

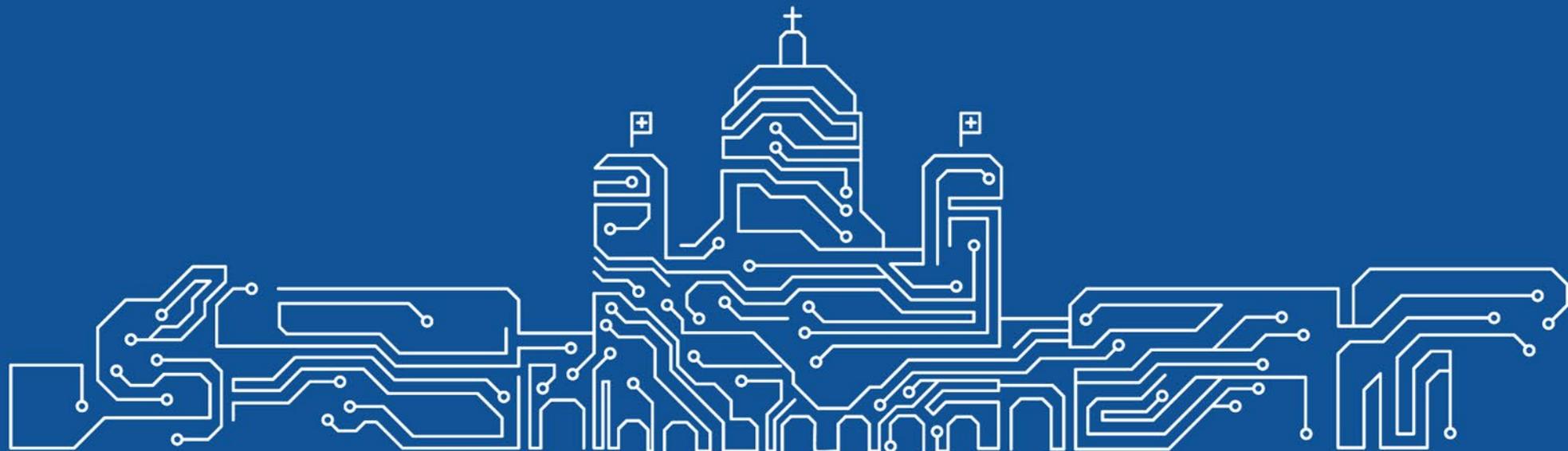


Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Bundeskanzlei BK  
Digitale Transformation und IKT-Lenkung (DTI)

# Lessons Learned aus der Cloud-Beschaffung der Bundesverwaltung

Dr. Erica Dubach, IT-Beschaffungskonferenz 2022





# Inhalt

- Public Clouds in der Cloud Strategie der Bundesverwaltung
- Darstellung Cloud-Nutzung in der Bundesverwaltung
- Verlauf: Ausschreibung, Zuschlag und Verhandlungsbeginn
- Vorhaben «Public Clouds Bund»: Zwei Schwerpunkte
- Interne Governance und Hilfestellungen in Arbeit
- Ausblick
- Diskussion



