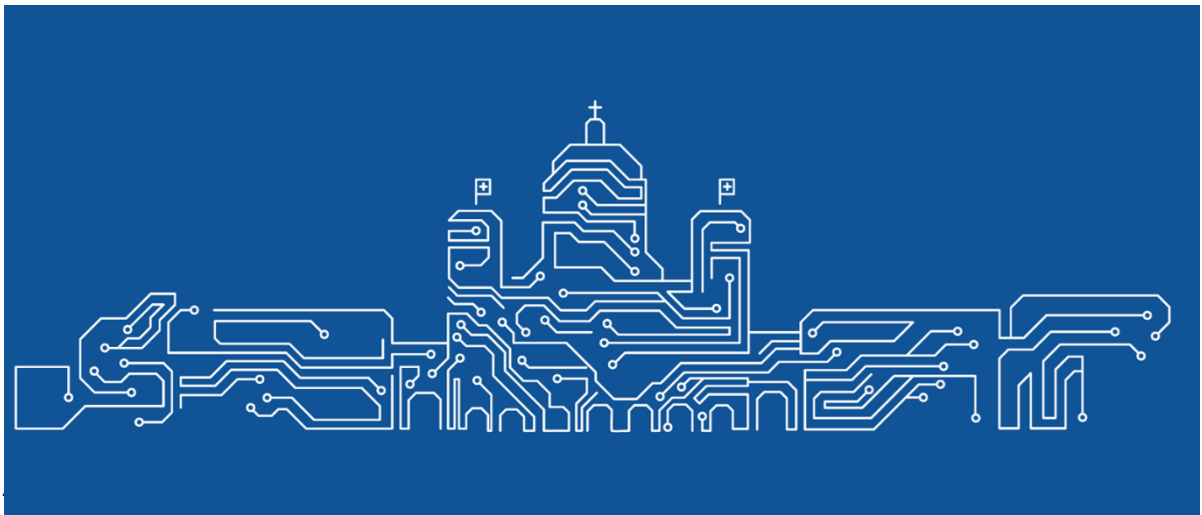




Cloud-Prinzipien der Bundesverwaltung, AR010, Version 1.2

Weisung des Bereichs Digitale Transformation und IKT-Lenkung DTI

gestützt auf Artikel 40 der Verordnung vom 1. Mai 2025 über die digitalen Dienste und die digitale Transformation in der Bundesverwaltung (Digitalisierungsverordnung, DigiV), SR 172.019.1



1 Kurzfassung

1.1 Wen betrifft diese Weisung?

Diese Weisung gilt für die Verwaltungseinheiten der zentralen Bundesverwaltung.

1.2 Warum ist diese Weisung notwendig?

Die Nutzung von Cloud-Diensten in der Bundesverwaltung soll geordnet, sicher und effizient erfolgen und dadurch Innovation, Skalierbarkeit und Schutz von Daten sichergestellt werden.

1.3 Was regelt diese Weisung auf welche Weise?

Die Cloud-Prinzipien regeln die Cloud-Governance der Bundesverwaltung (Private und Public Cloud) und legen die Leitplanken der Umsetzung der Cloud-Strategie fest.

1.4 Was wird von den Betroffenen dieser Weisung erwartet?

Die Departemente und Verwaltungseinheiten nutzen Cloud-Dienste nach einheitlichen Prinzipien, soweit diese als Weisungen verbindlich sind.

Die Departemente und Verwaltungseinheiten erhalten eine Hilfestellung bei der Beurteilung, welche Cloud-Stufe für ihre Fachanwendung geeignet ist.

Die Cloud-Intermediäre bauen auf einheitlichen Prinzipien auf.

Inhaltsverzeichnis

1	Kurzfassung	2
1.1	Wen betrifft diese Weisung?	2
1.2	Warum ist diese Weisung notwendig?.....	2
1.3	Was regelt diese Weisung auf welche Weise?	2
1.4	Was wird von den Betroffenen dieser Weisung erwartet?	2
2	Allgemeine Bestimmungen	4
2.1	Gegenstand.....	4
2.2	Geltungsbereich	5
2.3	Ziel der Cloud-Prinzipien	5
3	Cloud-Nutzung in der Bundesverwaltung anhand des Stufen-Modells	6
4	Cloud Governance und Grundsätze	9
4.1	Cloud Governance: organisatorisches Zusammenspiel	9
4.2	Grundsätze.....	10
5	Cloud-Prinzipien der Bundesverwaltung	12
5.1	Rechtlich verbindliche Weisungen	13
5.1.1	Sourcing & Beschaffung (SRC)	13
5.1.2	Organisation (ORG).....	14
5.1.3	Produkt Management (PM).....	15
5.2	Empfehlungen und Hinweise auf weitere Regelungen	16
5.2.1	Sourcing & Beschaffung (SRC)	16
5.2.2	Security, Risk & Compliance (SEC).....	19
5.2.3	Organisation (ORG).....	22

Anhänge

A.	Allgemeine Informationen zum Dokument	24
B.	Aufhebung bisheriger Vorgaben	24
C.	Übergangs- und Schlussbestimmungen	24
D.	Änderungen gegenüber Vorversion	24
E.	Bedeutung der Schlüsselwörter zur Bestimmung des Verbindlichkeitsgrades	24
F.	Beilagen, Referenzen und weiterführende Informationen	25
G.	Glossar	26
H.	Metadaten für die Suchoptimierung im Web	27

2 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 (gemäss "Strategie Rechenzentren der zivilen Bundesverwaltung" [24]) 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 Fertigtiefe).

