Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK
Digitale Transformation und IKT-Lenkung DTI

Strategische Initiative SI-4 «Hybrid Multi-Cloud»

AR010 – Cloud-Prinzipien der Bundesverwaltung

Weisung zur Bundesinformatik mit weiteren Hinweisen

Klassifizierung:	nicht klassifiziert
Verbindlichkeit:[1]	Weisung mit weiteren Hinweisen und Empfehlungen
Vorgabentyp:[2]	(AR) Architektur
Planungsfeld:[3]	Bundesweite IKT-Grundleistungen
Diese Version:	1.0
Ersetzt Version:	ohne Vorversion
Status (diese Version):	Final
Beschlussdatum / Datum der Inkraftsetzung (diese Version):	Beschluss: Datum der digitalen Signatur Inkraftsetzung: 1.10.2023
Erlassen von, Rechtsgrundlage:	Delegierter für digitale Transformation und IKT-Lenkung (D-DTI), gestützt auf Artikel 17 Absatz 1 der Verordnung vom 25. November 2020 über die Koordination der digitalen Transformation und die IKT-Lenkung in der Bundesverwaltung (VDTI), SR 172.010.58
Sprachen:	Hauptdokument: Deutsch (Original), Französisch (Übersetzung)
Beilagen:	Keine

[1] Zur Erlassform und zur Verbindlichkeit vgl. *Bundesamt für Justiz: Gesetzgebungsleitfaden, 4. verbesserte Auflage, 2019*

[2] gemäss *BK IKT-Vorgaben*

[3] Planungsfelder gemäss *IKT-Strategie des Bundes 2020-2023 vom 3. April 2020 (SB000)*

Inhaltsverzeichnis

1 Allgemeine Bestimmungen

Die vom Bundesrat am 11. Dezember 2020 verabschiedete Cloud-Strategie der Bundesverwaltung [1] hat zum Ziel, den Weg zum Einsatz von Cloud-Diensten zu ebnen. Gemäss seiner Strategie nutzt der Bund Private- und Public-Cloud-Dienste **geordnet, sicher und effizient**.

Die Bundesverwaltung setzt gemäss ihrer Cloud-Strategie weiterhin auf eigene Rechenzentren und Leistungen aus bundeseigenen Private Clouds. Ergänzend dazu setzt sie Public-Cloud-Dienste mehrerer Anbieter ein. Diese **Hybrid-Multi-Cloud-Strategie** als Kombination von Private Clouds und Public Clouds ermöglicht die optimale Abdeckung von Anforderungen (z.B. im Bereich Informationssicherheit und Datenschutz, Resilienz, Innovationskraft, Funktionalität, Einsatzkritikalität und optimierter Fertigungstiefe).

Dieses Dokument beinhaltet

- drei neue Public-Cloud-relevante DTI-Weisungen (siehe Kapitel 4.1), sowie
- Hinweise auf Public-Cloud-relevante Regelungen anderer Stellen mit weiterführenden Informationen und DTI-Empfehlungen (siehe Kapitel 4.2)

für die Nutzung von Public-Cloud-Diensten in der Bundesverwaltung. Diese Cloud-Prinzipien streben eine Harmonisierung innerhalb der Bundesverwaltung an.

1.1 Gegenstand

1. Die Cloud-Prinzipien regeln den Umgang mit Public-Cloud-Diensten in der Bundesverwaltung auf Stufe Infrastructure as a Service (IaaS) und Platform as a Service (PaaS).
2. Die Cloud-Prinzipien richten sich an die Leistungserbringer (LE), Leistungsbezüger (LB) und deren Anwendungsverantwortliche gemäss Geltungsbereich.
3. Die Cloud-Prinzipien sind thematisch gruppiert und werden im vorliegenden Dokument in Kapitel 4 beschrieben (siehe Abbildung 1).

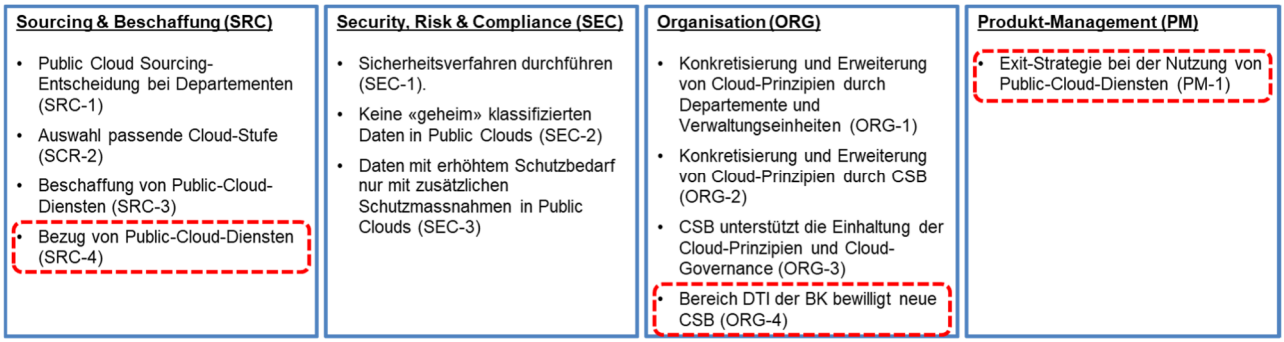

Abbildung 1: Übersicht Cloud-Prinzipien der Bundesverwaltung

Die rot umrandeten Prinzipien SRC-4, ORG-4, PM-1 sind in Kapitel 4.1 als DTI-Weisungen aufgeführt. Die weiteren Prinzipien sind als Hinweise auf relevante Regelungen anderer Stellen, weiterführende Informationen und Empfehlungen zu verstehen und werden in Kapitel 4.2 thematisch gruppiert erörtert.

1.2 Geltungsbereich

1. Der Geltungsbereich dieses Dokuments ist identisch mit dem Geltungsbereich der Verordnung über die digitale Transformation und die Informatik (VDTI), siehe Art. 2 VDTI [2].
2. Die Prinzipien SRC-4, ORG-4 und PM-1 sind als Weisungen des Bereichs DTI der BK verbindlich.

1.3 Ziel der Cloud-Prinzipien

Die Cloud-Prinzipien haben folgende Ziele:

1. Die Departemente und Verwaltungseinheiten nutzen Cloud-Dienste nach einheitlichen Prinzipien, soweit diese als Weisungen verbindlich sind.
2. Die Departemente und Verwaltungseinheiten erhalten eine Hilfestellung bei der Beurteilung, welche Cloud-Stufe für ihre Fachanwendung geeignet ist.
3. Die Cloud Service Broker (CSB) bauen auf einheitlichen Prinzipien auf.

Der Fokus des vorliegenden Dokuments liegt auf Governance-Themen. Es beantwortet folgende Fragen:

- Welche Abstufungen in Bezug auf Datenschutz und Informationssicherheit werden bei der Cloud-Nutzung in der Bundesverwaltung unterschieden (Kapitel 2)?
- Auf welchen Grundlagen bauen die Cloud-Prinzipien der Bundesverwaltung auf (Kapitel 3)?
- Welche bundesweiten Cloud-Prinzipien werden als verbindliche Weisung durch den Bereich digitale Transformation und IKT-Lenkung (DTI) der Bundeskanzlei (BK) vorgegeben (Kapitel 4)?

2 Cloud-Nutzung in der Bundesverwaltung anhand des Stufen-Modells

Wenn eine Verwaltungseinheit Private- und Public-Cloud-Dienste nutzen möchte, stehen ihr heute unterschiedliche Sourcing-Optionen zur Verfügung. Das Modell der Cloud-Stufen schafft ein gemeinsames Verständnis über diese Optionen. Es dient den Verwaltungseinheiten zudem als Unterstützung, um die jeweils richtige Cloud-Stufe auszuwählen.

