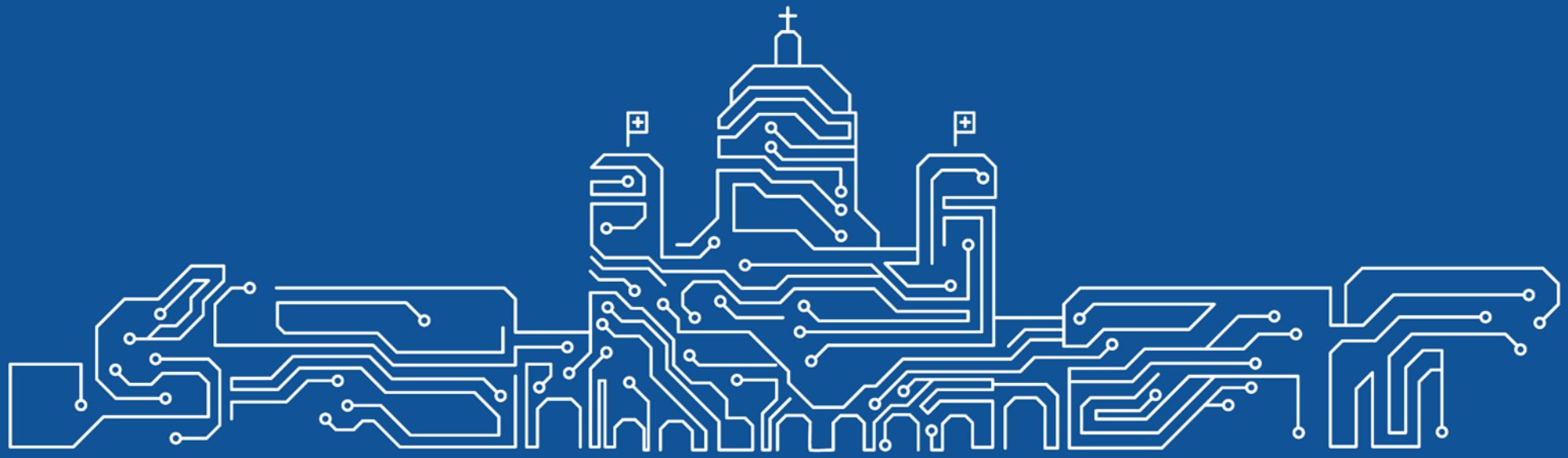
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK
Digitale Transformation und IKT-Lenkung DTI

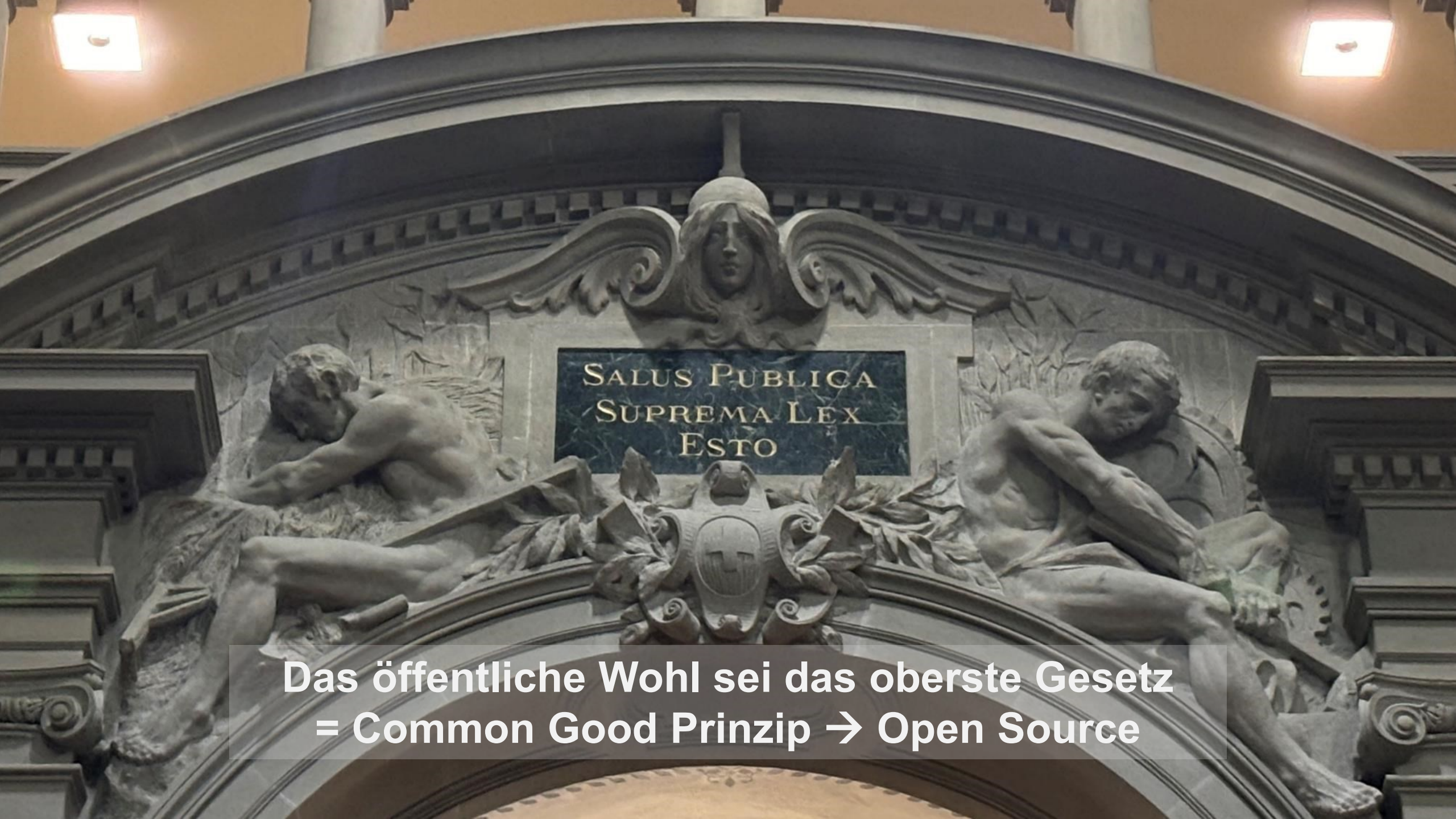
DVS – Cloud und Workplace Tagung Bern vom 19. August 2025

Open Source als ein Pfeiler der Digitalen Souveränität

Bruno Schöb, Unternehmensarchitekt BK




SALUS PUBLICA
SUPREMA LEX
ESTO



Das öffentliche Wohl sei das oberste Gesetz
= Common Good Prinzip → Open Source

Agenda

Es gibt viele Publikationen zum Begriff «digitale Souveränität»

➔ Begriffsklärung notwendig

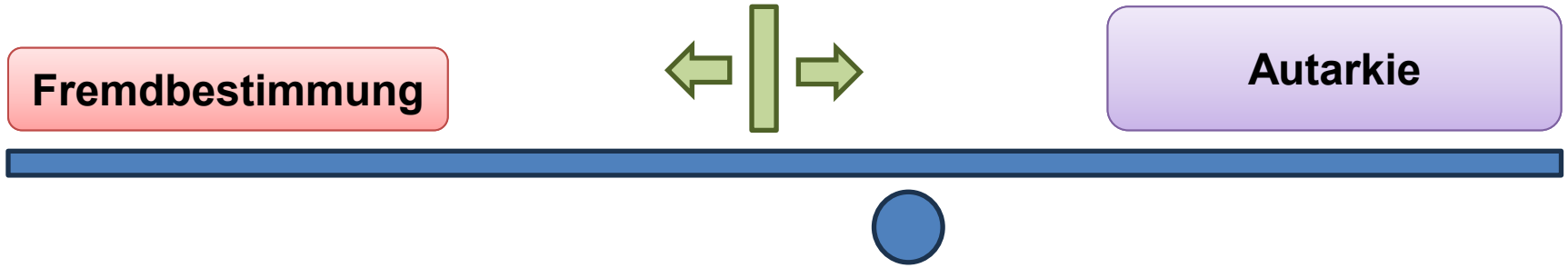
https://www.fondapol.org/app/uploads/2020/06/f-gueham-digital-sovereignty-3.pdf
https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitale-loesungen/eckpunktpapier-digitale-souveraenitaet.pdf?__blob=publicationFile&v=2
https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf
https://digitalautonomy.net/fileadmin/PR/Digitalautonomy/PDF/DAH_Policy_Brief__4_Digitale_Selbstbestimmung.pdf
https://www.acatech.de/publikation/digitale-souveraenitaet-status-quo-und-handlungsfelder/download-pdf?lang=de
https://the-report.cloud/wp-content/uploads/2022/03/CloudReport_2022_01-1.pdf
https://innovate-switzerland.ch/wp-content/uploads/2023/05/Position-Paper-Digitale-Souveranitat-Schweiz.pdf

Technologische Schichten der digitalen Souveränität

Technologisches Schichtenmodell als möglicher Rahmen für die Diskussion spezifischer Herausforderungen für die digitale Souveränität

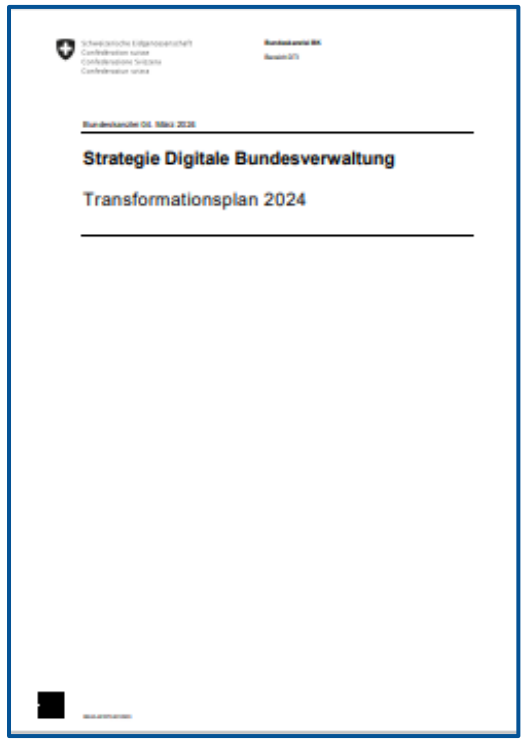
Was ist digitale Souveränität NICHT?