Dieses Dokument beinhaltet

- drei Cloud-relevante DTI-Weisungen (siehe Kapitel 5.1), sowie
- Hinweise auf Cloud-relevante Regelungen anderer Stellen mit weiterführenden Informationen und DTI-Empfehlungen (siehe Kapitel 5.2)

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

2.1 Gegenstand

1. Die Cloud-Prinzipien regeln den Umgang mit Private- und 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).

Sourcing & Beschaffung (SRC)	Security, Risk & Compliance (SEC)	Organisation (ORG)	Product Management (PM)
<ul style="list-style-type: none"> • Public Cloud Sourcing-Entscheidung bei Departementen und BK (SRC-1) • Vorabklärung bezüglich passender Cloud-Stufe (SRC-2) • Beschaffung von Public-Cloud-Diensten (SRC-3) • Bezug von Private- und Public-Cloud-Diensten (SRC-4) 	<ul style="list-style-type: none"> • Sicherheitsverfahren durchführen (SEC-1) • Keine «geheim» klassifizierten Daten in Public Clouds (SEC-2) • Daten mit erhöhtem Schutzbedarf nur mit zusätzlichen Schutzmassnahmen in Public Clouds (SEC-3) 	<ul style="list-style-type: none"> • Konkretisierung und Erweiterung von Cloud-Prinzipien durch Departemente und Verwaltungseinheiten (ORG-1) • Konkretisierung und Erweiterung von Cloud-Prinzipien durch Intermediäre (ORG-2) • Intermediär unterstützt die Einhaltung der Cloud-Prinzipien und Cloud-Governance (ORG-3) • DTI bewilligt neue Intermediäre für Public Cloud(ORG-4) 	<ul style="list-style-type: none"> • Exit-Strategie bei der Nutzung von Public-Cloud-Diensten (PM-1)

Abbildung 1: Übersicht Cloud-Prinzipien der Bundesverwaltung

Die rot umrandeten Prinzipien SRC-4, ORG-4, PM-1 sind in Kapitel 5.1 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 5.2 thematisch gruppiert erörtert.

2.2 Geltungsbereich

1. Die Cloud-Prinzipien gelten für die Verwaltungseinheiten der zentralen Bundesverwaltung.
2. Die Prinzipien SRC-4, ORG-4 und PM-1 sind als Weisungen des Bereichs DTI der BK verbindlich.

2.3 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 Intermediäre bauen auf einheitlichen Prinzipien auf.

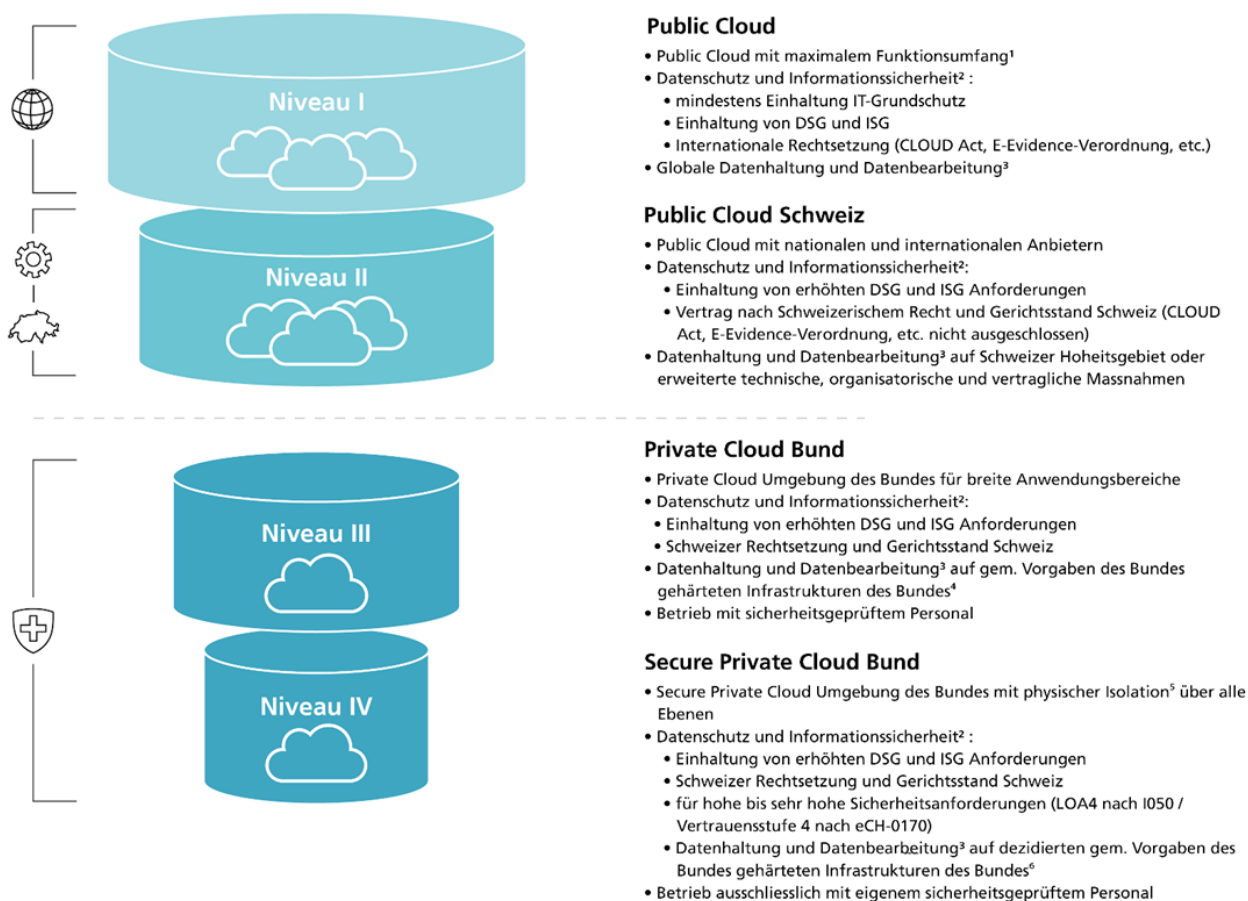
Der Fokus des vorliegenden Dokuments liegt auf Governance-Themen. Es beantwortet folgende Fragen:

- Welche Abstufungen in Bezug auf Datenschutz und Informationssicherheit werden bei der Cloud-Nutzung in der Bundesverwaltung unterschieden (Kapitel 3)?
- Auf welchen Grundlagen bauen die Cloud-Prinzipien der Bundesverwaltung auf (Kapitel 4)?
- Welche bundesweiten Cloud-Prinzipien werden als verbindliche Weisung durch den Bereich digitale Transformation und IKT-Lenkung (DTI) der Bundeskanzlei (BK) vorgegeben (Kapitel 5)?

3 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. Die Stufen sind zudem in Bezug auf Schutzbedarf aufsteigend additiv, d.h. jede Stufe erfüllt in dieser Hinsicht auch die Merkmale aller tieferen Stufen.