Die verschiedenen Stufen in Abbildung 2 unterscheiden sich nicht nur in ihren Funktionalitäten, sondern auch in den Daten, die darin bearbeitet werden dürfen. Je höher die Stufenzahl, desto höher ist in der Regel die Schutzstufe der Daten.

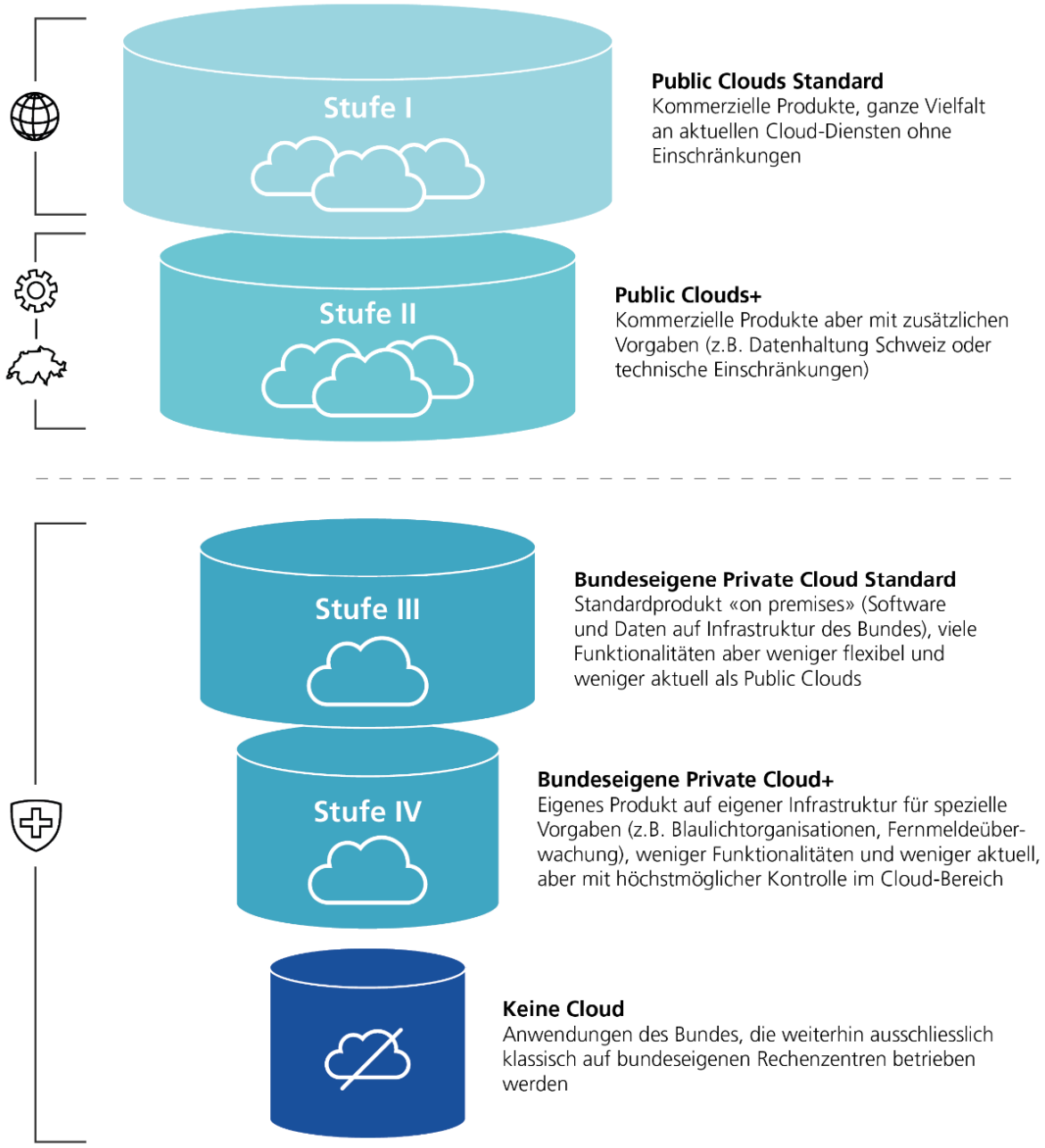

Abbildung 2: Darstellung Cloud-Nutzung in der Bundesverwaltung aus dem Bericht rechtlicher Rahmen für die Nutzung von Public-Cloud-Diensten in der Bundesverwaltung [3]

Wenn die Bundesverwaltung Private- und Public-Cloud-Dienste nutzt, spielen die digitale Souveränität sowie Informationssicherheit und Datenschutz eine zentrale Rolle. Daher müssen die Verwaltungseinheiten diese Themen mit äusserster Sorgfalt adressieren.

Die Bundesverwaltung klassifiziert ihre Informationen je nach Schutzbedarf als «intern», «vertraulich» oder «geheim» (siehe Art. 13 Informationssicherheitsgesetz [4]). Zusätzlich untersucht sie, ob die Informationen «Personendaten» oder sogar «besonders schützenswerte Personendaten» enthalten (siehe Datenschutzgesetz [5]) oder aus sonstigen Gründen (z.B. spezielle Gesetzgebung, Amtsgeheimnis) schützenswert sind.

Die folgende Tabelle gibt einen groben Überblick über die potenzielle Eignung der Cloud-Stufen aus Abbildung 2 für bestimmte Kategorien von Daten:

Cloud-Stufe	Datenhaltung	Klassifizierung	Datenschutz	Anforderungen an die staatliche Souveränität
I	weltweit	keine	Unkritische, anonyme und/oder öffentlichen Daten, die nicht datenschutzrelevant sind	Keine
II	z.B. EU / Schweiz	«intern»	Keine besonders schützenswerten Personendaten	Grundanforderungen
III	z.B. Swiss Government Cloud (3. Säule), BIT	«intern»	Keine besonders schützenswerten Personendaten	Erhöhte
IV	z.B. Secure Private Cloud, EJPD	«vertraulich»	Besonders schützenswerte Personendaten	Sehr hohe
	z.B. Neue Digitalisierungsplattform, VBS	«geheim»	Besonders schützenswerte Personendaten	Höchste
Keine Cloud	Umgebungen, die nicht auf Cloud-Technologien basieren. Auf dieser Stufe werden Anwendungen klassisch in den bundeseigenen Rechenzentren betrieben.			

Tabelle 1: Überblick über Cloud-Stufen

Die Aussagen zur potenziellen Eignung der verschiedenen Stufen für bestimmte Kategorien von Daten sind als grobe Orientierungshilfe zu verstehen. Abweichungen von den in Tabelle 1 beschriebenen Werten sind in beide Richtungen möglich, etwa wenn rechtliche Vorgaben den Einsatz einer bestimmten Cloud-Stufe verhindern oder wenn entsprechende kompensierende Massnahmen umgesetzt werden.

Für jede Anwendung prüft die zuständige Verwaltungseinheit im Rahmen der departementalen Vorgaben u.a. welche rechtlichen Vorgaben bestehen, wie der Schutzbedarf ist und welche Risiken vorliegen. Basierend auf diesen Prüfergebnissen entscheidet sie, welche Sourcing-Option bzw. Cloud-Stufe mit welchen vorzukehrenden Schutzmassnahmen zur Anwendung kommt.

Die Stufen sind nicht absolut trennscharf. Beispielsweise kann eine Fachanwendung als Hybrid-Cloud über mehrere Stufen verteilt betrieben werden, um besonders schützenswerte Personendaten in der Private Cloud zu bearbeiten und gleichzeitig für unkritische Daten

Cloud-Services in der Public Cloud zu nutzen. Hier ist hervorzuheben, dass solche komplexen Lösungen mit zusätzlichen Risiken verbunden sind, z.B. durch falsche Kategorisierung der Daten.