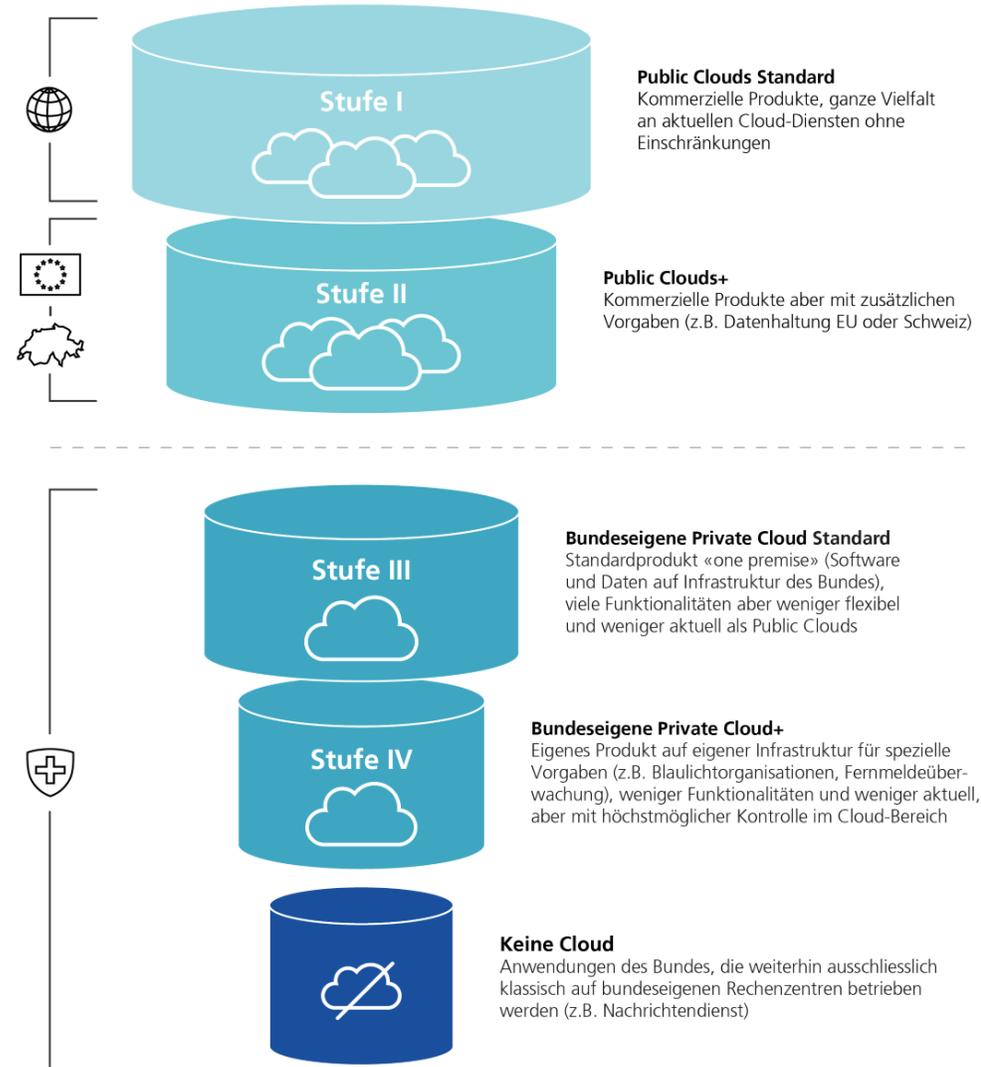
# Public Clouds in der Cloud Strategie der Bundesverwaltung

- Die Bundesverwaltung verfügt über die Fähigkeiten, IT-Dienste nach verschiedenen Liefermodellen geordnet, sicher und effizient bereitzustellen und zu nutzen
- Public Clouds sind ein wichtiger Bestandteil der Hybrid-Multi-Cloud Strategie des Bundes um die Digitale Transformation der Bundesverwaltung zu ermöglichen.
- Diese Ausschreibung WTO-20007 ermöglicht der Bundesverwaltung, innovative Vorhaben schneller und agiler umzusetzen
- Das Ziel sind effiziente Verwaltungsleistungen zu Gunsten der Bürger, Wirtschaft, Bildung, Wissenschaft und Behörden
- Das Projekt genießt eine sehr hohe interne und externe Aufmerksamkeit

[Cloud-Strategie der Bundesverwaltung \(admin.ch\)](#)



# Darstellung Cloud-Nutzung in der Bundesverwaltung (in Review)





## Verlauf: Ausschreibung, Zuschlag und Verhandlungsbeginn

- Ausschreibung «Public Clouds Bund» über 5 Jahre und 110 M CHF auf SIMAP (7. Dezember 2020)
- Zuschlag an 5 Anbieter (Juni 2021): Microsoft, Amazon (AWS), Oracle Software, IBM, Alibaba
- Beschwerde von Google gegen die Public-Cloud-Vergabe des Bundes (Juli 2021)
- Rückzug der Beschwerde durch Google (Oktober 2021)
- Beginn Vertragsverhandlungen (März 2022)

[«Public Clouds Bund»: Verträge mit den Anbietern werden ausgearbeitet \(admin.ch\)](https://www.admin.ch)



# Vorhaben «Public Clouds Bund»: Zwei Schwerpunkte

## Verträge mit Public Cloud Anbieter

- Parallele Verhandlungen mit allen fünf Anbietern
- Vertragsausarbeitung

## Interne Grundlagen

- Governance (Vorgaben) für Verwaltungseinheiten für Bezug von Cloud-Leistungen
- Hilfestellungen
- Technische Grundlagen

- Komplexe rechtliche, technische und organisatorische Arbeiten
- Leitung Bereich Digitale Transformation und IKTLenkung (DTI) der Bundeskanzlei in enger Zusammenarbeit mit Bundesamt für Bauten und Logistik (BBL) und dem Bundesamt für Informatik und Telekommunikation (BIT)
- 4 Teams: Vertragsverhandlungen, Interne Prozesse, Recht, Kommunikation



# Vertragsverhandlungen

- Kickoff mit allen 5 Anbietern gleichzeitig
- Kommunikationsregeln
- Rahmenvertrag, einheitliches Abrufverfahren und Anhänge
- Analyse der Offerten gegenüber einem Anforderungskatalog als Verhandlungsbasis
- Ziel: Verbesserung der Konditionen bei allen Vertragspartnern über den Anforderungen der Ausschreibung und höhere Schutzstandards als mindestens benötigt



