher zu – Stimme eher nicht zu – Stimme überhaupt nicht zu

Nr.	Frage
36.	**Der Cloud-Provider, von dem meine Organisation zukünftig Services bezieht, soll...** *(Bewertung jeder Option entlang folgender Skala: Wichtig, Eher wichtig, Eher unwichtig, Unwichtig)* – ... unter Schweizer Recht und Gerichtsstand stehen. – ... in Schweizer Mehrheitsbesitz sein. – ... meine Daten ausschliesslich in der Schweiz bearbeiten. – ... meine Daten ausschliesslich in der EU / EFTA bearbeiten. – ... keiner Pflicht zur Datenherausgabe an eine dritte Stelle unterliegen.
37.	**Cloud-Lösungen eines Schweizer Providers schätzen wir im Vergleich zu internationalen Providern wie folgt ein:** *(Bewertung jeder Option entlang folgender Skala: Hoch, Mittel, Tief)* – Im Nutzen vergleichsweise: *[Hoch, Mittel, Tief]* – Hinsichtlich Kosten vergleichsweise: *[Hoch, Mittel, Tief]*
38.	**Worin würde der Standortvorteil einer Schweizer Cloud für Ihre Organisation bestehen?** *(Mehrfachantwort möglich)* – Rechtliche Sicherheit – Datenschutz – Resilienz – Qualität – Kosten – Auf Schweizer Bedürfnisse ausgerichtete Angebote – Andere(r): [Freitextfeld] – Kein Standortvorteil
39.	**Unsere Organisation ist bereit, für vergleichbare Cloud-Services eines Schweizer Providers im Vergleich zu internationalen Cloud-Providern mehr zu bezahlen.** – Nein – Ja, bis zu 5% mehr – Ja, bis zu 10% mehr – Ja, bis zu 20% mehr – Ja, bis zu 30% mehr – Ja, über 30% mehr
40.	**Eine durch den Bund oder durch ein Konsortium unter Schweizer Kontrolle zur Verfügung gestellte Cloud-Infrastruktur würde zu einem substanziellen Mehrwert für meine Organisation führen (z. B. hinsichtlich Rechtssicherheit, betrieblichen Risiken, einfacherer Zusammenarbeit mit den Providern etc.).** – Stimme völlig zu – Stimme eher zu – Stimme eher nicht zu – Stimme überhaupt nicht zu
41.	**Unsere Organisation sieht die Aufgabe des Bundes im Zusammenhang mit der Verwendung von Cloud-Services wie folgt:** *(Mehrfachantwort möglich)* – Schaffung von verbindlichen, rechtlichen und regulatorischen Rahmenbedingungen für den Einsatz von Cloud-Services – Förderung von technischen Architekturstandards für eine sichere, transparente und zuverlässige Nutzung von Cloud-Services – Förderung eines Schweizer Marktplatzes für die Nutzung von nationalen wie internationalen Cloud-Services unter Einhaltung von lokalen und branchenüblichen Vorgaben und Gesetzen – Aufbau und Betrieb einer Schweizer Cloud-Infrastruktur – Bildung und Förderung eines Schweizer Konsortiums für den Aufbau und Betrieb einer Schweizer Cloud-Infrastruktur – Beteiligung am europäischen Cloud-Projekt GAIA-X – Andere: [Freitextfeld] – Wir sehen keinen Bedarf einer staatlichen Rolle