3 Cloud Governance und Grundsätze

Zwei Elemente bilden die Basis für die Cloud-Prinzipien der Bundesverwaltung:

1. Die Cloud Governance legt fest, wie der Bund die Nutzung der Cloud organisiert und steuert.
2. Die Grundsätze aus der Cloud-Strategie bilden die Basis für die Cloud-Prinzipien in Kapitel 4.

Die wichtigsten Grundlagen und Grundsätze aus der Cloud-Strategie der Bundesverwaltung [6] sind hier wiedergegeben. Sie wurden aktuellen Erkenntnissen angepasst.

3.1 Cloud Governance: organisatorisches Zusammenspiel

Um in der Bundesverwaltung eine geordnete, sichere und effiziente Nutzung von Public-Cloud-Diensten zu erreichen, sind vertragliche, organisatorische und technische Massnahmen notwendig. Abbildung 3 zeigt das angestrebte organisatorische Zusammenspiel.

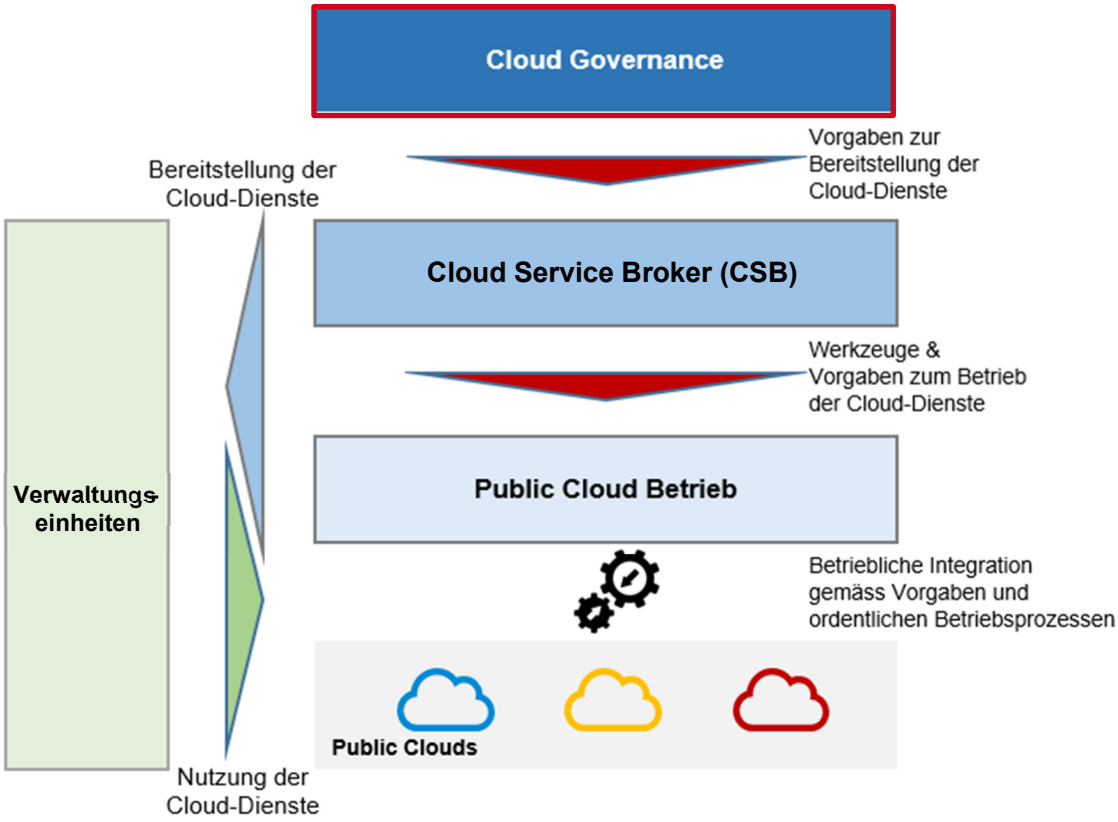

Abbildung 3: Cloud Governance Vorgaben zur Bereitstellung von Cloud-Diensten

Folgend sind die organisatorischen Fähigkeiten und Funktionen aus Abbildung 3 genauer

beschrieben:

- **Cloud Governance:** Der Bereich DTI der Bundeskanzlei definiert die Cloud-Prinzipien, welche bei der Nutzung von Public- und Private- Cloud-Diensten einzuhalten sind, und entscheidet gegebenenfalls auch über zu gewährende Ausnahmen. Er stellt zentral weitere Hilfsmittel zur Verfügung. Die Departemente, die BK und die CSB konkretisieren und erweitern die Governance für ihre jeweiligen Verantwortungsbereiche.
- **Cloud Service Broker (CSB):** Der CSB (in der Cloud-Strategie auch Intermediär genannt) unterstützt Verwaltungseinheiten beim geordneten, sicheren und effizienten Einsatz von Public-Cloud-Diensten. Er darf die Cloud-Prinzipien in seinem Zuständigkeitsbereich konkretisieren und/oder erweitern. Er berät bei der Wahl der richtigen Cloud-Stufe für Anwendungen. Ausserdem stellt er für Cloud-Projekte abgesicherte Umgebungen (sog. Landing Zones [7]) bereit, in denen Anwendungen aufgebaut und betrieben werden können. Der Bereich DTI der BK legt die Anforderungen an den CSB im CSB-Pflichtenheft in Absprache mit den Leistungserbringern fest.

  Die Rolle des vollumfänglichen CSB der Bundesverwaltung wird durch das Bundesamt für Informatik und Telekommunikation (BIT) wahrgenommen. Zusätzlich gibt es weitere dedizierte CSB, die spezifischen Bedürfnisse einzelner Departemente oder Bundesämter oder Fachgebiete abdecken (z.B. Swisstopo, MeteoSchweiz).
- **Public Cloud Betrieb:** Diese Funktion verantwortet betriebliche Leistungen im Rahmen der ordentlichen Betriebsprozesse für konkrete Fachanwendungen einer Verwaltungseinheit in der Public Cloud. Diese Aufgaben gehen über die reine Bereitstellung und den technischen Betrieb der Cloud-Dienste durch die Public-Cloud-Anbieter hinaus.

  Die zuständigen Verwaltungseinheiten sind verantwortlich für die vertragliche, bundeskonforme Bereitstellung des Betriebs durch interne Leistungserbringer oder externe Anbieter.
- **Public Clouds**: Diese Funktion verantwortet den Betrieb der Cloud-Dienste. Die Rolle wird von den Public-Cloud-Anbietern sichergestellt.

3.2 Grundsätze

Die strategischen Grundsätze bilden die Basis für die Cloud-Prinzipien in Kapitel 4. Sie stammen aus der Cloud-Strategie der Bundesverwaltung [2] und wurden punktuell ergänzt.

Grundsatz S-1: Strategische Sourcing-Optionen

Der Bundesverwaltung stehen verschiedene Sourcing-Optionen zur Verfügung: Bei der Verarbeitung und Speicherung von Daten sowie dem Betrieb von Anwendungen stehen die Public Clouds der grossen internationalen oder lokalen Schweizer Anbieter, Community-Clouds, die bundesinternen Private Clouds, die bundeseigenen Rechenzentren und die Rechenzentren herkömmlicher Outsourcing-Partner (Bezug Managed Service, Auslagerung von Betriebsleistungen, usw.) als Sourcing-Optionen zur Auswahl.

Grundsatz S-2: Die strategischen Sourcing-Optionen ergänzen sich – auch langfristig

Es bestehen heute und auch künftig Anwendungen und Daten, welche aus unterschiedlichen Gründen (z.B. rechtliche Vorgaben, digitale Souveränität) auf bundesinternen Infrastrukturen/ Plattformen in den Rechenzentren der Bundesverwaltung betrieben, respektive bearbeitet werden müssen.