- Digitale Souveränität ≠ Autarkie
- Digitale Souveränität ≠ vollständige digitale Selbstbestimmung
- Digitale Souveränität ≠ totale Datensouveränität
- Digitale Souveränität ≠ vollkommene Autonomie



Die Bundesverwaltung hat heute noch KEINE allgemeingültige Definition.

Aber: Strategie Digitale Bundesverwaltung



https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/digitale-bundesverwaltung.html

https://intranet.dti.bk.admin.ch/dam/isb_kp/de/dokumente/themen/StrategieDigitaleBundesverwaltung/transformationsplan.pdf.download.pdf/Transformationsplan_2024_DE.pdf

Strategie Digitale Bundesverwaltung → Schwerpunkt 4

Vision *Menschen und Unternehmen stehen im Fokus des digitalen Wandels und erhalten einfache, moderne und übergreifende Behördenleistungen des Bundes.*

Prinzipien

Digital by Design | Datengetrieben | Verwaltung als Plattform | Offenheit | Nutzerzentriert | Proaktivität | Sicherheit | Nachhaltigkeit

Strategische Ziele und Schwerpunkte

- Digitale Verwaltung vernetzt denken und gestalten
- Nutzer- und Nutzungsorientierung steigern
- Datennutzung vertrauensvoll aufbauen
- **Digitale Souveränität stärken**
- Innovation und Veränderung erleichtern
- Zeitgemässe Verwaltungsorganisation & Kulturwandel fördern
- Digitale Transformation koordiniert beschleunigen

Nutzen

- Durchgängige Behördenleistungen
- Synergien
- Interoperable Anwendungen & Informationen
- One-Stop-Government
- Nutzerorientierte Behördenleistungen
- Wertschöpfende Datennutzung
- Effiziente Behördeninteraktion (Once-Only)
- Nachvollziehbarkeit Datennutzung
- Gestärkte Strategische Autonomie
- Vertrauen in (Digitale) Verwaltung
- Innovationsfähige Verwaltung
- Veränderungsbereite Verwaltung
- Begleitung, Unterstützung MA
- Attraktive Arbeitgeberin
- Vereinfachte Problemlösung
- Wissensorientierte Verwaltung
- Laufende Kompetenzentwicklung
- Gemeinsames Verständnis & Prioritäten
- Beteiligung Mitarbeitende
- Reaktionsfähige Verwaltung

Messung

- Anzahl API
- Behördenleistungen
  - Verfügbarkeit
  - Zufriedenheit
  - Nutzerfokus
  - Transparenz
- Anzahl OGD
- Umsetzung Once-Only
- Behördenleistungen
  - Vertrauen
- Life-Cycle Management
- Entwicklung Beschaffung
- Anzahl Pilotversuche
- Anträge gem. Vorhaben
- Ranking Attraktivität Studierende
- Mitarbeitende
  - Zufriedenheit
  - Selbsteinschätzung
- Mitarbeitende
  - Einschätzung Org.

Schwerpunkt 4 - Digitale Souveränität stärken

Strategische Ziele

13	Die Bundesverwaltung verpflichtet sich der Förderung der eigenen Entscheidungsfreiheit im Umgang mit digitalen Diensten und setzt sich mit bestehenden Abhängigkeiten auseinander.
14	Die bundesspezifischen Anforderungen an Sicherheit und Verfügbarkeit der Rechenzentren, Netzwerke und Dienstleistungen werden durch die Betreiber erfüllt.
15	Die Bundesverwaltung stellt verwaltungsintern Private und Public Cloud-Dienste zur Verfügung und die Governance für deren Nutzung schafft klare Verantwortlichkeiten.

Nutzenerwartung

- Die Bundesverwaltung gestaltet ihre Entscheidungsfreiheit in strategischen Bereichen der digitalen Bundesverwaltung (digitale Souveränität).
- Bevölkerung, Unternehmen und Behördenpartnerinnen haben Vertrauen in die Bundesverwaltung.

Definition Digitale Souveränität

Digitale Souveränität bedeutet für Individuen und Institutionen über Fähigkeiten und Möglichkeiten zu verfügen, ihre Rollen in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können.

Quelle: Dirk Schrödter, Digitalisierungsminister Schleswig-Holstein

angelehnt an «Eckpunktepapier Digitale Souveränität» CIO Bund BRD

Als Arbeitsversion soll folgende Kurzdefinition gelten:

Digitale Souveränität bedeutet, über Kontroll- und Handlungsfähigkeit im digitalen Raum zu verfügen, um die Erfüllung staatlicher Aufgaben sicherzustellen.

Bedeutung von Digitaler Souveränität – aktueller denn je

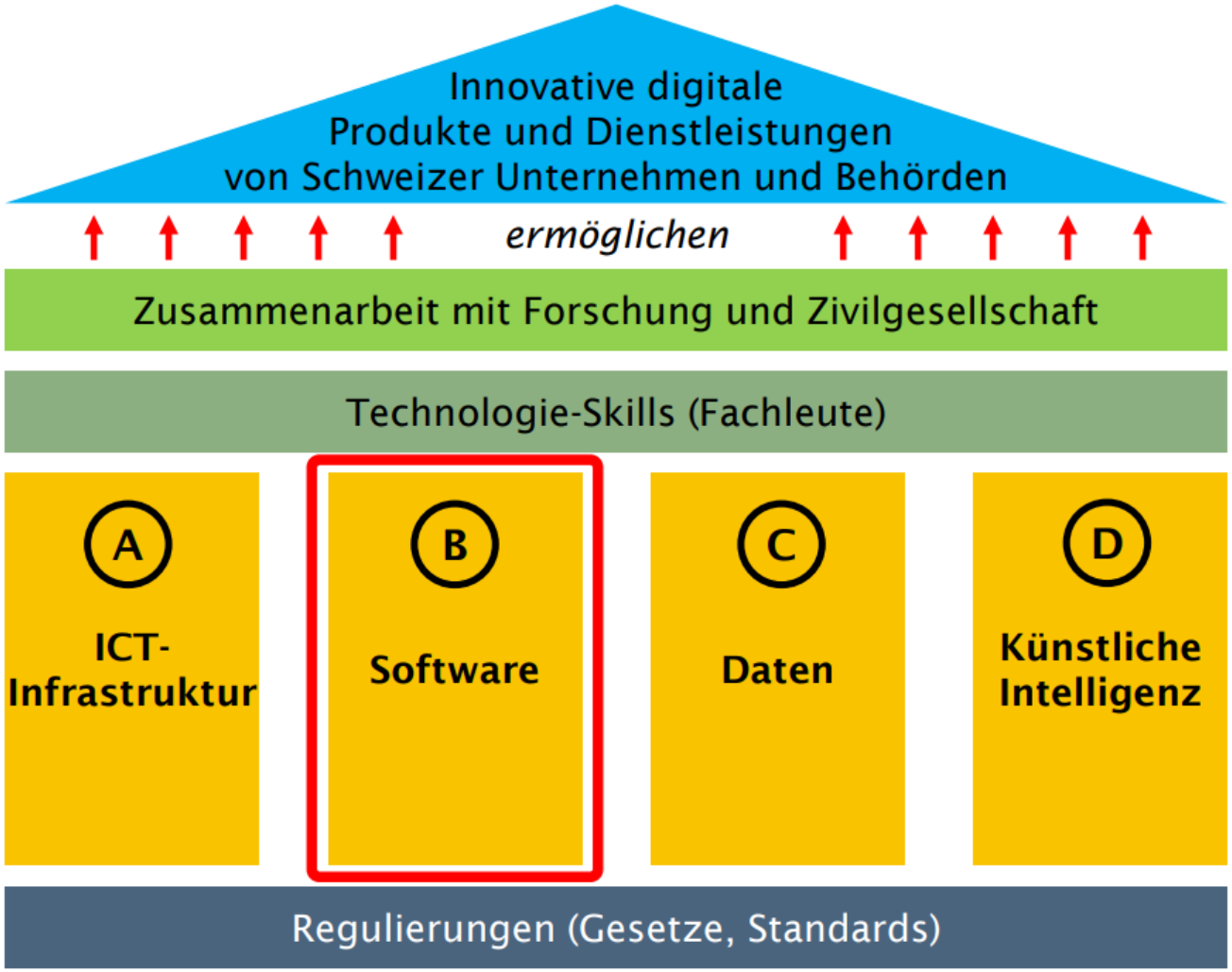
Die IT der Verwaltung ist zu einem geschäftskritischen Teil geworden und deren Funktionsfähigkeit systemrelevant.

Digitale Souveränität ist mindestens so wichtig wie die Energiesouveränität.

Dirk Schrödter, Digitalisierungsminister Schleswig-Holstein

➔ Abhängigkeiten bewusst managen

4 Handlungsfelder für digitale Souveränität (gemäss BFH)



Quelle: Studie BFH für das EDA «Technologische Perspektiven der digitalen Souveränität» (Stürmer)

Digitale Souveränität durch Vielfalt

Die Unabhängigkeit von einzelnen IT-Anbietern und damit die Sicherstellung der digitalen Souveränität wird durch eine vielfältige Anbieterlandschaft und offene Standards gewährleistet.