Keine Cloud: Es gibt weiterhin Anwendungen des Bundes, die ausschliesslich auf bundeseigenen Rechenzentren betrieben werden.

1) Edge Computing ist auf allen Stufen möglich.

2) Unterstützt durch technische, organisatorische und vertragliche Massnahmen auf der Ebene der Fachanwendung.

3) Datenhaltung und Datenbearbeitung beziehen sich auf Fach- und Personendaten (ohne Telemetrie).

4) Server Zonen Basic Bund & Basic Plus Bund

5) Optional ist physische Isolation auch für einzelne Mandanten möglich.

6) Server Zone Plus Enhanced Bund

Abbildung 2: Cloud-Stufenmodell der Bundesverwaltung (vgl. dazu auch die rechtlichen Rahmenbedingungen in [3])

Wenn die Bundesverwaltung Private- und Public-Cloud-Dienste nutzt, spielen die digitale Souveränität, Informationssicherheit und Datenschutz sowie auch Funktionalität und Skalierbarkeit eine zentrale Rolle. Daher müssen die Verwaltungseinheiten diese Themen mit äusserster Sorgfalt adressieren und die damit zusammenhängenden Trade-offs im Blick behalten.

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.

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 vorzuziehenden 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.

Stufe I	Stufe II	Stufe III	Stufe IV
Souveränität Anforderungen an den Cloud-Einsatz aufgrund politischer und geopolitischer Überlegungen			
<ul style="list-style-type: none"> globale Datenhaltung und Datenbearbeitung internationale Rechtssetzung: Cloud Act, E-Evidence-Verordnung, etc. 	<ul style="list-style-type: none"> Datenhaltung und Datenbearbeitung auf Schweizer Hoheitsgebiet oder erweiterte technische, organisatorische und vertragliche Massnahmen Vertrag nach Schweizer Recht und Gerichtsstand Schweiz (CLOUD Act, E-Evidence-Verordnung, etc. nicht ausgeschlossen) 	<ul style="list-style-type: none"> Datenhaltung und Datenbearbeitung auf gemäss Vorgaben des Bundes gehärteten Infrastrukturen des Bundes hohe Betriebssouveränität 	<ul style="list-style-type: none"> Datenhaltung und Datenbearbeitung auf dedizierten und gemäss Vorgaben des Bundes gehärteten Infrastrukturen des Bundes maximale Betriebssouveränität (minimale Abhängigkeit von Drittparteien) maximale Kontrolle über Daten und Systeme (maximale Zutritts- und Zugriffskontrolle)

Stufe I	Stufe II	Stufe III	Stufe IV
Skalierbarkeit Möglichkeiten und Flexibilität der Anpassungen an den effektiven Bedarf (Elastizität)			
<ul style="list-style-type: none"> maximale Flexibilität internationale Public Cloud-Anbieter mit globaler Infrastruktur Standardlösungen mit hoher Elastizität 	<ul style="list-style-type: none"> Public Cloud mit Einschränkungen internationale oder nationale Public Cloud-Anbieter 	<ul style="list-style-type: none"> Skalierbarkeit im Rahmen von «on premises» Infrastruktur des Bundes 	<ul style="list-style-type: none"> Skalierbarkeit im Rahmen von «on premises» Infrastruktur des Bundes und physische Isolation über alle Ebenen (HW/SW)

Stufe I	Stufe II	Stufe III	Stufe IV
Schutzbedarf Anforderungen an Einhaltung von Regeln, Standards und gesetzlichen Vorgaben			
<ul style="list-style-type: none"> • Einhaltung von IT Grundschutz (Mindestanforderung) • Einhaltung von DSG und ISG 	<ul style="list-style-type: none"> • Einhaltung von IT Grundschutz • Einhaltung von erhöhten DSG und ISG Anforderungen 	<ul style="list-style-type: none"> • Einhaltung von IT Grundschutz • Einhaltung von erhöhten DSG und ISG Anforderungen • interne Audits und Compliance-Prüfungen • Betrieb mit sicherheitsgeprüftem Personal 	<ul style="list-style-type: none"> • Einhaltung von IT Grundschutz und erweiterten Vorgaben • Einhaltung von erhöhten DSG und ISG Anforderungen • für hohe bis sehr hohe Sicherheitsanforderungen (LOA4 nach I050 / Vertrauensstufe 4 nach eCH-0170) • auch geeignet für Anwendungen mit geheim klassifizierten Daten und besonders schützenswerten Personendaten mit Gefährdung von Leib und Leben • Betrieb ausschliesslich mit eigenem sicherheitsgeprüftem Personal

Stufe I	Stufe II	Stufe III	Stufe IV
Funktionalität Portfolio an vielfältigen und innovativen Diensten			
<ul style="list-style-type: none"> • maximale Auswahl an Funktionalität • frühe innovative Lösungen • globales Massengeschäft 	<ul style="list-style-type: none"> • kleineres Funktionsportfolio als auf Stufe I • regionaler Fokus 	<ul style="list-style-type: none"> • standardisierte ausgewählte Services • hohe Kontrolle und Transparenz 	<ul style="list-style-type: none"> • Funktionalität für sicherheitskritische Anwendungen • maximale Kontrolle und Transparenz

Abbildung 3: Übersicht über die Cloud-Stufen anhand der vier relevanten Dimensionen und ihrer Trade-off-Beziehungen.

4 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 5.

Die wichtigsten Grundlagen und Grundsätze aus der Cloud-Strategie der Bundesverwaltung [1] sind hier wiedergegeben. Sie wurden aktuellen Erkenntnissen angepasst.

4.1 Cloud Governance: organisatorisches Zusammenspiel

Um in der Bundesverwaltung eine geordnete, sichere und effiziente Nutzung von Private- und Public-Cloud-Diensten zu erreichen, sind vertragliche, organisatorische und technische Massnahmen notwendig. Abbildung 4 zeigt das angestrebte organisatorische Zusammenspiel.