Durch die Nutzung von Public Clouds sollen die Verwaltungseinheiten der Bundesverwaltung effizient und zeitnah auf innovative Lösungen sowie neueste Technologien der Public-Cloud-Anbieter zugreifen können, sofern keine Gründe dagegensprechen (z.B. rechtliche Anforderungen, Schutzbedarf der Daten oder Bedenken zum Datensouveranität).

Grundsatz S-3: Die Wahl der Sourcing-Option verbleibt abgesehen von den Standarddiensten bei den jeweiligen Departementen, den verselbstständigten Verwaltungseinheiten und der Bundeskanzlei

Über Anträge der Leistungsbezüger/Verwaltungseinheiten bezüglich des Einsatzes einer Sourcing-Option für Anwendungen/Daten entscheiden nach Rücksprache mit den betroffenen Leistungserbringern dezentral jeweils die Departemente, die verselbstständigten Verwaltungseinheiten oder die BK selbständig.

Grundsatz O-1: Cloud Governance erfolgt durch gemeinsame Prinzipien

Für eine geordnete, sichere und effiziente Nutzung von Public-Cloud-Diensten werden durch den Bereich DTI der BK die vorliegenden Cloud-Prinzipien erlassen.

Die Departemente und die Verwaltungseinheiten dürfen die Cloud-Prinzipien und Empfehlungen des Bereichs DTI der BK in ihrem Zuständigkeitsbereich konkretisieren und/oder erweitern.

Grundsatz D-1: Datenverarbeitung in Public Clouds schrittweise angehen

Auch wenn der rechtliche Rahmen heute unter Umständen mehr zulässt (siehe Bericht Rechtlicher Rahmen für die Nutzung von Public-Cloud-Diensten in der Bundesverwaltung [3]), wird den Verwaltungseinheiten empfohlen, ihren Gang in die Cloud in einem ersten Schritt mit möglichst wenigen und maximal «intern» klassifizierten Informationen bzw. nicht besonders schützenswerten Personendaten zu beschreiten.

Höher klassifizierte Informationen, Personendaten oder Daten, die aus sonstigen Gründen schützenswert sind (z.B. aufgrund spezialgesetzlicher Grundlage), können in Public Clouds bearbeitet werden, sofern das geltende Recht eingehalten wird, die entsprechenden Schutzkonzepte bestehen und die im Einzelfall definierten Massnahmen umgesetzt werden. Die Generalsekretärenkonferenz (GSK) sowie der Delegierte des Bundes für Cybersicherheit und der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftrage (EDÖB) sind entsprechend zu informieren.

Die Verwaltungseinheiten sind verantwortlich, für ihre Anwendungen und Daten eine Prüfung der Rechtskonformität (inklusive Datenschutz und allfälliger Geheimhaltungspflichten, wie z.B. das Amtsgeheimnis) sowie die entsprechenden Sicherheitsverfahren durchzuführen (siehe [3]).

4 Cloud-Prinzipien der Bundesverwaltung

In diesem Kapitel werden die bundesweiten Cloud-Prinzipien beschrieben. Für eine bessere Übersichtlichkeit sind die Prinzipien in Abbildung 4 in Kategorien strukturiert. Zu den hell schattierten Kategorien sind aktuell noch keine bundesweiten Cloud-Prinzipien definiert.

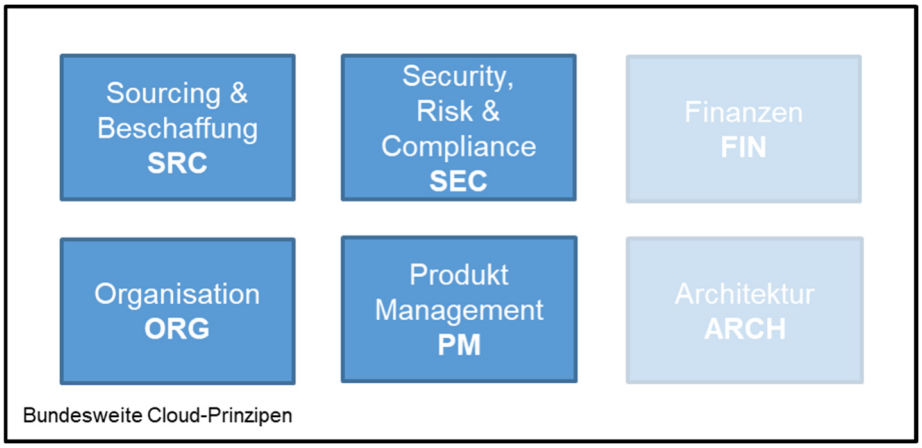

Abbildung 4: Kategorisierung Cloud-Prinzipien

Die bundesweiten Cloud-Prinzipien werden zentral durch den Bereich DTI der Bundeskanzlei erarbeitet und verwaltet. In Kapitel 4.1 werden die rechtlich verbindlichen Weisungen behandelt. Die weiteren Prinzipien sind als Hinweise auf Cloud-relevante Regelungen anderer Stellen, weiterführenden Informationen und Empfehlungen zu verstehen und werden in Kapitel 4.2 thematisch gruppiert erörtert.

Zu jeder Kategorie können die Departemente und Verwaltungseinheiten oder CSBs bei Bedarf für sie weiterführende, spezifische Cloud-Prinzipien definieren. Diese sind nicht Teil des vorliegenden Dokuments.

Weitergehende Vorgaben, welche nur die CSB betreffen, sind im CSB-Pflichtenheft [8] als Aufgaben, Kompetenzen und Verantwortlichkeiten beschrieben.

4.1 Rechtlich verbindliche Weisungen

Die in diesem Kapitel aufgeführten Prinzipien stellen rechtlich verbindliche Weisungen dar.

4.1.1 Sourcing & Beschaffung (SRC)

ID	Name	Verbindlich-keitsgrad[4]	Bezug zu Grundsatz aus Cloud-Strategie
SRC-4	**WEISUNG: Bezug von Public-Cloud-Diens-ten**	**MUSS**	**S-1, O-1**
Bestimmung Jede Verwaltungseinheit MUSS ihre Public-Cloud-Dienste für Infrastructure as a Service (IaaS) und Platform as a Service (PaaS) über einen CSB ihrer Wahl beziehen. Ausgenommen von diesem Prinzip sind Software as a Service (SaaS), ERP-Angebote und Büroautomation.			
Erläuterungen Durch dieses Prinzip werden die Bezüge kanalisiert und die Leistungsbezüger erhalten Unterstützung in der Einhaltung der Governance. Dieses Prinzip hilft, den Bezug für die Verwaltungseinheiten geordnet und effizient zu gestalten, und möglichst viele Schritte auf CSB-Seite zu automatisieren.			
Bezug zu Cloud-Stufen Stufe I, II			
Weiterführende Informationen Definitionen IaaS, PaaS, SaaS [9]: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecial-publication800-145.pdf			

[4] Zur Bedeutung der Schlüsselwörter zur Bestimmung des Verbindlichkeitsgrade siehe Anhang B.

4.1.2 Organisation (ORG)

ID	Name	Verbindlich-keitsgrad	Bezug zu Grundsatz aus Cloud-Strategie
ORG-4	**WEISUNG: Bereich DTI der BK bewilligt neue CSBs**	**MUSS**	**O-1**

Bestimmung

Möchte eine Verwaltungseinheit die CSB Funktion übernehmen, MUSS sie einen Antrag mit einer Begründung beim Bereich DTI der BK stellen. Dieser prüft die Gründe und die Erfüllung der Anforderungen aus dem CSB-Pflichtenheft. Gegebenenfalls bewilligt der Bereich DTI der BK den Antrag.