Nr.	Frage
42.	**Für die künftige Cloud-Nutzung unserer Organisation spielt der leichte Zugang zu Technologien (wie z. B. IoT, Data Analytics, Big Data, künstlicher Intelligenz, Automatisierung) eine entscheidende Rolle.** – Stimme völlig zu – Stimme eher zu – Stimme eher nicht zu – Stimme überhaupt nicht zu
43.	**Unsere Geschäftstätigkeit wird sich durch über die Cloud bereitgestellte Technologien (wie z. B. IoT, Data Analytics, Big Data, künstlicher Intelligenz, Automatisierung) in Zukunft stark verändern.** – Stimme völlig zu – Stimme eher zu – Stimme eher nicht zu – Stimme überhaupt nicht zu
44.	**Der Einsatz von Cloud-Services führt zu einem Wettbewerbsvorteil unserer Organisation (z. B. schnellere Time-to-Market oder grössere Innovationskraft).** – Stimme völlig zu – Stimme eher zu – Stimme eher nicht zu – Stimme überhaupt nicht zu
45.	**Wie wichtig sind die folgenden Cloud-Fähigkeiten bei der Beschaffung von neuen Lösungen bzw. bei der Ablösung vorhandener Anwendungen?** *(Bewertung jeder Option entlang folgender Skala: Wichtig, Eher wichtig, Eher unwichtig, Unwichtig)* – Skalierbarkeit / Elastizität (herauf- sowie herunterskalieren von Ressourcen) – Rasche Verfügbarkeit von Services – Automatisierung – Hochverfügbarkeit – Dynamische Verrechnungsmodelle – Globale Verfügbarkeit von Services
46.	**Unsere Organisation verfügt über praktikable Rechtsgrundlagen für die Cloud-Nutzung.** – Ja – Nein – Keine Angabe
47.	**Personenbezogene Daten von Schweizern werden von unserer Organisation teilweise auch im Ausland gespeichert/verarbeitet.** – Ja – Nein – Keine Angabe
48.	**In unserer Organisation werden personenbezogene Daten von EU / EFTA-Bürgern gespeichert / verarbeitet.** – Ja – Nein – Keine Angabe
49.	**Zusätzlich zu den generellen gesetzlichen Vorgaben unterliegt unsere Organisation den folgenden Vorgaben, die für den Einsatz von Cloud-Services zu berücksichtigen sind:** *(Mehrfachantwort möglich)* – Regulatorischen Vorgaben (z. B. der FINMA) – Richtlinien oder Empfehlungen übergeordneter Organisationen (z. B. von Branchenverbänden) – Einer eigenen Governance – Anderem: [Freitextfeld] – Keine Angabe

Nr.	Frage
50.	**Ungenügende Leistungsversprechen hinsichtlich Service-Levels behindern eine verstärkte Cloud-Nutzung in unserer Organisation.** – Stimme völlig zu – Stimme eher zu – Stimme eher nicht zu – Stimme überhaupt nicht zu
51.	**Für unsere Organisation nicht akzeptable Vertragsbedingungen behindern eine verstärkte Cloud-Nutzung.** – Stimme völlig zu – Stimme eher zu – Stimme eher nicht zu – Stimme überhaupt nicht zu
52.	**Eine verstärkte Nutzung der Cloud in unserer Organisation wird durch hohe Betriebskosten behindert.** – Stimme völlig zu – Stimme eher zu – Stimme eher nicht zu – Stimme überhaupt nicht zu
53.	**Der Wechsel in die Cloud wird durch hohe Transitionsrisiken behindert.** – Stimme völlig zu – Stimme eher zu – Stimme eher nicht zu – Stimme überhaupt nicht zu
54.	**Unsere Organisation würde künftig mehr Cloud-Services beziehen, wenn wir dem Vorbild eines grossen Vertreters unserer Branche folgen könnten.** – Stimme völlig zu – Stimme eher zu – Stimme eher nicht zu – Stimme überhaupt nicht zu
55.	**Unsere Organisation sieht sich befähigt, Cloud-Vorhaben ohne externe Beratung oder Unterstützung umsetzen zu können.** – Stimme völlig zu – Stimme eher zu – Stimme eher nicht zu – Stimme überhaupt nicht zu
56.	**Die Nutzung einer Public Cloud führt zu kritischen Abhängigkeiten vom jeweiligen Cloud-Provider.** – Stimme völlig zu – Stimme eher zu – Stimme eher nicht zu – Stimme überhaupt nicht zu
57.	**Die Nutzung einer Public Cloud erhöht das Risiko eines (unerwünschten) Datenabflusses.** – Stimme völlig zu – Stimme eher zu – Stimme eher nicht zu – Stimme überhaupt nicht zu

Nr.	Frage
58.	**Internationale Public Cloud Provider behandeln Daten unserer Organisation nach branchenüblichen Standards.** – Stimme völlig zu – Stimme eher zu – Stimme eher nicht zu – Stimme überhaupt nicht zu – Keine Angabe
59.	**Der Bund hat für die Cloud-Nutzung bessere Rahmenbedingungen zu schaffen (z. B. hinsichtlich Rechtssicherheit, Datenschutz, Standortförderung).** – Stimme völlig zu – Stimme eher zu – Stimme eher nicht zu – Stimme überhaupt nicht zu
60.	**Unsere Branchenverbände respektive Dachorganisationen haben für die Cloud-Nutzung bessere Rahmenbedingungen zu schaffen (z. B. hinsichtlich Rechtsicherheit, Datenschutz, Standortförderung).** – Stimme völlig zu – Stimme eher zu – Stimme eher nicht zu – Stimme überhaupt nicht zu
61.	**Dürfen wir Sie bei Bedarf zur Vertiefung Ihrer Antworten kontaktieren?** – Nein – Ja. Meine Kontaktdaten (Name und Emailadresse) sind: *[Freitextfeld]*