# Initiale Gap Analyse der Angebote

Domain	Anforderung	Anbieter				
		1	2	3	4	5
<b>Datenschutz</b>	Weisungsgebundenheit der Auftragsbearbeitung (Art. 10a DSG, Art. 9 nDSG)	Green	Green	Green	Red	Yellow
	Keine Bearbeitung für eigene Zwecke (Art. 10a DSG, Art. 9 nDSG)	Yellow	Green	Yellow	Yellow	Red
	Einbindung Unterauftragsbearbeiter (Art. 10a DSG, Art. 9 nDSG)	Red	Yellow	Yellow	Yellow	Red
	Bekanntgabe ins Ausland (Art. 6 DSG, Art. 16)	Yellow	Yellow	Green	Yellow	Yellow
<b>Security</b>	Umsetzung TOMs zur Gewährleistung CIA (Confidentiality, Integrity, Availability)	Green	Red	Green	Green	Red
	Zertifizierungen, Auditberichte	Green	Yellow	Green	Red	Yellow
	Datenhaltungs- und -bearbeitungsstandorte	Yellow	Yellow	Yellow	Red	Red
	Migration und endgültige Löschung der Daten	Green	Yellow	Yellow	Red	Red
	Transportschutz- und -verschlüsselung	Green	Green	Green	Red	White
	Meldung von Sicherheitsvorfällen	Red	Red	Yellow	Green	Yellow
<b>Geheimnisrecht</b>	Geheimhaltungsvereinbarungen (inkl. Mitarbeiter und Subunternehmer)	Red	Yellow	Yellow	Yellow	Red
	Angemessener Schutz vor Klartextzugriffen (inkl. Mitarbeiter)	Yellow	Yellow	Yellow	Red	White
	Einbindung als Hilfsperson (Art. 320, 321 StGB)	White	White	White	White	White
<b>Data Sovereignty</b>	Anerkennung Garantieverantwortung (tbd)	White	White	White	White	White
	Umgang mit Zugriffen durch Dritte (Verfahren, insb. Verweis auf Kunde, Information, Rechtsmittel)	Red	Green	Green	Red	Red
<b>BCM</b>	Datenexport	Yellow	Yellow	Yellow	Yellow	Red
	Notfallplanung	Red	Yellow	Green	Yellow	Red
	Kündigung und Termination Assistance	Red	White	White	White	Red
<b>Allgemein</b>	Audit	Yellow	Yellow	Red	Red	Red
	Anwendbares Recht, Gerichtsstand Schweiz	Yellow	Yellow	Yellow	Green	Red
	Haftung	Red	Yellow	Yellow	Yellow	Red
	<b>Anzahl "gut (grün)" und Anzahl "genügend (orange)"</b>	<b>12</b>	<b>16</b>	<b>17</b>	<b>10</b>	<b>4</b>
	Anzahl "rot (ungenügend) und Anzahl "nicht vorhanden (weiss)"	9	5	4	11	17



# Interne Governance und Hilfestellungen in Arbeit (1/2)

## Anbieterneutrales Pflichtenheft

- Ausgangslage und Beschreibung des Abrufgegenstandes
- Risikobeurteilung (Datenschutz, Informationssicherheit, organisatorische, technische und vertragliche Massnahmen)
- Funktionale Anforderungen
- High Level Solution Architektur
- Evaluationskriterien

## Evaluationskriterien

- Preis: Kosten / Service-Kosten (bezogen auf geplante Bezugsmenge)
- Allfällige Migrationskosten
- Erfüllungsgrad der technischen Anforderungen
- Risikobeurteilung (Datenschutz, Informationssicherheit, zugehörige organisatorische- und technische Massnahmen)
- Konformität zur Cloud-Strategie und zur bestehenden Ausgangslage bei der Bezugsberechtigten



# Interne Governance und Hilfestellungen in Arbeit (2/2)

## Pflichtenheft Cloud Service Broker

- Rechte und Pflichten des CSB
- Abrufverfahren
- Verrechnungsmodell
- Controlling
- Publikationen der Zuschläge
- Security, Risk und Compliance

## Rechtlicher Rahmen für die Nutzung von Public-Cloud-Diensten in der Bundesverwaltung

- Datenschutzgesetzgebung des Bundes
- Amtsgeheimnis
- Cyberrisikenverordnung
- Bestimmungen zum Informationsschutzgesetz des Bundes
- Risikoaspekte (inkl. Hilfestellungen)
- Relevante Rechtsgrundlagen
- Checkliste Daten und technische Massnahmen



# Ausblick

- Finalisierung und Verabschiedung der Dokumente (verschiedene Gremien)
- Abklärungen und Vorbereitung zur internen und externen Kommunikation
- Unterstützung Verwaltungseinheiten für Erstbezug auf WTO-20007



# Diskussion