Erläuterungen

Der Grundsatz O-1 sieht vor, dass neben dem CSB der Bundesverwaltung weitere CSBs möglich sind. Um CSB zu werden, müssen gewisse Anforderungen durch die Verwaltungseinheit erfüllt werden. Diese sind im sogenannten CSB-Pflichtenheft definiert [8]. Darin wird zwischen einem CSB der Bundesverwaltung und dedizierter CSB unterschieden; an sie werden unterschiedliche Anforderungen gestellt. Wenn diese Anforderungen erfüllt sind und gute Gründe für die Übernahme der CSB-Funktion durch die Verwaltungseinheit gegeben sind, bewilligt der Bereich DTI der BK den Antrag in Form eines D-DTI Beschlusses nach Anhörung des DRB.

Bezug zu Cloud-Stufen

Stufe I, II

Weiterführende Informationen

CSB-Pflichtenheft mit Aufgaben, Kompetenzen und Verantwortlichkeiten eines CSB siehe [8]

4.1.3 Produkt-Management (PM)

ID	Name	Verbindlich-keitsgrad	Bezug zu Grundsatz aus Cloud-Strategie
PM-1	**WEISUNG: Exit-Strategie bei der Nutzung von Public-Cloud-Diensten**	**MUSS**	**-**

Bestimmung

Damit Abhängigkeiten von Cloud-Anbietern bewusst und kontrolliert eingegangen werden, MUSS die zuständige Verwaltungseinheit mit Unterstützung durch den verantwortlichen CSB pro Vorhaben (oder pro Anwendungsgruppe) eine Exit-Strategie definieren. Diese beschreibt, wie eine Software-Lösung in nützlicher Frist auf eine andere Plattform, ein Service oder eine Technologie überführt werden kann. Die Exit-Strategie MUSS bei Erweiterungen der Anwendung aktualisiert werden.

Erläuterungen

Bei der Nutzung von Public-Cloud-Diensten entstehen Abhängigkeiten vom Cloud-Anbieter oder gewissen Technologien (sog. Lock-in).

Dieses Prinzip soll das Bewusstsein schärfen, dass schon bei der Konzeption einer Software-Lösung bzw. vor Beginn der Nutzung von Cloud-Diensten an mögliche Abhängigkeiten und Cloud-Lock-ins gedacht wird. So können frühzeitig ungewollte Abhängigkeiten antizipiert und wo möglich abgefedert werden.

Je nach Kontext kann es sinnvoll sein, eine gemeinsame Exit-Strategie für eine Gruppe von Anwendungen (z.B. alle Anwendungen einer Verwaltungseinheit, die beim gleichen Cloud-Anbieter laufen) zu formulieren.

Zu bemerken ist, dass Abhängigkeiten zu Providern oder Technologien auch bei Private Cloud Umgebungen und auch ausserhalb der Cloud entstehen können.

Bezug zu Cloud-Stufen

Stufe I, II

Weiterführende Informationen

Keine

4.2 Empfehlungen und Hinweise auf weitere Regelungen

In diesem Kapitel werden zum einen Empfehlungen aufgeführt und zum anderen Prinzipen, die ihren Ursprung an anderer Stelle haben, wiedergegeben und ihre Anwendbarkeit auf den Cloud-Kontext mittels Hinweise und weiterführende Informationen erklärt.

4.2.1 Sourcing & Beschaffung (SRC)

ID	Name	Bezug zu Grundsatz aus Cloud-Strategie
SRC-1	**Public Cloud Sourcing-Entscheidung bei Departementen und BK**	**S-1**
Bestimmungen Der Entscheid über den Einsatz von Public-Cloud-Diensten liegt in der Hoheit der Departemente, der BK oder der verselbstständigten Verwaltungseinheiten. Dieser Sourcing-Entscheid erfolgt unter Berücksichtigung der IKT-Sourcing-Strategie des Bundes [10], den Vorgaben und Standards des Bundes zur Sicherstellung der Interoperabilität, der Unternehmensarchitektur der Verwaltungseinheit sowie basierend auf einer Risikobeurteilung und Prüfung der Rechtskonformität.		
Erläuterungen Analog zur Entscheidungsbefugnis in anderen Sourcing-Bereichen hält dieses Prinzip die Entscheidungsbefugnis im Bereich der Public-Cloud-Dienste fest (Auswahl der geeigneten Cloud-Stufe). Die Befugnisse entsprechen den Grundsätzen, die in Art. 8 VDTI [2] definiert sind. Bei der Rechtskonformität wird insbesondere auf Datenschutz, Informationssicherheit und allfällige Geheimhaltungspflichten geachtet.		
Bezug zu Cloud-Stufen Alle Stufen		
Weiterführende Informationen Art. 8 VDTI: Entscheid über den Leistungsbezug und Art. 18 VDTI: Weisungen der Bundeskanzlerin oder des Bundeskanzlers über Standarddienste mit Bezugszwang [2]: https://www.fedlex.admin.ch/eli/cc/2020/988/de IKT-Sourcing-Strategie des Bundes [10]: https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/ikt-vorgaben/strategien-teilstrategien/sb017-ikt-strategie_sourcing.html IKT-Vorgaben des Bundes [11]: https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/ikt-vorgaben/alle-ikt-vorgaben.html		

ID	Name	Bezug zu Grundsatz aus Cloud-Strategie
SRC-2	**Vorabklärung bezüglich passender Cloud-Stufe**	**S-2, D-1**

Bestimmung

Vor der Beschaffung resp. vor dem Abruf bzw. dem produktiven Einsatz von Public-Cloud-Diensten muss die Rechtskonformität geprüft (Rechtsgrundlagenanalyse) und eine Schutzbedarfs- sowie gegebenenfalls eine Risikoanalyse erstellt werden. Bei Personendaten ist gegebenenfalls auch eine Datenschutz-Folgenabschätzung durchzuführen.

Basierend auf den Erkenntnissen aus den Überprüfungen und Analysen wird durch die Verwaltungseinheit bzw. deren Departement entschieden, ob die Sourcing-Option Public Cloud (Stufe I und II) oder die bundeseigene Private Cloud (Stufe III und IV) oder gar keine Cloud-Lösung in Frage kommt (siehe Kapitel 2). Die Verantwortung liegt bei der jeweiligen Verwaltungseinheit bzw. deren Departement.

Falls höher klassifizierte Informationen, Personendaten oder Daten, die aus sonstigen Gründen schützenswert sind (z.B. aufgrund spezialgesetzlicher Grundlage) in die Public Clouds bearbeitet werden, muss die Generalsekretärenkonferenz (GSK) sowie der Delegierte des Bundes für Cybersicherheit und der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftrage (EDÖB) vorgängig informiert werden.

Erläuterungen

Dieses Prinzip beschreibt den Entscheidungsprozess bezüglich Auswahl der passenden Sourcing-Option: Public oder Private Cloud und der passenden Cloud-Stufe. Die Analysen betreffend die Cybersicherheit basieren auf den Vorgaben des Nationalen Cyber Security Center (NCSC) [12].

Für weitere Details zur Anwendung der Sicherheitsverfahren siehe Prinzip SEC-1.

Bezug zu Cloud-Stufen

Alle Stufen

Weiterführende Informationen

Bericht Rechtlicher Rahmen für die Nutzung von Cloud-Diensten in der Bundesverwaltung [3]: https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html

NCSC Sicherheitsverfahren [12]: https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren.html

Projektvorgehensmethodik HERMES [13]: https://www.hermes.admin.ch/

ID	Name	Bezug zu Grundsatz aus Cloud-Strategie
SRC-3	**Beschaffung von Public-Cloud-Diensten**	**S-1, S-2, S-3**

Bestimmung

Jede Verwaltungseinheit soll ihre Public-Cloud-Dienste für Infrastructure as a Service (IaaS) und Platform as a Service (PaaS) über die WTO 20007 abrufen.