➔ **Es gilt die Herausforderung mit proprietärer und quelloffener Software zu adressieren**

Digitale Souveränität bei Software stärken

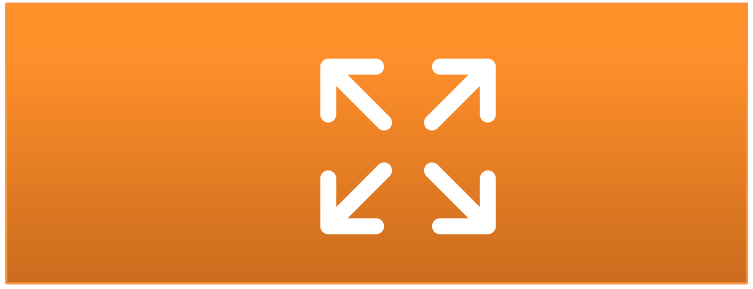
Dimensionen von digitaler Souveränität - drei Rollen der Öffentlichen Verwaltung

Wechselfähigkeit

Die *Öffentliche Verwaltung* kann als **Nutzerin** frei zwischen Anbietern und Technologien wählen.

Gestaltungsfähigkeit

Die *Öffentliche Verwaltung* kann als **Bereitstellerin** IT eigenständig gestalten.



Einflussnahme

Die *Öffentliche Verwaltung* kann als **Auftraggeberin** die eigenen Anforderungen gegenüber Anbietern kommunizieren.

Digitale Souveränität bei Software stärken

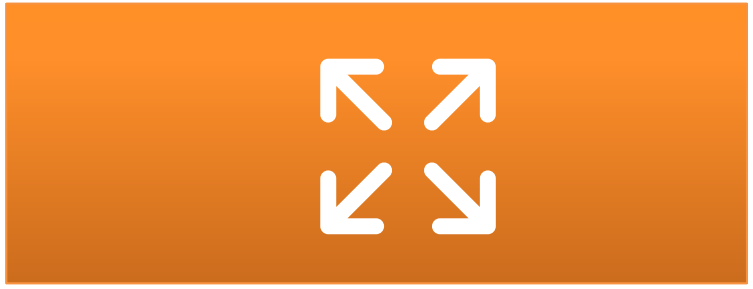
Dimensionen von digitaler Souveränität - drei Rollen der Öffentlichen Verwaltung

Wechselfähigkeit

Die *Öffentliche Verwaltung* kann als **Nutzerin** frei zwischen Anbietern und Technologien wählen.

Gestaltungsfähigkeit

Die *Öffentliche Verwaltung* kann als **Bereitstellerin** IT eigenständig gestalten.



Einflussnahme

Die *Öffentliche Verwaltung* kann als **Auftraggeberin** die eigenen Anforderungen gegenüber Anbietern kommunizieren.

➔ **Open Standards und Open Source Software unterstützen diese Ziele optimal**

Fazit

Open Source Prinzipen

mit

Open Standards

und

Open Source Software

sind wichtig für die

digitale Souveränität

Mit der aktuellen Strategie Digitale Schweiz 2025 wird der Einsatz von Open Source Software in der Bundesverwaltung gefördert

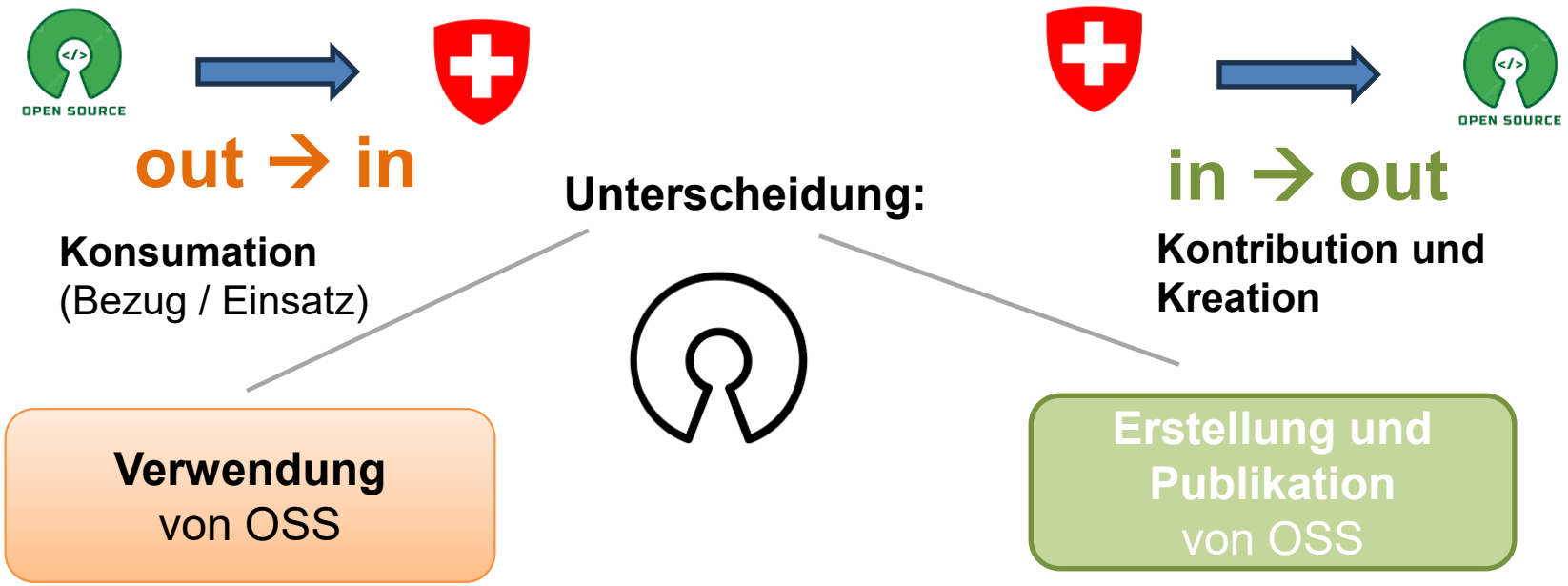
Out ➔ In (Bezug/Verwendung):

Abhängigkeit von kommerziellen Anbietern reduzieren

In ➔ Out (Publikation):

Bund stellt eigene Entwicklungen als Open Source zur Verfügung

Artikel 9 EMBAG regelt nur in → out



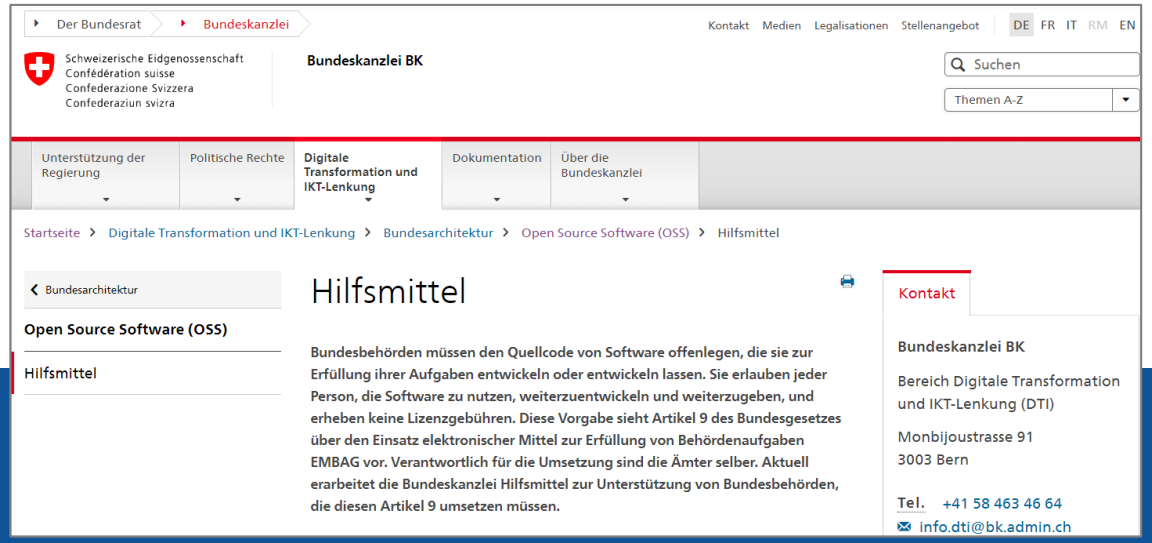
→ *nicht* im EMBAG geregelt
→ ist ein **Beschaffungsthema**
(hier gibt es keinen OSS Vorrang
- Grundsatz der Gleichbehandlung)

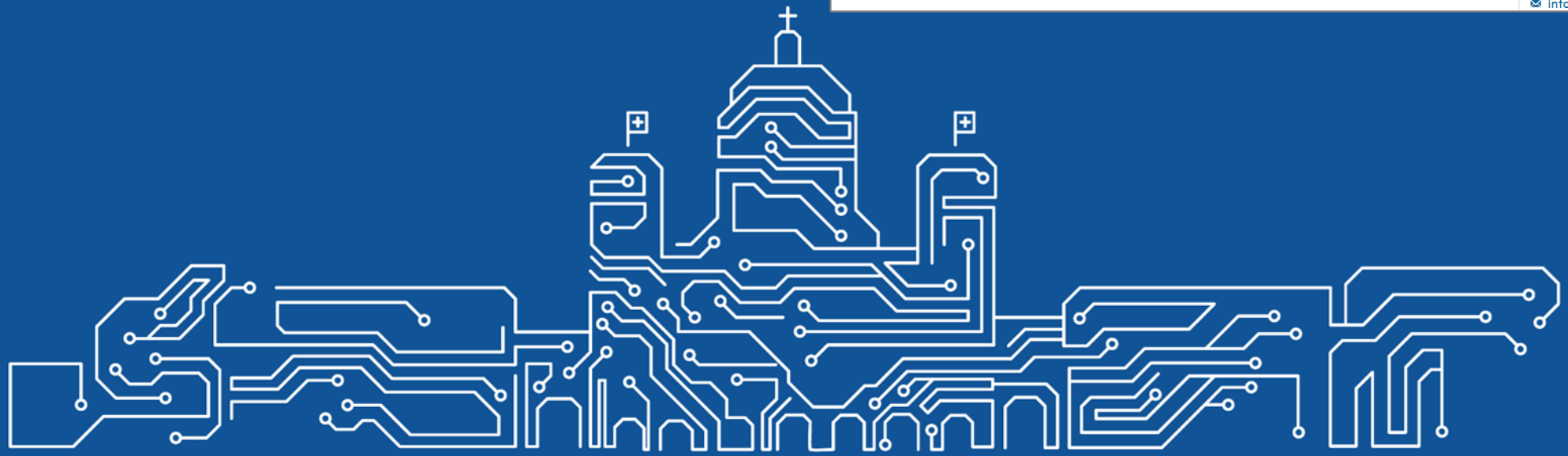
→ **Art. 9 EMBAG**

Aber Achtung: bei der SW Produktion werden oft **OSS Libraries** verwendet
Thema: Lizenzkompatibilität

EMBAG: Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben

3. OSS-Hilfsmittel Version 2.0





Was ist das EMBAG?