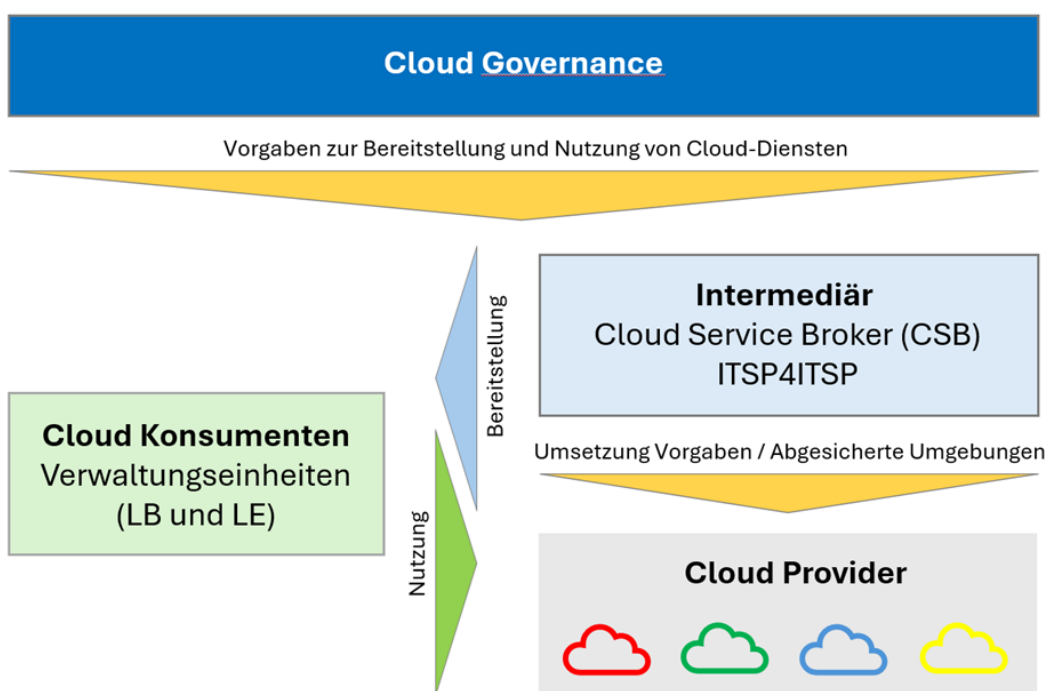


Abbildung 4: Cloud Governance Vorgaben zur Bereitstellung von Cloud-Diensten

Folgend sind die organisatorischen Fähigkeiten und Funktionen aus Abbildung 4 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 Intermediäre konkretisieren und erweitern die Governance für ihre jeweiligen Verantwortungsbereiche. DTI sorgt insbesondere auch dafür, dass die Angebote der Cloud Provider und Intermediäre konform mit dem Cloud-Stufenmodell sind. Im Zweifels- oder Streitfall entscheidet der D-DTI nach Anhörung des DRB. Die Verwaltungseinheiten bleiben verantwortlich für die Wahl der korrekten Stufe unter Einhaltung der allgemeinen Governance.

- **Intermediär:** Der Intermediär (auch Cloud Service Broker oder CSB genannt) unterstützt Verwaltungseinheiten beim geordneten, sicheren und effizienten Einsatz von Private- und 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 Intermediär im Intermediär-Pflichtenheft in Absprache mit den Leistungserbringern fest.
Der bisherige CSB des Bundesamts für Informatik und Telekommunikation (BIT) nimmt die Rolle des Intermediärs der Bundesverwaltung für Abrufe von Public Cloud (Stufen I & II) über die WTO-20007 wahr. Mit der Swiss Government Cloud (SGC) übernimmt das BIT die Rolle des Intermediärs der Bundesverwaltung für Private und Public Cloud (Stufen I-III). Das Angebot des Intermediärs der SGC umfasst auch ITSP4ITSP («IT Service Provider for IT Service Provider») für IKT-Leistungserbringer (LE). Der CSB des Informatik Service Center des EJPD (ISC-EJPD) ist Intermediär der Bundesverwaltung für Secure Private Cloud (Stufe IV). Zusätzlich gibt es für Public Cloud (Stufen I & II) weitere Intermediäre, die als dedizierte CSBs die spezifischen Bedürfnisse einzelner Departemente oder Bundesämter oder Fachgebiete abdecken (Stand Ende 2025: Swisstopo, MeteoSchweiz).
- **Cloud Provider:** Diese Funktion verantwortet den Betrieb der Cloud-Dienste. Die Rolle wird von den Private- und Public-Cloud-Anbietern sichergestellt.
- **Cloud Konsumenten:** Die Verwaltungseinheiten (LB und LE) sind verantwortlich für den Betrieb der Fachanwendungen in der Cloud.

4.2 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 (gemäss "Strategie Rechenzentren der zivilen Bundesverwaltung" [24]) und die Rechenzentren herkömmlicher Outsourcing-Partner (Bezug Managed Service, Auslagerung von Betriebsleistungen, usw.) als Sourcing-Optionen zur Auswahl. Mit der Swiss Government Cloud (SGC) wollen Bundesrat und Parlament der Bundesverwaltung zudem ermöglichen, das Massengeschäft auf den Cloud-Stufen I-III künftig über eine einheitliche Gesamtlösung abzuwickeln («Botschaft zu einem Verpflichtungskredit zum Aufbau einer Swiss Government Cloud» [25]).

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 (gemäss "Strategie Rechenzentren der zivilen Bundesverwaltung" [24]) 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 Datensouveränität).

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 Private- und 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 Public Cloud in einem ersten Schritt mit möglichst wenigen und maximal «intern» klassifizierten Informationen bzw. nicht besonders schützenswerten Personendaten zu beschreiten. Die Verwaltungseinheiten sollen sich zu diesem Thema vom Intermediär beraten lassen.

Höher als «intern» klassifizierte Informationen, besonders schützenswerte Personendaten oder Daten, die aus sonstigen Gründen speziell 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 das Staatssekretariat für Sicherheitspolitik (SEPOS) und der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (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]).

5 Cloud-Prinzipien der Bundesverwaltung

In diesem Kapitel werden die bundesweiten Cloud-Prinzipien beschrieben. Für eine bessere Übersichtlichkeit sind die Prinzipien in Abbildung 5 in Kategorien strukturiert. Zu den hell schattierten Kategorien sind aktuell noch keine bundesweiten Cloud-Prinzipien definiert.