Ausgenommen von diesem Prinzip sind Software as a Service (SaaS), ERP-Angebote und der Standarddienst Büroautomation. Ebenfalls ausgenommen sind Angebote von Drittfirmen auf den Marktplätzen der Public-Cloud-Anbieter.

Die vergaberechtlichen Grundsätze müssen stets eingehalten werden.

Erläuterungen

Die Schaffung einer anderen beschaffungsrechtlichen Grundlage ist dann vorzusehen, wenn der Leistungsgegenstand nicht von der WTO 20007 erfasst ist bzw. die Zuschlagsempfänger die nachgefragten Leistungen nicht gestützt auf diese WTO-Ausschreibung erbringen können.

Neben SaaS, ERP-Angeboten und Büroautomation sind auch Angebote von Drittfirmen (d.h. Unternehmen, die nicht zu den Zuschlagsempfängern der WTO gehören) im Marketplace der Zuschlagsempfänger nicht im Leistungsumfang der WTO 20007.

Bezug zu Cloud-Stufen

Stufe I, II

Weiterführende Informationen

Definitionen IaaS, PaaS, SaaS [9]: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Bundesgesetz über das öffentliche Beschaffungswesen (BöB) SR 172.056.1 [14]: https://www.fedlex.admin.ch/eli/cc/2020/126/de

Verordnung über das öffentliche Beschaffungswesen (VöB) (SR 172.056.11) [15]: https://www.fedlex.admin.ch/eli/cc/2020/127/de

4.2.2 Security, Risk & Compliance (SEC)

ID	Name	Bezug zu Grundsatz aus Cloud-Strategie
SEC-1	**Sicherheitsverfahren durchführen**	**D-1**

Bestimmung

Die Departemente und die Verwaltungseinheiten sind verantwortlich, für ihre Anwendungen und Daten eine Prüfung der Rechtskonformität (inklusive Datenschutz und allfälliger Geheimhaltungspflichten) sowie die entsprechenden Sicherheitsverfahren durchzuführen.

Vor der Beschaffung/ dem Abruf bzw. dem produktiven Einsatz von Public-Cloud-Diensten muss eine Schutzbedarfsanalyse (SCHUBAN) durchgeführt werden.

Ergibt die Schutzbedarfsanalyse einen erhöhten Schutzbedarf, so ist zusätzlich zur Dokumentation der Umsetzung des IT-Grundschutzes ein Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) mit Risikoanalyse zu erstellen.

Bei jedem Entscheid über die Auslagerung von Personendaten in eine Cloud und bei der Ausgestaltung dieser Bearbeitung ist der Datenschutzberater oder die Datenschutzberaterin der Verwaltungseinheit beizuziehen (Art. 26 Abs. 2 Bst. a DSV).

Die Verwaltungseinheit muss eine Datenschutz-Folgenabschätzung durchführen, sofern eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann. Es ist der Leitfaden des EDÖB zu den technischen und organisatorischen Massnahmen des Datenschutzes [16] zu konsultieren und gegebenenfalls eine Datenschutzfolgenabschätzung (DSFA) durchzuführen.

Erläuterungen

Die Vorgaben des Nationalen Zentrums für Cyber-Sicherheit (NCSC) zum Sicherheitsverfahren [12] sind auch für potentielle Public-Cloud-Projekte anzuwenden.

Dieses Prinzip bezieht sich auf die etablierten Prozesse SCHUBAN und ISDS-Konzept und stellt die Konformität bei Software-Lösungen hinsichtlich Informationssicherheit sicher. Diese Prozesse decken Risikoanalyse und Risikomanagement ab.

Die Prüfung der Rechtskonformität wird unterstützt durch den Bericht zum rechtlichen Rahmen der Nutzung von Cloud-Diensten in der Bundesverwaltung [3] und die entsprechende Checkliste [17].

Bezug zu Cloud-Stufen

Alle Stufen

Weiterführende Informationen

Informationsseite zur Cloud in der Bundesverwaltung [17]: https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html

Bericht Rechtlicher Rahmen für die Nutzung von Cloud-Diensten in der Bundesverwaltung [3]: https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html

NCSC Sicherheitsverfahren [12]: https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren.html

Projektvorgehensmethodik HERMES [13]: https://www.hermes.admin.ch/

EDÖB Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes [16]: https://www.edoeb.admin.ch/dam/edoeb/de/Dokumente/aDSG/guide-TOM_de.pdf.download.pdf/guideTOM_de.pdf

Richtlinien des Bundesrates für die Risikovorprüfung und die Datenschutz-Folgenabschätzung bei Datenbearbeitungen durch die Bundesverwaltung (BBl 2023 1882) [18]: https://www.fedlex.admin.ch/eli/fga/2023/1882/de

Instrument für die Risikovorprüfung und DSFA-Leitfaden [19]: https://www.bj.admin.ch/bj/de/home/staat/datenschutz/info-bundesbehoerden.html

ID	Name	Bezug zu Grundsatz aus Cloud-Strategie
SEC-2	**Keine «geheim» klassifizierten Daten in Public Clouds**	**D-1**

Bestimmung

Als «geheim» klassifizierte Daten dürfen nicht in Public Clouds (Stufe 1 und 2) sowie der Private Cloud Stufe 3 gespeichert oder bearbeitet werden.

Erläuterungen

Die Verwaltungseinheit stellt sicher, dass «geheim» klassifizierte Daten unter der alleinigen Kontrolle der Bundesverwaltung bleiben.

Bezug zu Cloud-Stufen

Stufe I, II, III

Weiterführende Informationen

Bericht Rechtlicher Rahmen für die Nutzung von Cloud-Diensten in der Bundesverwaltung [3]: https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html

Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) [4]: https://www.fedlex.admin.ch/eli/fga/2020/2696/de

Verordnung über die Informationssicherheit bei der Bundesverwaltung und bei der Armee (Informationssicherheitsverordnung, ISV) [20]

ID	Name	Bezug zu Grundsatz aus Cloud-Strategie
SEC-3	**Daten mit erhöhtem Schutzbedarf nur mit zusätzlichen Schutzmassnahmen in Public Clouds**	**D-1**

Bestimmung

Als Voraussetzung für die Bearbeitung und Speicherung in der Public Cloud von «intern» oder «vertraulich» klassifizierten Informationen, sowie Daten, die Geheimhaltungspflichten unterliegen, müssen angemessene vertragliche, organisatorische und technische Schutzmassnahmen die Einhaltung des anwendbaren Rechts sicherstellen.

Dies gilt auch bei Personendaten oder besonders schützenswerten Personendaten, wenn die Abklärungen ein Risiko für die Persönlichkeit der betroffenen Personen ergeben. Besteht ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen, muss nach Artikel 22 Absatz 1 des revidierten Datenschutzgesetzes eine Datenschutz-Folgenabschätzung durchgeführt werden (siehe SEC-1).

Wenn durch den Umfang der Auslagerung oder die Natur der ausgelagerten Daten hohe Risiken für die staatliche Souveränität entstehen, muss geprüft werden, ob angemessene Massnahmen die Bearbeitung in der Public Cloud erlauben.

Erläuterungen

In der Schutzbedarfsanalyse wird geklärt, ob eine Anwendung klassifizierte Daten oder Personendaten beinhaltet oder generiert.

Sofern im Einzelfall beurteilte und angebrachte vertragliche, organisatorische und technische Schutzmassnahmen die Einhaltung des geltenden Rechts erlauben, können auch Daten, die einen erhöhten Schutzbedarf nach Informationsschutz aufweisen oder datenschutzrechtlich geschützt sind, in einer Public Cloud gespeichert und verarbeitet werden.