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

BBl 2023
www.fedlex.admin.ch
Massgebend ist die signierte elektronische Fassung

Ablauf der Referendumsfrist: 6. Juli 2023

Bundesgesetz
über den Einsatz elektronischer Mittel
zur Erfüllung von Behördenaufgaben
(EMBAG)

vom 17. März 2023

Die Bundesversammlung der Schweizerischen Eidgenossenschaft,
gestützt auf Artikel 173 Absatz 2 der Bundesverfassung[1],
nach Einsicht in die Botschaft des Bundesrates vom 4. März 2022[2],
beschliesst:

Art. 1 Zweck

Dieses Gesetz soll die Voraussetzungen schaffen für:

a. die Zusammenarbeit unter Behörden verschiedener Gemeinwesen und mit Dritten beim Einsatz elektronischer Mittel zur Unterstützung der Erfüllung von Behördenaufgaben;

b. den Ausbau und die Weiterentwicklung des Einsatzes von elektronischen Mitteln zur Unterstützung der Erfüllung von Behördenaufgaben.

Art. 2 Geltungsbereich

[1] Dieses Gesetz gilt für die zentrale Bundesverwaltung.

[2] Es gilt auch für Einheiten der dezentralen Bundesverwaltung. Der Bundesrat kann Ausnahmen vorsehen.

[3] Die Parlamentsdienste, die eidgenössischen Gerichte und die Bundesanwaltschaft können sich diesem Gesetz oder Teilen davon durch Vereinbarung mit dem Bundesrat unterstellen.

1 SR **101**
2 BBl **2022** 804

2023-0825 BBl 2023 787

➔ Bundesgesetz gültig ab 1.1.2024

EMBAG

Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben

Einführung

Art 1 Zweck → Voraussetzung schaffen für *elektronische Zusammenarbeit* unter Behörden und Dritten
Ausbau und Weiterentwicklung IKT
Art 2 Geltungsbereich → zentrale Bundesverwaltung / z.T. dezentrale BV

Tallinn Prinzipien

Einsatz von IKT-Mitteln und Infrastruktur Elementen

Standardmässig Digital
Inklusivität /Zugänglichkeit
Art 3 Grundlagen
→ Digital first Prinzip

Einmalige Eingabe
Art 11 Bereitstellung und Nutzung von IKT Mitteln des Bundes
→ Once only Prinzip

Vertrauenswürdigekeit
Sicherheit
Art 15 Pilotversuche
→ mindert Risiken

Offenheit
Transparenz
Art 9 Open Source Software
Art 10 Open Government Data

Standardmässige
Interoperäbilität
Art 12 Standards
Art 13 Schnittstellen
Art 14 Interoperabilitätsplattform

Nutzen für Bevölkerung

Finanzierung

Art 6 Kostentragen bei Vereinbarungen
Art 7 Finanzhilfen
Art 16 Anschubfinanzierung Infrastrukturen + Basisdienste
Art 17 Anschubfinanzierung Digitalisierungsprojekte

Zusammenarbeit

Art 4 Abschluss von Vereinbarungen
Art 5 Beteiligung des Bundes an Organisationen (→ z.B. eOperations, DVS,....)
Art 8 Übertragung von Aufgaben der administrativen Hilfstätigkeit

Nutzen / Effekte

Schafft Rechtssicherheit für:

Digitale Verwaltung Schweiz
Administration numérique suisse
Amministrazione digitale Svizzera

eOperations Schweiz Suisse Svizzera

eCH E-Government Standards

Pilotversuche +
Gesetzentwicklung parallel
(wie z.B E-ID)

Bund als Leistungs-
erbringer für qualifizierte Dritte
(wie z.B Swiss Gov PKI)

Zur Umsetzung von:

- AGOV (Authentifizierungportal für Behörden)
- BTB (Bundes Trust Broker) als OSS
- SGC (Swiss Government Cloud) für Dritte
- OpenGovCode.ch
-

Neue gesetzliche Grundlage im EMBAG

➔ Der Bund darf nicht nur, nein er MUSS

Art. 9 Open Source Software

1 Die diesem Gesetz unterstehenden Bundesbehörden legen den Quellcode von Software offen, die sie zur Erfüllung ihrer Aufgaben entwickeln oder entwickeln lassen, es sei denn die Rechte Dritter oder sicherheitsrelevante Gründe würden dies ausschliessen oder einschränken.

2 Sie erlauben jeder Person, die Software zu nutzen, weiterzuentwickeln und weiterzugeben, und erheben keine Lizenzgebühren.

3 Die Rechte nach Absatz 2 werden in der Form von privatrechtlichen Lizenzen erteilt, soweit andere Erlasse nichts Abweichendes vorschreiben. Streitigkeiten zwischen den Lizenzgebern und den Lizenznehmern werden zivilrechtlich beurteilt.

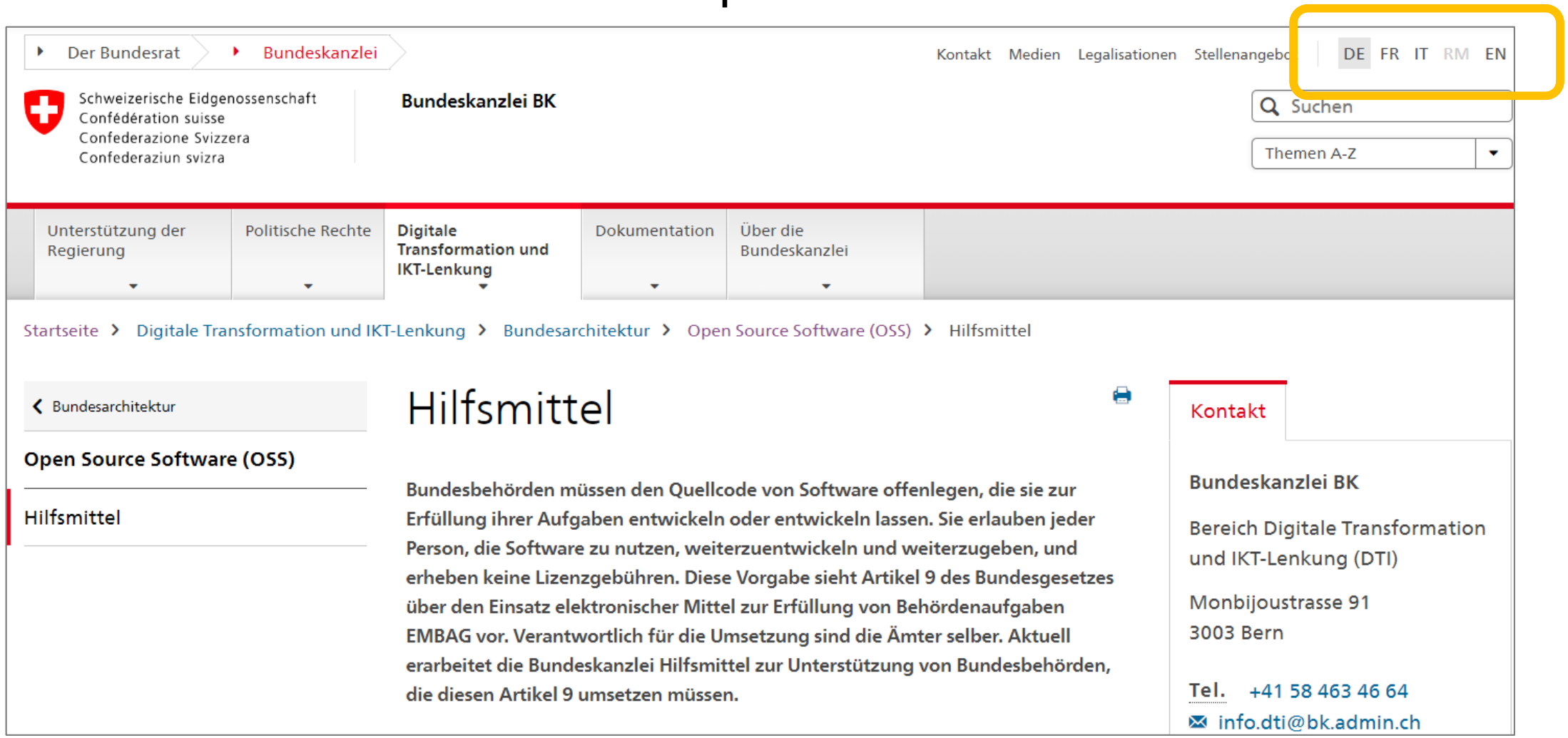
4 Soweit möglich und sinnvoll sind international etablierte Lizenztexte zu verwenden. Haftungsansprüche von Lizenznehmern sind auszuschliessen, soweit dies rechtlich möglich ist.

5 Die diesem Gesetz unterstehenden Bundesbehörden können ergänzende Dienstleistungen, insbesondere zur Integration, Wartung, Gewährleistung der Informationssicherheit und zum Support erbringen, soweit die Dienstleistungen der Erfüllung von Behördenaufgaben dienen und mit verhältnismässigem Aufwand erbracht werden können.

6 Sie verlangen für die ergänzenden Dienstleistungen ein kostendeckendes Entgelt. Das zuständige Departement kann für bestimmte Leistungen Ausnahmen zulassen, wenn dadurch die Privatwirtschaft nicht konkurrenziert wird.