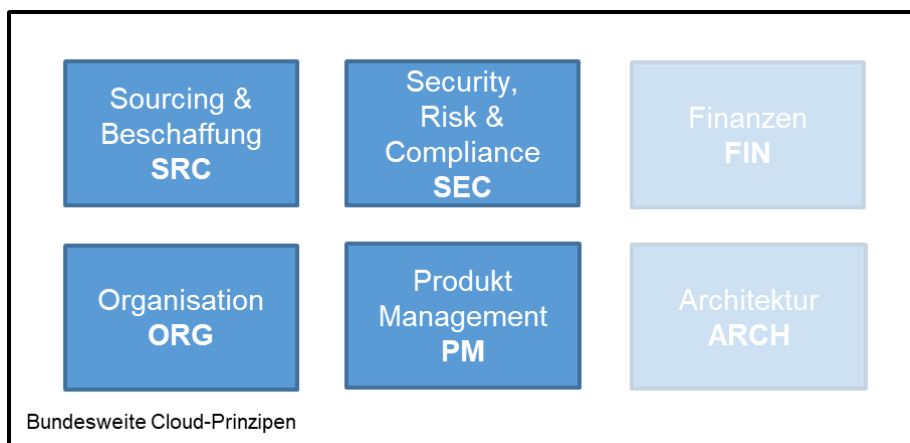


Abbildung 5: Kategorisierung Cloud-Prinzipien

Die bundesweiten Cloud-Prinzipien werden zentral durch den Bereich DTI der Bundeskanzlei erarbeitet und verwaltet. In Kapitel 5.1 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 5.2 thematisch gruppiert erörtert.

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

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

5.1 Rechtlich verbindliche Weisungen

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

5.1.1 Sourcing & Beschaffung (SRC)

ID	Name	Verbindlichkeitsgrad ¹	Bezug zu Grundsatz aus Cloud-Strategie
SRC-4	WEISUNG: Bezug von Private- und Public-Cloud-Diensten	MUSS	S-1, O-1
<p>Bestimmung</p> <p>Jede Verwaltungseinheit MUSS ihre Private- und Public-Cloud-Dienste für Infrastructure as a Service (IaaS) und Platform as a Service (PaaS) über einen Intermediär beziehen. Private Cloud der Stufe III MUSS nach Bezugsbereitschaft der Swiss Government Cloud (SGC) über den Intermediär der SGC bezogen werden.</p> <p>Ausgenommen von diesem Prinzip sind Software as a Service (SaaS), ERP-Angebote und Büroautomation.</p>			
<p>Erläuterungen</p> <p>Durch dieses Prinzip werden die Bezüge kanalisiert und die Leistungsbezüger erhalten Unterstützung in der Einhaltung der Governance.</p> <p>Dieses Prinzip hilft, den Bezug für die Verwaltungseinheiten geordnet und effizient zu gestalten, und möglichst viele Schritte auf Intermediär-Seite zu automatisieren.</p> <p>DTI sorgt insbesondere auch dafür, dass die Angebote der Cloud Provider und Intermediäre konform mit dem Cloud-Stufenmodell sind. Im Zweifels- oder Streitfall entscheidet der D-DTI nach Anhörung des DRB.</p>			
<p>Bezug zu Cloud-Stufen</p> <p>Alle Stufen</p>			
<p>Weiterführende Informationen</p> <p>Definitionen IaaS, PaaS, SaaS [9]: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecial-publication800-145.pdf</p>			

¹ Zur Bedeutung der Schlüsselwörter zur Bestimmung des Verbindlichkeitsgrade siehe Anhang E.

5.1.2 Organisation (ORG)

ID	Name	Verbindlichkeitsgrad	Bezug zu Grundsatz aus Cloud-Strategie
ORG-4	WEISUNG: DTI bewilligt neue Intermediäre für Public Cloud	MUSS	O-1
<p>Bestimmung</p> <p>Möchte eine Verwaltungseinheit die Intermediär-Funktion für Public Cloud 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 Intermediär-Pflichtenheft. Gegebenenfalls bewilligt der Bereich DTI der BK den Antrag.</p> <p>Erläuterungen</p> <p>Der Grundsatz O-1 sieht vor, dass neben den umfassenden Intermediären der Bundesverwaltung weitere Intermediäre für Public Cloud, sogenannte dedizierte Intermediäre oder CSBs, möglich sind. Um dedizierter CSB zu werden, müssen gewisse Anforderungen durch die Verwaltungseinheit erfüllt werden. Diese sind im Intermediär-Pflichtenheft definiert [8]. Darin wird zwischen einem Intermediär der Bundesverwaltung und dedizierten CSBs unterschieden; an sie werden unterschiedliche Anforderungen gestellt. Wenn diese Anforderungen erfüllt sind und gute Gründe für die Übernahme der Intermediär-Funktion für Public Cloud durch die Verwaltungseinheit gegeben sind, bewilligt der Bereich DTI der BK den Antrag in Form eines D-DTI Beschlusses nach Anhörung des DRB.</p>			
<p>Bezug zu Cloud-Stufen</p> <p>Stufe I, II</p>			
<p>Weiterführende Informationen</p> <p>Intermediär-Pflichtenheft mit Aufgaben, Kompetenzen und Verantwortlichkeiten eines Intermediärs siehe [8]</p>			

5.1.3 Produkt Management (PM)

ID	Name	Verbindlichkeitsgrad	Bezug zu Grundsatz aus Cloud-Strategie
PM-1	WEISUNG: Exit-Strategie bei der Nutzung von Public-Cloud-Diensten	MUSS	-
<p>Bestimmung Verwaltungseinheiten sind verantwortlich für das Business Continuity Management (BCM) ihrer Anwendungen. Damit Abhängigkeiten von Public-Cloud-Anbietern bewusst und kontrolliert eingegangen werden, MUSS die zuständige Verwaltungseinheit mit Unterstützung durch den verantwortlichen Intermediär 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.</p> <p>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. Die Verwaltungseinheiten sorgen dafür, dass ihre Anwendungen wo immer möglich anbieterunabhängig in der Cloud betrieben werden können und wiederherstellbar sind. Dies kann beispielsweise durch eine anbieteragnostische Implementierung oder die (redundante) Speicherung der Daten ausserhalb der Anbieterplattform erreicht 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. Unterstützende Hinweise und Hilfestellungen zur Ausgestaltung der Exit-Strategie finden sich in der Cloud-Exit-Strategie-Guideline [6].</p>			
<p>Bezug zu Cloud-Stufen Stufe I, II</p>			
<p>Weiterführende Informationen Keine</p>			