Ob die vorgesehenen Schutzmassnahmen ausreichen, wird im Rahmen der NCSC Sicherheitsverfahren [12] und/oder einer Datenschutz-Folgenabschätzung geprüft.

Technische Schutzmassnahmen heute sind z.B. Verschlüsselung bei Speicherung, Verschlüsselung bei Transit, Verwendung von eigenen Schlüsseln (bring your own key, hold your own key), Einsatz von Confidential Computing usw.

Eine Massnahme im Bereich der digitalen Souveränität kann z.B. eine redundante Datenhaltung (Public Cloud und in einem Rechenzentrum der Bundesverwaltung) zur Sicherstellung der Verfügbarkeit sein.

Solche Massnahmen sollten mit dem zuständigen Departement abgestimmt sein.

Bezug zu Cloud-Stufen

Stufe I, II

Weiterführende Informationen
Bericht Rechtlicher Rahmen für die Nutzung von Cloud-Diensten in der Bundesverwaltung [3]: Cloud (admin.ch) NCSC Sicherheitsverfahren [12]: https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren.html EDÖB Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes [16]: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/leitfaeden/technische-und-organisatorische-massnahmen-des-datenschutzes.html

4.2.3 Organisation (ORG)

ID	Name	Bezug zu Grundsatz aus Cloud-Strategie
ORG-1	**Konkretisierung und Erweiterung von Cloud-Prinzipien durch Departemente und Verwaltungseinheiten**	**O-1**
Bestimmung Die Cloud-Prinzipien der Bundesverwaltung sind für die gesamte Bundesverwaltung gültig. Die Departemente und Verwaltungseinheiten dürfen die Cloud-Prinzipien in ihrem Zuständigkeitsbereich im Rahmen der bestehenden gesetzlichen Vorgaben konkretisieren und/oder erweitern.		
Erläuterungen Dieses Prinzip gibt den Departementen und Verwaltungseinheiten die Freiheit, die allgemeingültigen Cloud-Prinzipien auf ihre Gegebenheiten anzupassen. So können z.B. Prinzipien verschärft, präzisiert oder erweitert bzw. neue Prinzipien hinzugefügt werden.		
Bezug zu Cloud-Stufen alle Stufen		
Weiterführende Informationen Regierungs- und Verwaltungsorganisationsgesetz (RVOG) [21]: https://www.fedlex.admin.ch/eli/cc/1997/2022_2022_2022/de Verordnung über die Koordination der digitalen Transformation und die IKT-Lenkung in der Bundesverwaltung (VDTI) [2]: https://www.fedlex.admin.ch/eli/cc/2020/988/de		

ID	Name	Bezug zu Grundsatz aus Cloud-Strategie
ORG-2	**Konkretisierung und Erweiterung von Cloud-Prinzipien durch CSB**	**O-1**
Bestimmung Die CSB dürfen die Cloud-Prinzipien in ihrem Zuständigkeitsbereich konkretisieren und/oder erweitern. Die Kunden können bei Anpassungen von Cloud-Prinzipien über den verantwortlichen CSB Einfluss nehmen. Diese Anpassungen gelten nur für die Kunden des jeweiligen CSB.		
Erläuterungen Dieses Prinzip gibt den CSB die Freiheit die allgemeingültigen Cloud-Prinzipien auf ihre Gegebenheiten anzupassen. So können z.B. Prinzipien verschärft, präzisiert oder erweitert bzw. neue Prinzipien hinzugefügt werden.		
Bezug zu Cloud-Stufen Stufe I, II		
Weiterführende Informationen Regierungs- und Verwaltungsorganisationsgesetz (RVOG) [21]: https://www.fedlex.admin.ch/eli/cc/1997/2022_2022_2022/de Verordnung über die Koordination der digitalen Transformation und die IKT-Lenkung in der Bundesverwaltung (VDTI) [2]: https://www.fedlex.admin.ch/eli/cc/2020/988/de		

ID	Name	Bezug zu Grundsatz aus Cloud-Strategie
ORG-3	**CSB unterstützt die Einhaltung der Cloud-Prinzipien und Cloud-Governance**	**O-1**
Bestimmung Ein CSB soll seine Kunden bei der Ausübung ihrer Tätigkeiten bezüglich der Einhaltung der Cloud-Prinzipien und der definierten Cloud-Governance unterstützen.		
Erläuterungen Dieses Prinzip formuliert eine der Aufgaben eines CSB: Er unterstützt die Departemente und Verwaltungseinheiten bei der Einhaltung der Cloud-Prinzipien und Governance-Vorgaben. Die Verantwortung für die Einhaltung liegt jedoch bei der jeweiligen Verwaltungseinheit.		
Bezug zu Cloud-Stufen Stufe I, II		
Weiterführende Informationen CSB-Pflichtenheft mit Aufgaben, Kompetenzen und Verantwortlichkeiten eines CSB siehe [8]		

5 Schlussbestimmungen

5.1 Übergangsbestimmungen zu den Weisungen SRC-4, ORG-4 und PM-1

Anwendungen, die vor Inkrafttreten der vorliegenden Weisung realisiert wurden, dürfen unverändert weiterlaufen. Bei der nächsten Erneuerung oder erweiterten Funktionsnutzung der Anwendung, müssen die Weisungen geprüft und deren Erfüllung initialisiert werden.

5.2 Einhaltung der Weisungen SRC-4, ORG-4 und PM-1

Die Departemente und die Bundeskanzlei sorgen gemäss Artikel 3 VDTI in ihrem Zuständigkeitsbereich für die Umsetzung der Weisungen.

5.3 Überprüfung

Der Bereich DTI der BK überprüft die Aktualität und Zweckmässigkeit der Cloud-Prinzipien regelmässig, spätestens vier Jahre nach deren Inkraftsetzung.

5.4 Inkrafttreten der Weisungen SRC-4, ORG-4 und PM-1

Die Weisungen treten per 1.10.2023 in Kraft.

Anhänge

A. Änderungen gegenüber Vorversion

Version	Beschreibung	Änderung am/durch
0.1 – 0.8	Initiale Version basierend auf Cloud-Strategie Arbeitsdokument, Erarbeitung Inhalte	05.09.2022: 13.09.2022 D. Albisser, E. Dubach, S. Hüsemann
0.92	Einarbeitung Feedback E. Dubach, Markwalder, Stephan Brunner	15.09.2022: S. Hüsemann, D. Albisser
0.93	Einarbeitung Befunde aus Konsultation	11.10.2022: S. Hüsemann, D. Albisser
0.94	Finalisierung Formulierungen nach Konsultation	01.11.2022: S. Hüsemann, D. Albisser, R. Lichtsteiner, E. Dubach
0.95	Feedback aus Review Daniel Markwalder eingearbeitet	08.11.2022: S. Hüsemann
0.96	Einarbeitung Befunde aus 2. Ämter-Feedback-Runde	25.11.2022: S. Hüsemann, R. Lichtsteiner, E. Dubach
0.98	Anpassung Dokument zur Architekturvorgabe Umstrukturierung der Kapitel, textuelle Überarbeitung, Einarbeitung Feedback DTI T&I	24.01.2023: S. Hüsemann, E. Dubach, R. Lichtsteiner, S. Meyer, A. Spichiger
0.99	Einarbeitung Befunde BK-interne Konsultation	02.02.2023: S. Hüsemann, E. Dubach, R. Lichtsteiner
1.0	Einarbeitung Befunde Ämterkonsultation und Bereinigungsrunde	22.09.2023: N. Gammenthaler, S. Hüsemann, E. Dubach

B. Bedeutung der Schlüsselwörter zur Bestimmung des Verbindlichkeitsgrades

Der Verbindlichkeitsgrad[5] der einzelnen Bestimmungen in dieser Weisung wird mittels folgender Schlüsselwörter in Grossbuchstaben gekennzeichnet:

Schlüsselwort	Verbindlichkeitsgrad
MUSS	Vorgabe, die einzuhalten ist (gewährte Ausnahmen ausgenommen)
DARF NICHT	Option, die nicht gewählt werden darf
DARF	Die Option ist explizit erlaubt. Die Nutzer entscheiden, ob sie die Option nutzen möchten. Betrifft die Vorgabe eine IKT-Lösung, muss der Anbieter der Lösung die Option anbieten.