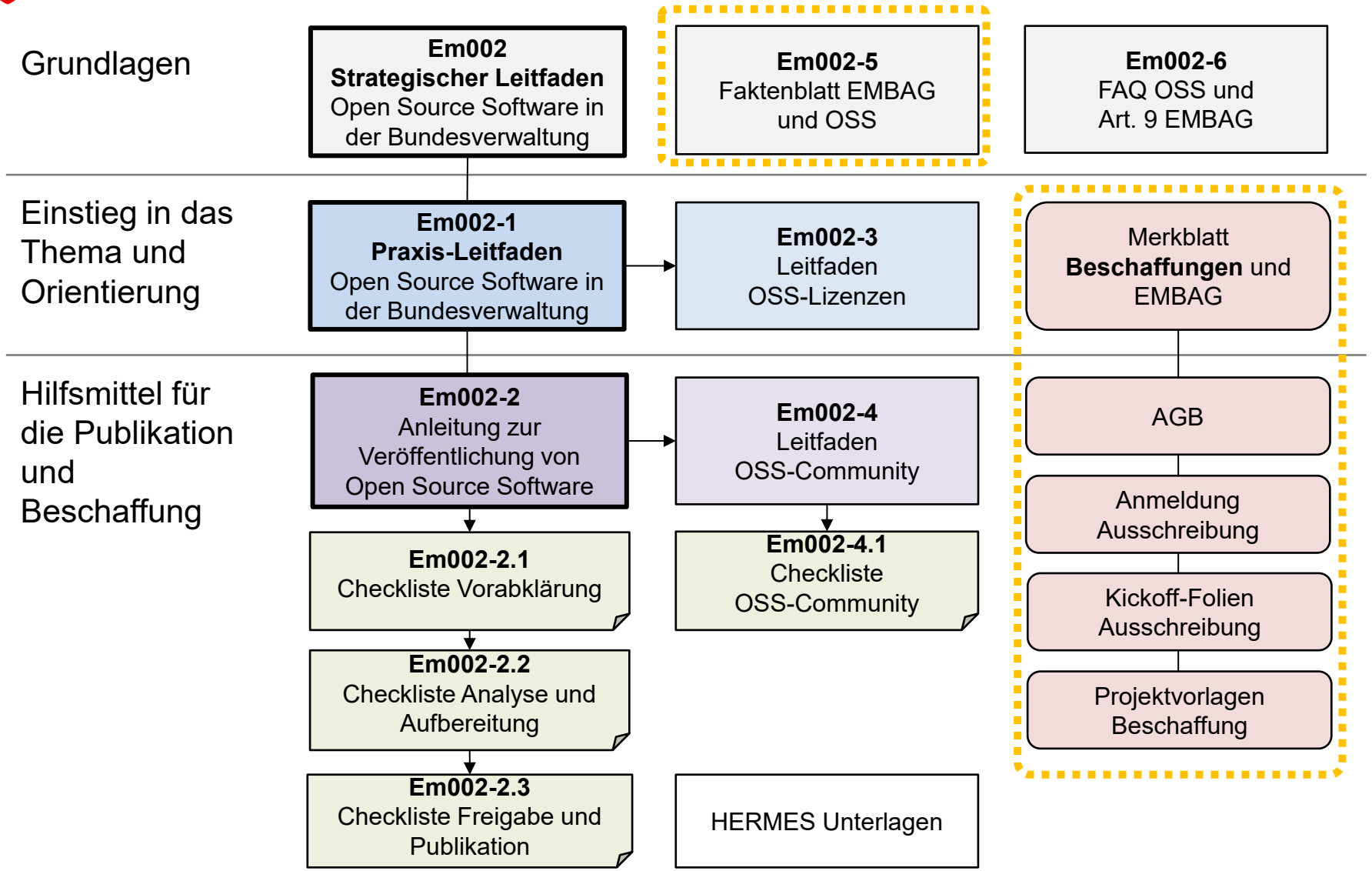
EMBAG: Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben

Die Hilfsmittel sind im Internet publiziert



[Hilfsmittel (admin.ch)]
https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/bundesarchitektur/open_source_software/hilfsmittel_oss.html

Überblick OSS-Hilfsmittel (Version 1.0)



Legende

grau	Grundlagen
blau	Einstieg in das Thema OSS
violett	Publikation von OSS
grün	Checklisten (.docx)
rot	Beschaffung