5.2 Empfehlungen und Hinweise auf weitere Regelungen

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

5.2.1 Sourcing & Beschaffung (SRC)

ID	Name	Bezug zu Grundsatz aus Cloud-Strategie
SRC-1	Cloud Sourcing-Entscheidung bei Departementen und BK	S-1
<p>Bestimmungen</p> <p>Der Entscheid über den Einsatz von 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.</p>		
<p>Erläuterungen</p> <p>Analog zur Entscheidungsbefugnis in anderen Sourcing-Bereichen hält dieses Prinzip die Entscheidungsbefugnis im Bereich der Cloud-Dienste fest (Auswahl der geeigneten Cloud-Stufe). Die Befugnisse entsprechen den Grundsätzen, die in Art. 9 DigiV [2] definiert sind. Bei der Rechtskonformität wird insbesondere auf Datenschutz, Informationssicherheit und allfällige Geheimhaltungspflichten geachtet.</p>		
<p>Bezug zu Cloud-Stufen</p> <p>Alle Stufen</p>		
<p>Weiterführende Informationen</p> <p>Art. 9 DigiV: Entscheid über den Leistungsbezug und Art. 11 DigiV: Weisungen der Bundeskanzlerin oder des Bundeskanzlers über Standarddienste mit Bezugswang [2]: https://www.fedlex.admin.ch/eli/cc/2025/235/de</p> <p>IKT-Sourcing-Strategie des Bundes [10]: https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/vorgaben/sb017-ikt-strategie_sourcing.html</p> <p>IKT-Vorgaben des Bundes [11]: https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/vorgaben.html</p>		

ID SRC-2	Name Vorabklärung bezüglich passender Cloud-Stufe	Bezug zu Grundsatz aus Cloud-Strategie S-2, D-1
<p>Bestimmung</p> <p>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.</p> <p>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 Error! Reference source not found.). Die Verantwortung liegt bei der jeweiligen Verwaltungseinheit bzw. deren Departement.</p> <p>Falls höher als «intern» klassifizierte Informationen, besonders schützenswerte Personendaten oder Daten, die aus sonstigen Gründen speziell schützenswert sind (z.B. aufgrund spezialgesetzlicher Grundlage) in den Public Clouds bearbeitet werden, muss die Generalsekretärenkonferenz (GSK) sowie das Staatssekretariat für Sicherheitspolitik (SEPOS) und der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) vorgängig informiert werden.</p>		
<p>Erläuterungen</p> <p>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 Bundesamts für Cybersicherheit (BACS) [12].</p> <p>Für weitere Details zur Anwendung der Sicherheitsverfahren siehe Prinzip SEC-1.</p>		
<p>Bezug zu Cloud-Stufen</p> <p>Alle Stufen</p>		
<p>Weiterführende Informationen</p> <p>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</p> <p>BACS Sicherheitsverfahren [12]: https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren.html</p> <p>Projektvorgehensmethodik HERMES [13]: https://www.hermes.admin.ch/</p>		

ID	Name	Bezug zu Grundsatz aus Cloud-Strategie
SRC-3	Beschaffung von Public-Cloud-Diensten	S-1, S-2, S-3
<p>Bestimmung</p> <p>Jede Verwaltungseinheit soll ihre Public-Cloud-Dienste für Infrastructure as a Service (IaaS) und Platform as a Service (PaaS) über die WTO 20007 bzw. nach Bezugsbereitschaft WTO der Swiss Government Cloud (SGC) über die SGC abrufen.</p> <p>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.</p> <p>Die vergaberechtlichen Grundsätze müssen stets eingehalten werden.</p>		
<p>Erläuterungen</p> <p>Die Schaffung einer anderen beschaffungsrechtlichen Grundlage ist dann vorzusehen, wenn der Leistungsgegenstand nicht von der WTO 20007 oder der WTO der SGC erfasst ist bzw. die Zuschlagsempfänger die nachgefragten Leistungen nicht gestützt auf diese WTO-Ausschreibungen erbringen können.</p> <p>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 bzw. der WTO der SGC.</p>		
<p>Bezug zu Cloud-Stufen</p> <p>Stufe I, II</p>		
<p>Weiterführende Informationen</p> <p>Definitionen IaaS, PaaS, SaaS [9]: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecial-publication800-145.pdf</p> <p>Bundesgesetz über das öffentliche Beschaffungswesen (BöB) SR 172.056.1 [14]: https://www.fedlex.admin.ch/eli/cc/2020/126/de</p> <p>Verordnung über das öffentliche Beschaffungswesen (VöB) (SR 172.056.11) [15]: https://www.fedlex.admin.ch/eli/cc/2020/127/de</p>		

5.2.2 Security, Risk & Compliance (SEC)

ID	Name	Bezug zu Grundsatz aus Cloud-Strategie
SEC-1	Sicherheitsverfahren durchführen	D-1
<p>Bestimmung</p> <p>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.</p> <p>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.</p> <p>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).</p> <p>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.</p>		
<p>Erläuterungen</p> <p>Die Vorgaben des Bundesamts für Cybersicherheit (BACS) zum Sicherheitsverfahren [12] sind auch für potentielle Public-Cloud-Projekte anzuwenden.</p> <p>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.</p> <p>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].</p>		
<p>Bezug zu Cloud-Stufen</p> <p>Alle Stufen</p>		
<p>Weiterführende Informationen</p> <p>Informationsseite zur Cloud in der Bundesverwaltung [17]: https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html</p> <p>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</p> <p>BACS Sicherheitsverfahren [12]: https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren.html</p> <p>Projektvorgehensmethodik HERMES [13]: https://www.hermes.admin.ch/</p> <p>EDÖB Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes [16]: https://www.edoeb.admin.ch/dam/de/sd-web/eVhrh8wY3QcR/leitfaden_tom.pdf</p> <p>Richtlinien des Bundesrates für die Risikovorprüfung und die Datenschutz-Folgenabschätzung bei Datenbearbeitungen durch die Bundesverwaltung (BBI 2023 1882) [18]: https://www.fedlex.admin.ch/eli/fga/2023/1882/de</p> <p>Instrument für die Risikovorprüfung und DSFA-Leitfaden [19]: https://www.bj.admin.ch/bj/de/home/staat/datenschutz/info-bundesbehoerden.html</p>		