[5] Verbindlichkeitsgrade gemäss *Request of Comments: RFC 2119 (PCB 14), The Internet Engineering Task Force (IETF).* Die Angabe von Verbindlichkeitsgraden gemäss [RFC 2119] ist eine verbreitete Praxis in der internationalen Standardisierung.

SOLL	Option, die im Normalfall zu wählen ist. Es kann jedoch ohne Ausnahmegewährung des Bereich DTI bzw. des NCSC davon abgewichen werden, insbesondere wenn die Wirtschaftlichkeit oder Sicherheit andernfalls nicht mehr gewährleistet werden können. Die Abweichung von der Vorgabe ist jedoch schriftlich zu begründen.
KANN	Akzeptierte Option. Betrifft die Vorgabe eine Lösung, entscheidet der Anbieter der Lösung darüber, ob er die Option unterstützen will.

C. Referenzen

[1] Bundeskanzlei, Digitale Transformation und IKT Steuerung (DTI), Cloud-Strategie der Bundesverwaltung, 2020; https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/ikt-vorgaben/strategien-teilstrategien/sb020-cloud-strategie_der_bundesverwaltung.html.

[2] Der Schweizerische Bundesrat, Verordnung über die digitale Transformation und die Informatik (VDTI), SR 172.010.58, 2020, https://www.fedlex.admin.ch/eli/cc/2020/988/de.

[3] Bundeskanzlei, Bericht Rechtlicher Rahmen für die Nutzung von Public-Cloud-Diensten in der Bundesverwaltung, 2022, https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html.

[4] Die Bundesversammlung der Schweizerischen Eidgenossenschaft, Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG), 2020, https://www.fedlex.admin.ch/eli/fga/2020/2696/de.

[5] Die Bundesversammlung der Schweizerischen Eidgenossenschaft, Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG), 2020, https://www.fedlex.admin.ch/eli/cc/2022/491/de.

[6] Der Schweizerische Bundesrat, Verordnung über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV), 2007, https://www.fedlex.admin.ch/eli/cc/2007/414/de.

[7] IT-Business, Was ist eine Landing Zone?, 2022, https://www.it-business.de/was-ist-eine-landing-zone-a-0c951fabad3e2dcc1bf4e7cd50d2d2f5/#:~:text=Eine%20Landing%20Zone%20ist%20eine,sich%20nach%20den%20jeweiligen%20Firmenbed%C3%BCrfnissen.&text=Unternehmen%20stellen%20Apps%20immer%20h%C3%A4ufiger%20%C3%B [Zugriff am 28 7 2023].

[8] Bundeskanzlei, CSB-Pflichtenheft [in Arbeit].

[9] National Institute of Standards and Technology (NIST), The NIST Definition of Cloud Computing, 2011, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

[10] Bundeskanzlei, IKT-Sourcing-Strategie des Bundes 2018–2023, 2018, https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/ikt-

vorgaben/strategien-teilstrategien/sb017-ikt-strategie_sourcing.html.

[11] Bundeskanzlei, IKT-Vorgaben, https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/ikt-vorgaben/alle-ikt-vorgaben.html.

[12] Nationales Zentrum für Cybersicherheit (NCSC), Sicherheitsverfahren, 2022, https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren.html.

[13] Bundeskanzlei, HERMES Projektmanagement 5.1 Methodik, https://www.hermes.admin.ch/.

[14] Die Bundesversammlung der Schweizerischen Eidgenossenschaft, Bundesgesetz über das öffentliche Beschaffungswesen (BöB) (SR 172.056.1), 2019, https://www.fedlex.admin.ch/eli/cc/2020/126/de.

[15] Der Schweizerische Bundesrat, Verordnung über das öffentliche Beschaffungswesen (VöB) (SR 172.056.11), 2020, https://www.fedlex.admin.ch/eli/cc/2020/127/de.

[16] Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), Technische und organisatorische Massnahmen des Datenschutzes, 2015, https://www.edoeb.admin.ch/dam/edoeb/de/Dokumente/aDSG/guideTOM_de.pdf.download.pdf/guideTOM_de.pdf.

[17] Bundeskanzlei, Digitale Transformation und IKT Steuerung (DTI), Cloud, 2022, https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html.

[18] Der Schweizerische Bundesrat, Richtlinien des Bundesrates für die Risikovorprüfung und die Datenschutz-Folgenabschätzung bei Datenbearbeitungen durch die Bundesverwaltung, 2023, https://www.fedlex.admin.ch/eli/fga/2023/1882/de.

[19] Bundesamt für Justiz, Instrument für die Risikovorprüfung und DSFA-Leitfaden, https://www.bj.admin.ch/bj/de/home/staat/datenschutz/info-bundesbehoerden.html.

[20] Der Schweizerische Bundesrat, Verordnung über die Informationssicherheit bei der Bundesverwaltung und bei der Armee (Informationssicherheitsverordnung, ISV), 2022 (tritt am 1.1.2024 in Kraft).

[21] Die Bundesversammlung der Schweizerischen Eidgenossenschaft, Regierungs- und Verwaltungsorganisationsgesetz (RVOG), 1997, https://www.fedlex.admin.ch/eli/cc/1997/2022_2022_2022/de.

[22] Cloudcomputing Insider, Cloud Governance, 2021, https://www.cloudcomputing-insider.de/was-ist-cloud-governance-a-990452/ [Zugriff am 28.07.2023].

[23] Bundesamt für Informatik und Telekommunikation (BIT), Shared Responsibility Model, 2022, https://confluence.bit.admin.ch/x/I5vzFw.

D. Abkürzungen / Glossar

Begriff / Kürzel	Bedeutung
BK	Bundeskanzlei
Cloud Governance	Die Cloud Governance soll die nachvollziehbare, sichere und regelkonforme Nutzung von Cloud Services sicherstellen. Sie besteht aus einem Regelwerk und organisatorischen sowie technischen Maßnahmen, die unterschiedliche Aspekte der Cloud-Nutzung betreffen. [22]
CSB	Cloud Service Broker
DRB	Digitalisierungsrat Bund
DTI	Digitale Transformation und IKT Steuerung (Bereich der BK)
EDÖB	Eidgenössische/r Datenschutz- und Öffentlichkeitsbeauftrage/r
GSK	Generalsekretärenkonferenz
ID	Identifikator
IaaS	Infrastructure as a Service
IKT	Informations- und Kommunikationstechnik
ISDS	Informationssicherheits- und Datenschutzkonzept (ISDS)
ITSM	IT Service Management
Landing Zone	Eine Landing Zone ist eine sichere Umgebung in der Cloud, auf die unterschiedliche Anwender zugreifen können. Sie dient der Bereitstellung und der Nutzung von Apps und Workloads. Ihr Aufbau richtet sich nach den jeweiligen Firmenbedürfnissen. [7]
NCSC	Nationales Zentrum für Cybersicherheit
PaaS	Platform as a Service
SaaS	Software as a Service
SD	Standarddienst
SCHUBAN	Schutzbedarfsanalyse
VE	Verwaltungseinheit