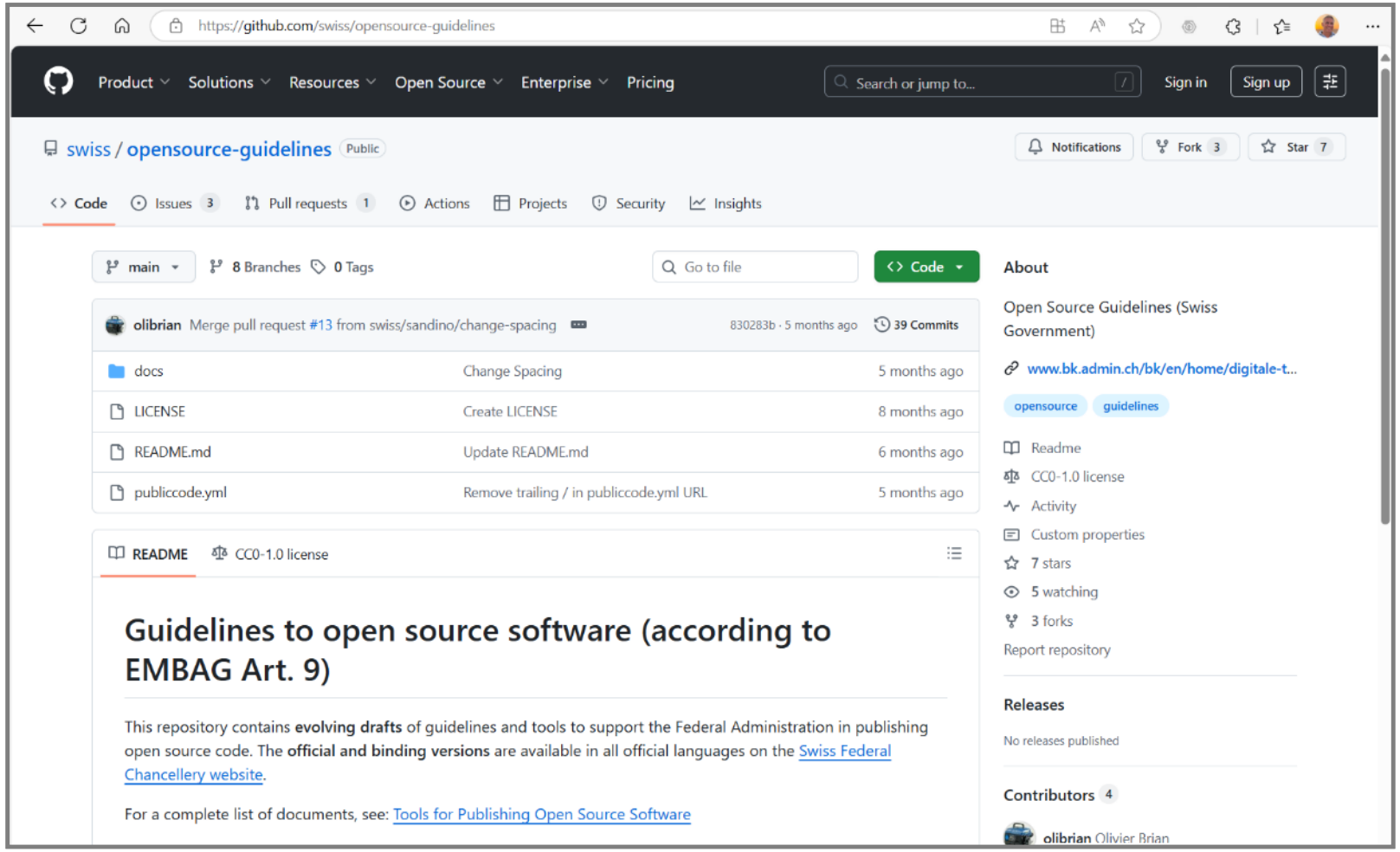
Verantwortung DTI

Verantwortung BBL

11 Dokumente
von DTI mit über
140 Seiten

Version 1.0

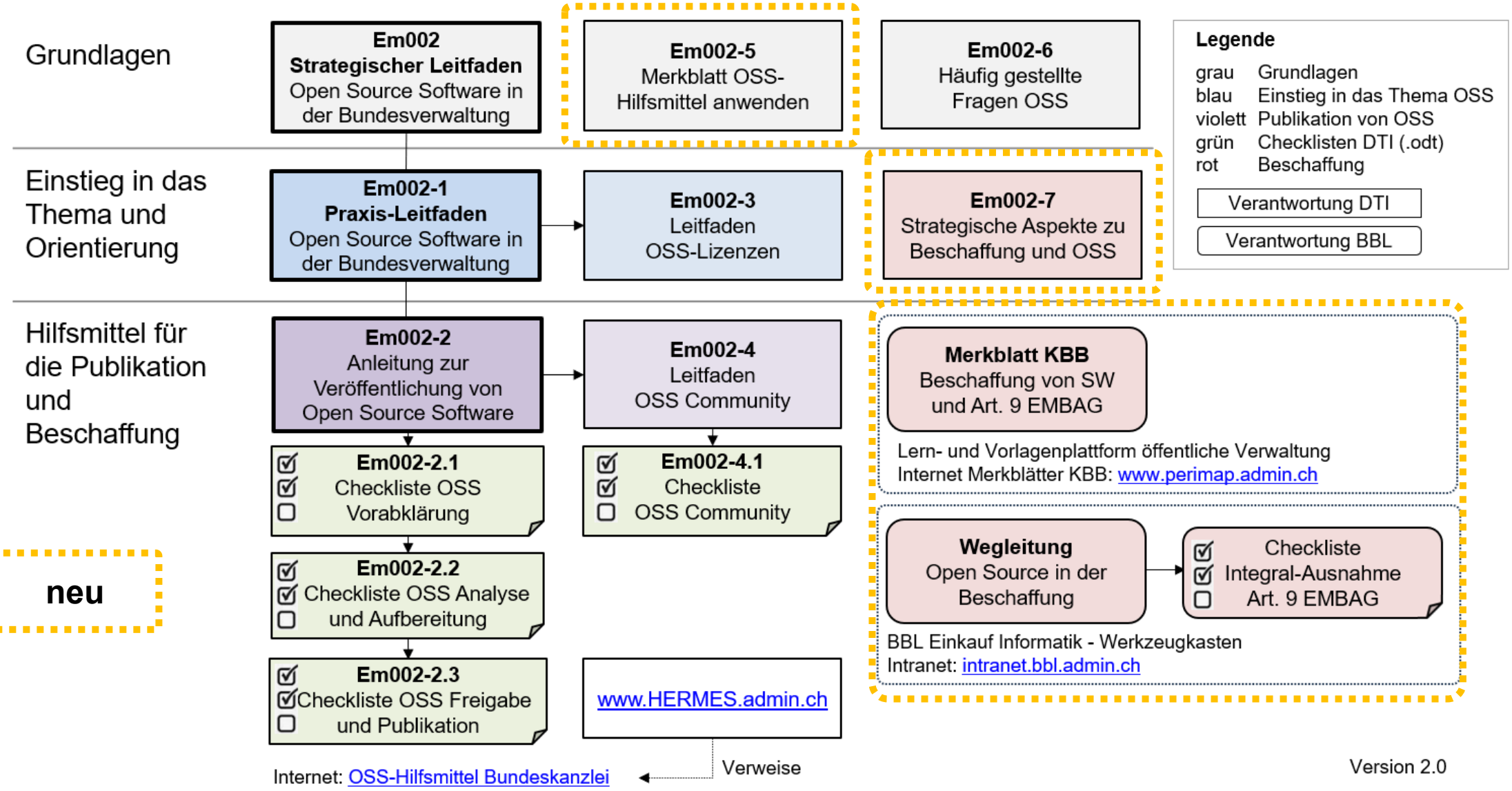
Open Source Hilfsmittel auf Github (Guidelines)



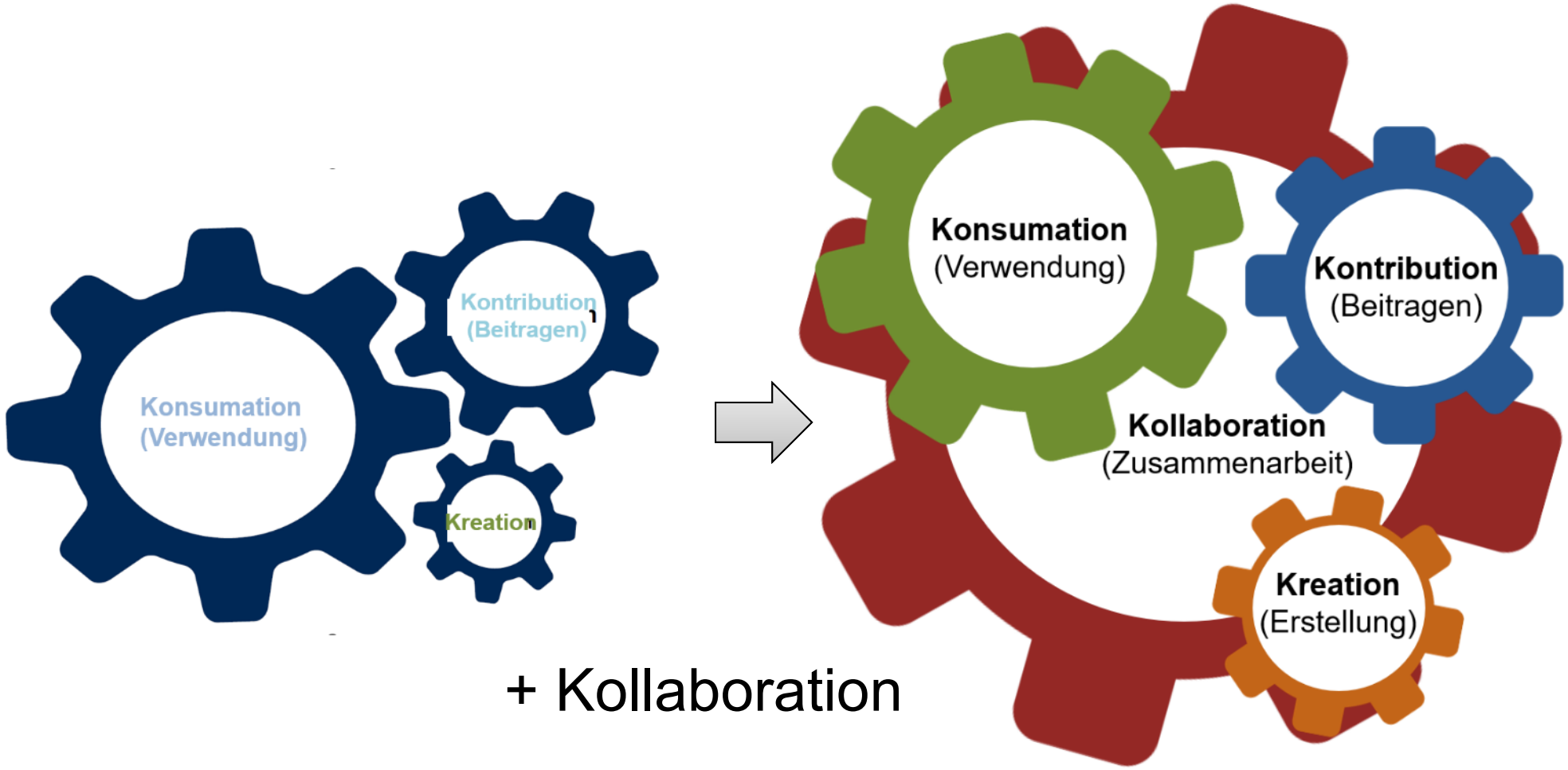
➔ es gibt einen Feedback-Kanal

[GitHub - swiss/opensource-guidelines: Open Source Guidelines (Swiss Government)]

Übersicht OSS-Hilfsmittel Version 2.0



Open Source Governance – aus 3 K werden 4 K



+ Kollaboration

➔ Open Source funktioniert ohne Zusammenarbeitskultur nicht

Neu: Merkblatt OSS-Hilfsmittel anwenden (Em002-5)

→ Einstieg für Projektleitende und Projektbeteiligte

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK
Digitale Transformation und IKT-Lenkung DTI

Merkblatt:
OSS Artikel 9 EMBAG anwenden

Seit dem 1. Januar 2024 ist das neue Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBAG) in Kraft. Es schreibt vor, dass die Bundesbehörden den Quellcode von Software offenlegen, die sie entwickeln oder entwickeln lassen. Ausnahmen sind möglich, wenn die Rechte Dritter oder sicherheitsrelevante Gründe dies ausschliessen oder einschränken.

Dieses Dokument gibt Projektleitenden oder anderen für die Beschaffung von Software verantwortlichen Personen eine Hilfestellung.

Einstiegsfragen:

Beschafft oder verwendet die Bundesbehörde eine Standardsoftware ohne Anpassungen?
→ Wenn ja, siehe a)

oder

Muss eine Software-Anwendung oder eine Komponente eigens für den Bund entwickelt werden (Individualsoftware = Make)?
→ Wenn ja, siehe b)

a) Beschaffung und Verwendung von Standard-Software

Wenn der Bund Software ohne Anpassungen einkauft, gilt Artikel 9 EMBAG nicht. Es steht jeder Bundesbehörde frei, ob sie Open Source oder eine andere Software beschafft und verwendet. Hilfestellungen für die Beschaffung von Software bietet die Internetseite des Bundesamtes für Bauten und Logistik (BBL) und das *Merkblatt Beschaffung von Software und Art. 9 EMBAG* des KBB. Allenfalls kann auch *Em002-7 Strategische Aspekte zu Beschaffung und OSS* konsultiert werden.

b) Kreation oder Weiterentwicklung von Software

Entwickelt eine Bundesbehörde Software selbst oder durch Dritte, muss OSS Artikel 9 EMBAG angewendet werden. Darunter fällt auch Software, welche im Rahmen einer Kontribution in bestehenden OSS Projekten weiterentwickelt wird. Einer Veröffentlichung von Quellcode stehen nur Rechte Dritter oder sicherheitsrelevante Gründe entgegen.
Füllen Sie dazu die *Checkliste Em002-2.1 OSS Vorabklärung* aus.

Hinweis: Diese Checkliste dient auch als Begründung, weshalb Software nicht veröffentlicht werden muss. Sie sollte daher möglichst früh im Projekt beigezogen werden. Im Leitfaden *Em002-2* ist der ganze Prozess beschrieben.

Weitere zu klärende Fragen sind:

- **Unter welcher Open Source Lizenz wird veröffentlicht?**

  Die Grundsatzfrage, ob die Software unter einer Copyleft Lizenz (dann ist z.B. AGPL V3 eine gute Wahl) oder permissiv veröffentlicht wird (dann z.B. unter MIT-Lizenz), muss beantwortet werden. Bezüglich Lizenzwahl gibt der *Leitfaden Em002-3 OSS-Lizenzen* vertieft Auskunft.
  Füllen Sie dazu die *Checkliste Em002-2.2 OSS Analyse und Aufbereitung* aus.

  Hinweis: Diese ist idealerweise durch den (technischen) Projektleitenden oder IT-Architekten auszufüllen.

- **Wo und wie soll die Software und alle dazugehörenden Artefakte publiziert werden?**

  Füllen Sie dazu die *Checkliste Em002-2.3 OSS Freigabe und Publikation* aus.

  Hinweis: Hier wird gesammelt festgehalten, wo und wie Software publiziert wird. Unter Umständen braucht es die Involvierung weiterer Stellen.