ID	Name	Bezug zu Grundsatz aus Cloud-Strategie
SEC-2	Keine «geheim» klassifizierten Daten in Public Clouds	D-1
<p>Bestimmung Als «geheim» klassifizierte Daten dürfen nicht in Public Clouds (Stufen I und II) sowie der Private Cloud Stufe III gespeichert oder bearbeitet werden.</p>		
<p>Erläuterungen Die Verwaltungseinheit stellt sicher, dass «geheim» klassifizierte Daten unter der alleinigen Kontrolle der Bundesverwaltung bleiben. Dies gilt auch für Informatikmittel der Sicherheitsstufe «sehr hoher Schutz» gemäss ISG [4]</p>		
<p>Bezug zu Cloud-Stufen Stufe I, II, III</p>		
<p>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]: https://www.fedlex.admin.ch/eli/cc/2023/735/de</p>		

ID SEC-3	Name Daten mit erhöhtem Schutzbedarf nur mit zusätzlichen Schutzmassnahmen in Public Clouds	Bezug zu Grundsatz aus Cloud-Strategie D-1
<p>Bestimmung</p> <p>Als Voraussetzung für die Bearbeitung und Speicherung in der Public Cloud von «vertraulich» klassifizierten Informationen, sowie Daten, die Geheimhaltungspflichten unterliegen, müssen angemessene vertragliche, organisatorische und technische Schutzmassnahmen die Einhaltung des anwendbaren Rechts sicherstellen.</p> <p>Dies gilt auch bei besonders schützenswerten Personendaten bzw. 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).</p> <p>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.</p>		
<p>Erläuterungen</p> <p>In der Schutzbedarfsanalyse wird geklärt, ob eine Anwendung klassifizierte Daten oder Personendaten beinhaltet oder generiert.</p> <p>Sofern im Einzelfall beurteilte und angebrachte vertragliche, organisatorische und technische Schutzmassnahmen die Einhaltung des geltenden Rechts erlauben, können auch Daten, die einen erhöhten Schutzbedarf aufweisen oder datenschutzrechtlich geschützt sind, in einer Public Cloud gespeichert und verarbeitet werden.</p> <p>Ob die vorgesehenen Schutzmassnahmen ausreichen, wird im Rahmen des BACS Sicherheitsverfahrens [12] und/oder einer Datenschutz-Folgenabschätzung geprüft.</p> <p>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.</p> <p>Eine Massnahme im Bereich der digitalen Souveränität kann z.B. eine redundante Datenerhaltung (Public Cloud und in einem Rechenzentrum der Bundesverwaltung) zur Sicherstellung der Verfügbarkeit sein.</p> <p>Solche Massnahmen sollten mit dem zuständigen Departement abgestimmt sein.</p>		
<p>Bezug zu Cloud-Stufen</p> <p>Stufe I, II</p>		
<p>Weiterführende Informationen</p> <p>Bericht Rechtlicher Rahmen für die Nutzung von Cloud-Diensten in der Bundesverwaltung [3]: Cloud (admin.ch)</p> <p>BACS Sicherheitsverfahren [12]: https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren.html</p> <p>EDÖB Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes [16]: https://www.edoeb.admin.ch/dam/de/sd-web/eVhrh8wY3QcR/leitfaden_tom.pdf</p>		

5.2.3 Organisation (ORG)

ID	Name	Bezug zu Grundsatz aus Cloud-Strategie
ORG-1	Konkretisierung und Erweiterung von Cloud-Prinzipien durch Departemente und Verwaltungseinheiten	O-1
<p>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.</p>		
<p>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.</p>		
<p>Bezug zu Cloud-Stufen alle Stufen</p>		
<p>Weiterführende Informationen Regierungs- und Verwaltungsorganisationsgesetz (RVOG) [21]: https://www.fedlex.admin.ch/eli/cc/1997/2022_2022_2022/de</p>		

ID	Name	Bezug zu Grundsatz aus Cloud-Strategie
ORG-2	Konkretisierung und Erweiterung von Cloud-Prinzipien durch Intermediäre	O-1
Bestimmung Die Intermediäre dürfen die Cloud-Prinzipien in ihrem Zuständigkeitsbereich konkretisieren und/oder erweitern. Die Kunden können bei Anpassungen von Cloud-Prinzipien über den verantwortlichen Intermediär Einfluss nehmen. Diese Anpassungen gelten nur für die Kunden des jeweiligen Intermediärs.		
Erläuterungen Dieses Prinzip gibt den Intermediären 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		

ID	Name	Bezug zu Grundsatz aus Cloud-Strategie
ORG-3	Intermediär unterstützt die Einhaltung der Cloud-Prinzipien und Cloud-Governance	O-1
Bestimmung Ein Intermediär 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 Intermediärs: 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 Alle Stufen		
Weiterführende Informationen Intermediär-Pflichtenheft mit Aufgaben, Kompetenzen und Verantwortlichkeiten eines Intermediärs siehe [8]		

Anhänge

A. Allgemeine Informationen zum Dokument

Version und Status	Version 1.2 In Kraft
Originalsprache	Deutsch
Beschluss vom	10. Dezember 2025
Inkraftsetzung am	1. Januar 2026
Ablaufdatum	Der Bereich DTI der BK überprüft die Aktualität und Zweckmässigkeit der Cloud-Prinzipien regelmässig, spätestens vier Jahre nach deren Inkraftsetzung.

B. Aufhebung bisheriger Vorgaben

Diese Version ersetzt die bisherige Version 1.1.

C. Übergangs- und Schlussbestimmungen

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.
2. *Einhaltung der Weisungen SRC-4, ORG-4 und PM-1*
Die Departemente und die Bundeskanzlei sorgen gemäss Artikel 6 DigiV in ihrem Zuständigkeitsbereich für die Umsetzung der Weisungen.

D. Änderungen gegenüber Vorversion

Ausweitung der Intermediär-Rolle auf alle Stufen (Private und Public Cloud), Berücksichtigung des bundesweiten Secure Private Cloud-Angebots des ISC-EJPD und Übergang von «Public Clouds» (WTO-20007) zur SGC.

E. Bedeutung der Schlüsselwörter zur Bestimmung des Verbindlichkeitsgrades

Der Verbindlichkeitsgrad der einzelnen Bestimmungen dieser Weisung wird mittels folgender Schlüsselwörter in Grossbuchstaben gekennzeichnet. Die Verbindlichkeitsgrade basieren auf dem internationalen Standard IETF/RFC 2119 BCP14 und lehnen sich damit an eine verbreitete Praxis in der internationalen Standardisierung.

Schlüsselwort	Verbindlichkeitsgrad
MUSS	Anordnung, Anforderung, Bestimmung die einzuhalten ist. Für Ausnahmen und Abweichungen muss ein schriftliches Gesuch gestellt und vom Bereich DTI genehmigt werden. (MUST, REQUIRED, SHALL)
SOLL	Anordnung, Anforderung, Bestimmung, die einzuhalten ist. Ausnahmen und Abweichungen, z.B. aus wirtschaftlichen oder sicherheitstechnischen Aspekten, müssen schriftlich begründet werden. Eine explizite Ausnahmegewährung des Bereichs DTI ist nicht erforderlich. (SHOULD, RECOMMENDED)

DARF NICHT	Option, die nicht gewählt, bzw. Massnahme, die nicht umgesetzt werden darf. (MUST NOT, SHALL NOT)
DARF	Option, die explizit erlaubt ist. Die potenziell Nutzenden bzw. Anwendenden der Option entscheiden, ob sie diese nutzen wollen. Der Anbieter muss die Option unterstützen bzw. anbieten.
KANN	Option, die akzeptiert ist. Der Anbieter der Option entscheidet darüber, ob er diese unterstützen bzw. anbieten will.

F. Beilagen, Referenzen und weiterführende Informationen

ID Referenz

- [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/vorgaben/sb020-cloud-strategie_der_bundesverwaltung.html.
- [2] Der Schweizerische Bundesrat, Verordnung über die digitalen Dienste und die digitale Transformation in der Bundesverwaltung (DigiV), SR 172.019.1, 2025, <https://www.fedlex.admin.ch/eli/cc/2025/235/de>.
- [3] Bundeskanzlei, Bericht Rechtlicher Rahmen für die Nutzung von Public-Cloud-Diensten in der Bundesverwaltung (Version 2.0), 2025, <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] Bundeskanzlei, Cloud-Exit-Strategie-Guideline [in Arbeit].
- [7] IT-Business, Was ist eine Landing Zone?, 2022, <https://www.it-business.de/was-ist-eine-landing-zone-a-0c951fabad3e2dcc1bf4e7cd50d2d2f5/> [Zugriff am 29.10.2025].
- [8] Bundeskanzlei, Intermediär-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/vorgaben/sb017-ikt-strategie_sourcing.html.
- [11] Bundeskanzlei, IKT-Vorgaben, <https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/vorgaben.html>.
- [12] Bundesamt für Cybersicherheit (BACS), Sicherheitsverfahren, 2022, <https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren.html>.
- [13] Bundeskanzlei, HERMES Projektmanagement Methodik, <https://www.hermes.admin.ch/>.

ID Referenz

- [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), Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes (TOM), 2024, https://www.edoeb.admin.ch/dam/de/sd-web/eVhrh8wY3QcR/leitfaden_tom.pdf.
- [17] Bundeskanzlei, Digitale Transformation und IKT Steuerung (DTI), Cloud, 2025, <https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html>.
- [18] Der Schweizerische Bundesrat, Richtlinien des Bundesrates für die Risikoprüfung 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 Risikoprüfung 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), 2024, <https://www.fedlex.admin.ch/eli/cc/2023/735/de>.
- [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 29.10.2025].
- [23] Bundesamt für Informatik und Telekommunikation (BIT), Shared Responsibility Model, 2022, <https://confluence.bit.admin.ch/x/I5vzFw>.
- [24] SB022 - Strategie Rechenzentren der zivilen Bundesverwaltung, 2025, <https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/vorgaben/sb022-strategie-rechenzentren-der-zivilen-bundesverwaltung.html>.
- [25] Botschaft zu einem Verpflichtungskredit zum Aufbau einer Swiss Government Cloud, 2024, <https://www.fedlex.admin.ch/eli/fga/2024/1408/de>.

Links zu weiterführenden Informationen

Keine.

G. Glossar

Abkürzung/ Begriff	Bedeutung
BACS	Bundesamt für Cybersicherheit
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 (siehe Intermediär)

Abkürzung/ Begriff	Bedeutung
DRB	Digitalisierungsrat Bund
DTI	Digitale Transformation und IKT Steuerung (Bereich der BK)
EDÖB	Eidgenössische/r Datenschutz- und Öffentlichkeitsbeauftragte/r
GSK	Generalsekretärenkonferenz
ID	Identifikator
IaaS	Infrastructure as a Service
IKT	Informations- und Kommunikationstechnik
Intermediär	Der Intermediär (auch Cloud Service Broker oder CSB genannt) unterstützt Verwaltungseinheiten beim geordneten, sicheren und effizienten Einsatz von Private- und Public-Cloud-Diensten.
ISDS	Informationssicherheits- und Datenschutzkonzept (ISDS)
ITSM	IT Service Management
ITSP4ITSP	IT Service Provider for IT Service Provider (Modell der SGC, über welches IKT-Leistungserbringer ihren Kunden aus dem Bund sowie anderen Stellen der öffentlichen Verwaltung Leistungen aus der SGC anbieten können).
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]
PaaS	Platform as a Service
SaaS	Software as a Service
SD	Standarddienst
SCHUBAN	Schutzbedarfsanalyse
SEPOS	Staatssekretariat für Sicherheitspolitik
SGC	Swiss Government Cloud
VE	Verwaltungseinheit

H. Metadaten für die Suchoptimierung im Web

Thema DigiV Art. 40 Abs 1	Prozess
Strategiebezug	Verwaltung als Plattform (auch Interoperabilität)
Fähigkeitsdomäne	Services & Anwendungen Entwicklung & Auslieferung & Betrieb
Bezug zur Architekturvision 2050	Standardmässig interoperabel
Dokumentenhierarchie	W010 Architekturprinzipien und W012 Digitale Souveränität der Bundesverwaltung sind dieser Weisung übergeordnet.