- **Soll eine OSS-Community aufgebaut werden?**

  Im *Leitfaden Em002-4 OSS Community* sind die Vorteile und Aufgaben für einen Aufbau einer OSS-Community anhand eines Konzeptes beschrieben.

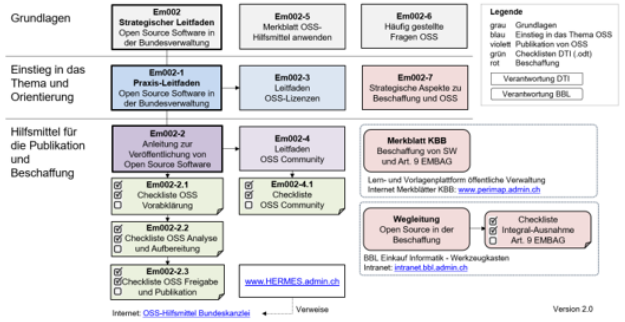
  Falls ja: Füllen Sie die *Checkliste Em002-4.1 OSS Community* aus, die Auskunft über die gewünschte Art und Plattform für die Community gibt.

  Hinweis: Das Projektteam hat hier grossen Spielraum, ob und welche Art der Community geschaffen werden soll. Unter Umständen braucht es hier die Involvierung weiterer Stellen.

Beantworten Sie diese Fragen und prüfen Sie regelmässig (ca. 1x pro Jahr), ob sich wesentliche Änderungen ergeben haben.

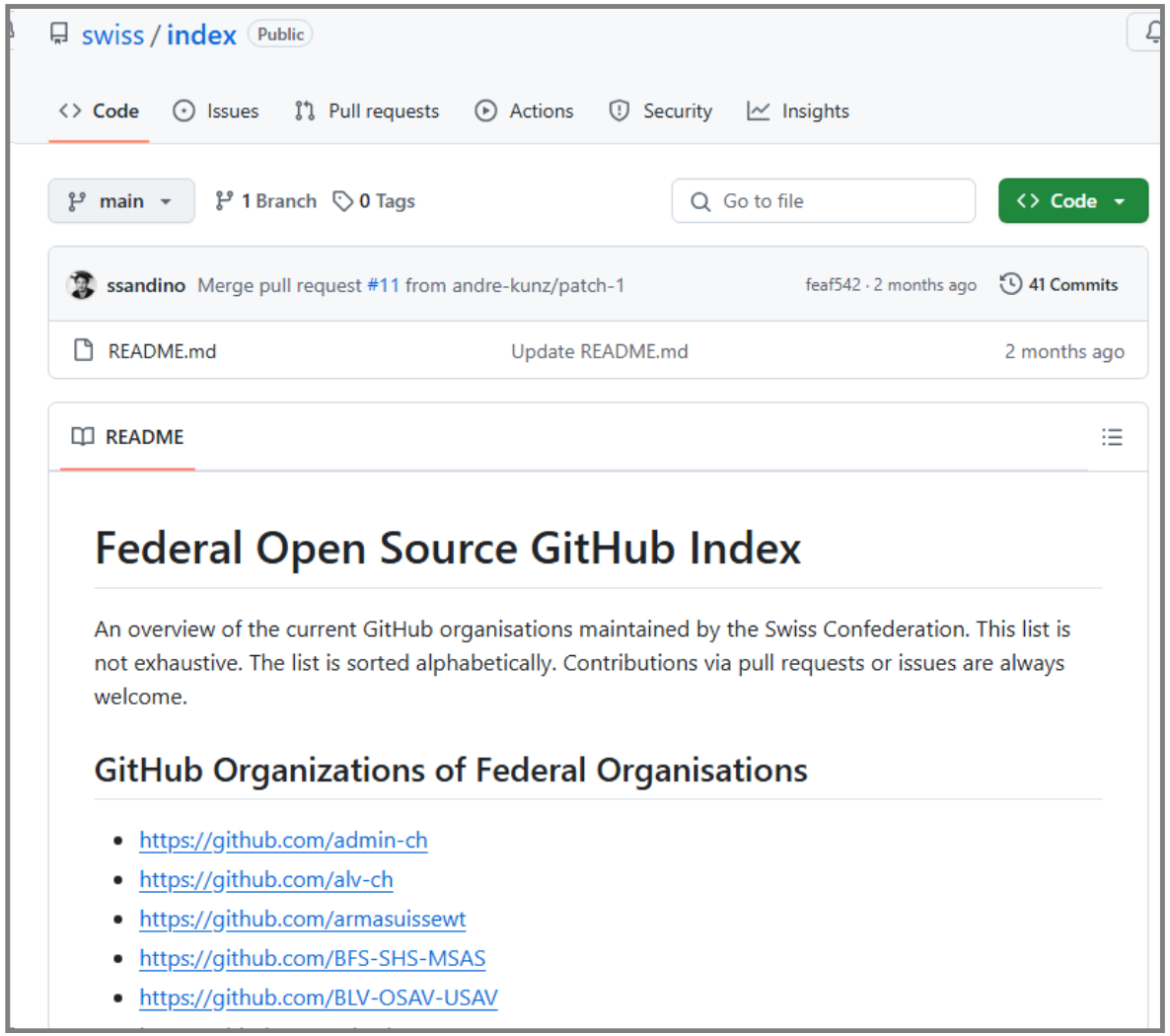
Jede Bundesbehörde (z.B. Amt, Verwaltungseinheit), welche Software entwickelt oder entwickeln lässt, ist selbständig für die Veröffentlichung verantwortlich.

Übersicht Hilfsmittel



Die Hilfsmittel sind veröffentlicht auf der Webseite der Bundeskanzlei OSS-Hilfsmittel. Sie sind zudem in Englisch auf Github publiziert, wo Sie direkt Feedback geben können. Bei Fragen wenden Sie sich an: opensource@bk.admin.ch.

Bundes Open Source Auflistung auf github

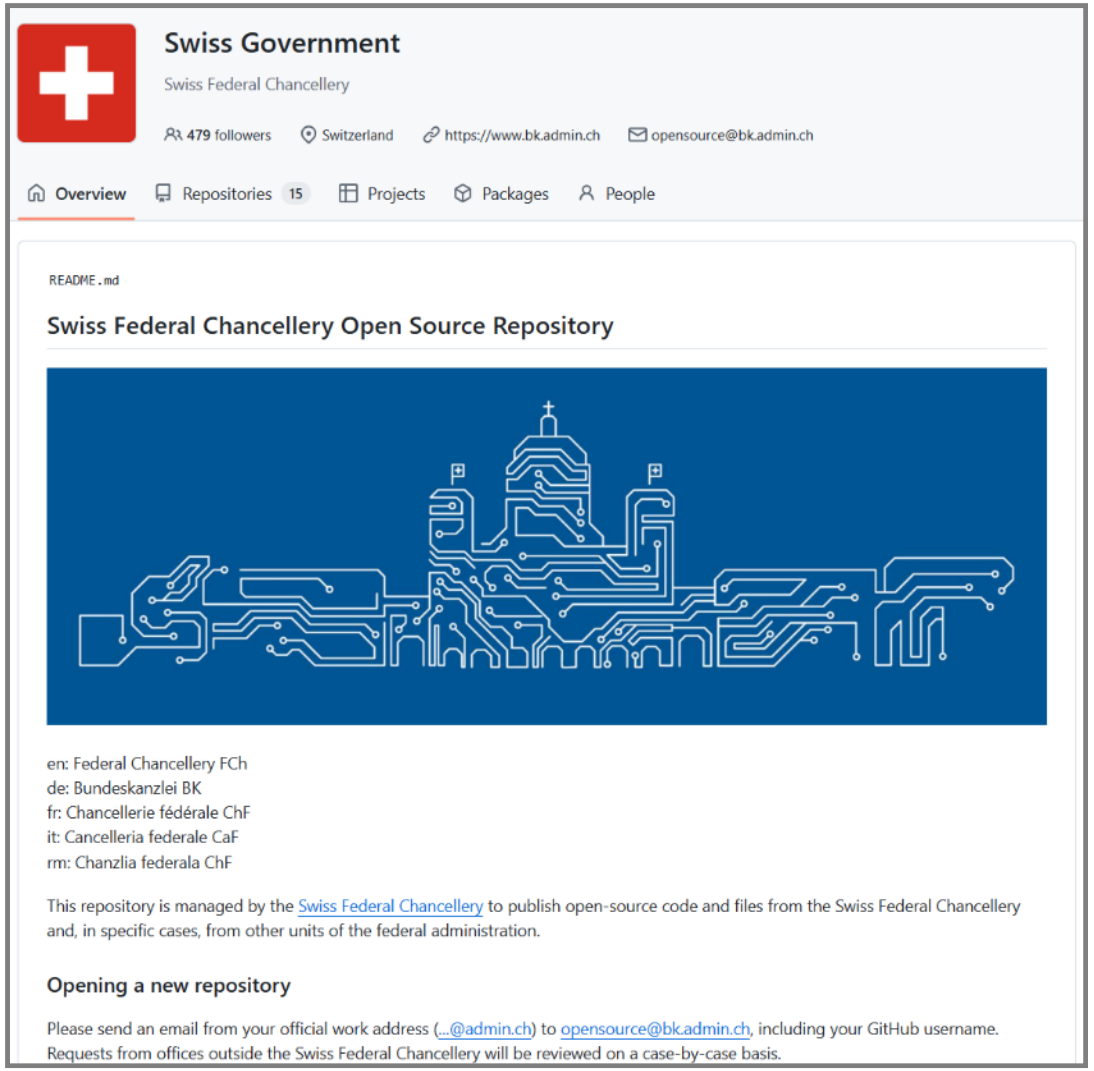


➔ Alle Publikationen aufgeführt, welche DTI bekannt sind

➔ Aufruf an die Bundesveraltung: Meldet uns Publikationen auf *opensource@bk.admin.ch*

https://github.com/swiss/index

Zentrales Swiss Government Repo auf github



➔ Die Bundeskanzlei hat ein zentrales Repository auf github aufgeschaltet

➔ Bundesbehörden können hier ihre eigenen Projekte publizieren

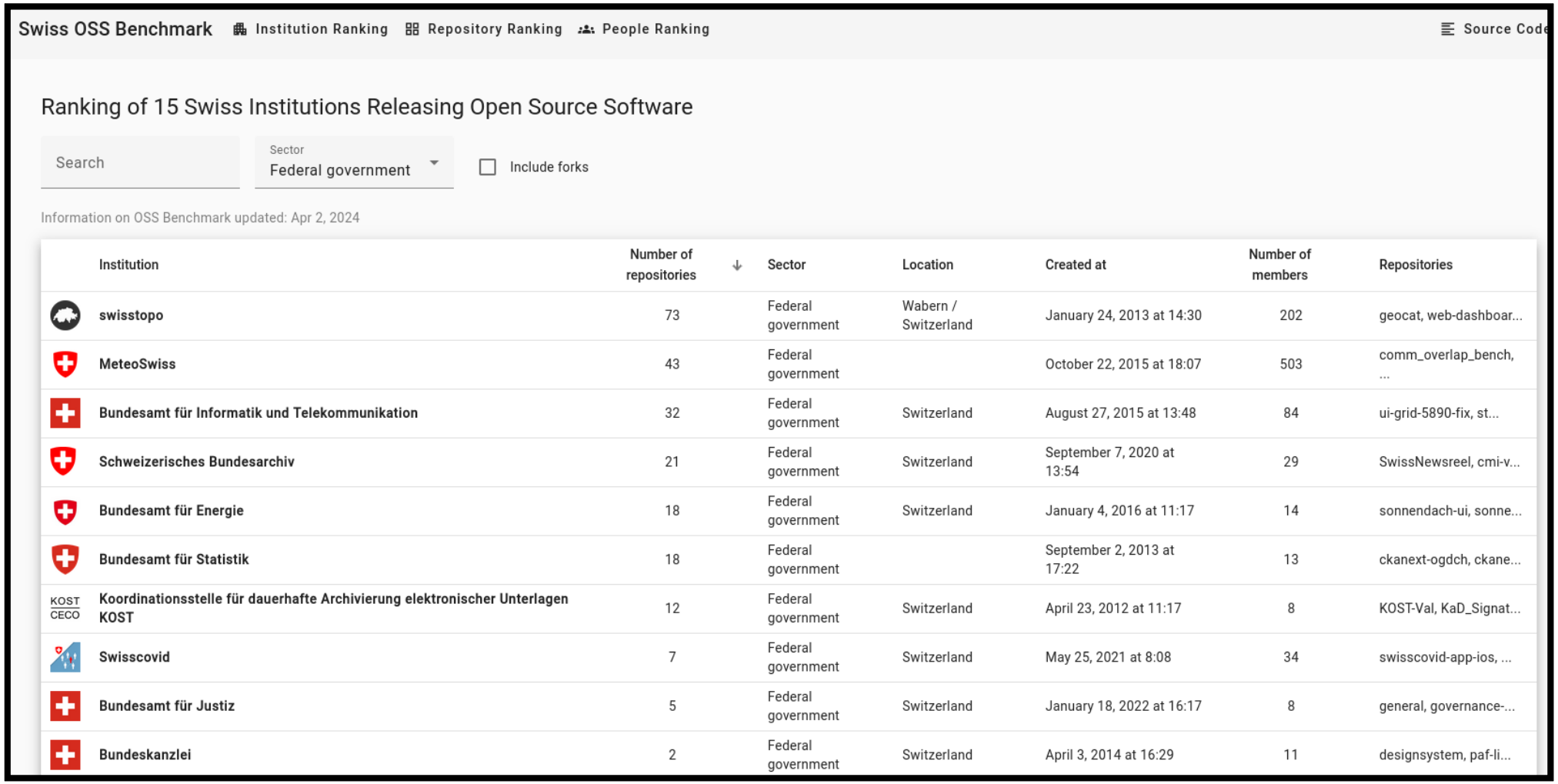
➔ Empfehlung (freiwillig)

➔ evtl. Übergangslösung bis eigene Instanz aufgebaut wird

➔ Kontakt via *opensource@bk.admin.ch*

https://github.com/swiss

Weitere Übersicht Open Source beim Bund



Swiss OSS Benchmark | Institution Ranking | Repository Ranking | People Ranking | Source Code

Ranking of 15 Swiss Institutions Releasing Open Source Software

Search | Sector: Federal government | Include forks

Information on OSS Benchmark updated: Apr 2, 2024

Institution	Number of repositories	Sector	Location	Created at	Number of members	Repositories
swisstopo	73	Federal government	Wabern / Switzerland	January 24, 2013 at 14:30	202	geocat, web-dashboar...
MeteoSwiss	43	Federal government		October 22, 2015 at 18:07	503	comm_overlap_bench, ...
Bundesamt für Informatik und Telekommunikation	32	Federal government	Switzerland	August 27, 2015 at 13:48	84	ui-grid-5890-fix, st...
Schweizerisches Bundesarchiv	21	Federal government	Switzerland	September 7, 2020 at 13:54	29	SwissNewsreel, cmi-v...
Bundesamt für Energie	18	Federal government	Switzerland	January 4, 2016 at 11:17	14	sonnendach-ui, sonne...
Bundesamt für Statistik	18	Federal government		September 2, 2013 at 17:22	13	ckanext-ogdch, ckane...
Koordinationsstelle für dauerhafte Archivierung elektronischer Unterlagen KOST	12	Federal government	Switzerland	April 23, 2012 at 11:17	8	KOST-Val, KaD_Signat...
Swisscovid	7	Federal government	Switzerland	May 25, 2021 at 8:08	34	swisscovid-app-ios, ...
Bundesamt für Justiz	5	Federal government	Switzerland	January 18, 2022 at 16:17	8	general, governance-...
Bundeskanzlei	2	Federal government	Switzerland	April 3, 2014 at 16:29	11	designsystem, paf-li...

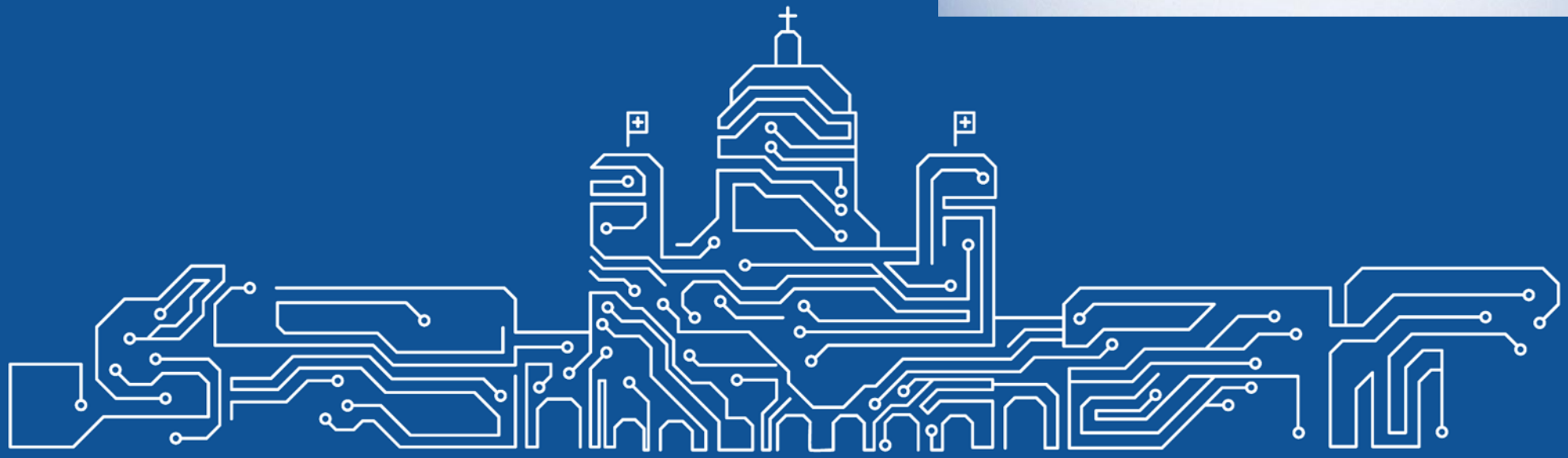
Quelle: https://ossbenchmark.com/

Zusammenfassung: Weiterentwicklung der Hilfsmittel

Immer noch PDF, aber es gibt eine englische Markdown Version auf Github

Faktenblatt durch Merkblatt OSS ersetzt	Kurze Hilfestellung für projekt- oder beschaffungsverantwortliche Mitarbeitende
OSS-Hilfsmittel V1.0	Jetzt auch auf Französisch, Englisch und Italienisch verfügbar
OSS-Hilfsmittel V1.0 auf GitHub	Neu auf Englisch veröffentlicht und offen für Community-Inputs
OSS-Hilfsmittel V2.0	Gesammelte Inputs – direkt und via GitHub – verarbeitet (es gibt aber immer noch Pendenzen (z.B. CLA, Art. 9 Ziff. 5 + 6) Checklisten nun im **.odt Format** **Publicode.yml** (inkl. Editor)
Meta-Verzeichnis	**Wer hat was veröffentlicht?** → Eine Übersicht aller dem DTI bekannten OSS-Publikationen des Bundes gibt es hier. Prüfung Publikation auf Plattfrom i14y.ch
Beschaffungsthemen	Merkblätter KBB und BBL erstellt (→ in Verantwortung BBL)
HERMES Projektmanagement	Einbau Verweise in HERMES

3. Digitale Souveränität und Beschaffung



Neu Em002-7 Strategische Aspekte zu Beschaffung und OSS

Grundsatz: OSS ist gleichberechtigt zu proprietärer Software zu behandeln.

➔ aber: in der Praxis meist Entscheidung für proprietäre Produkte

In einer Ausschreibung darf OSS gefordert werden, wenn strategische Anforderungen bestehen.

➔ **Digitale Souveränität kann so eine Anforderung sein.**

➔ **Wie kann der Grad der digitalen Souveränität gemessen werden?**

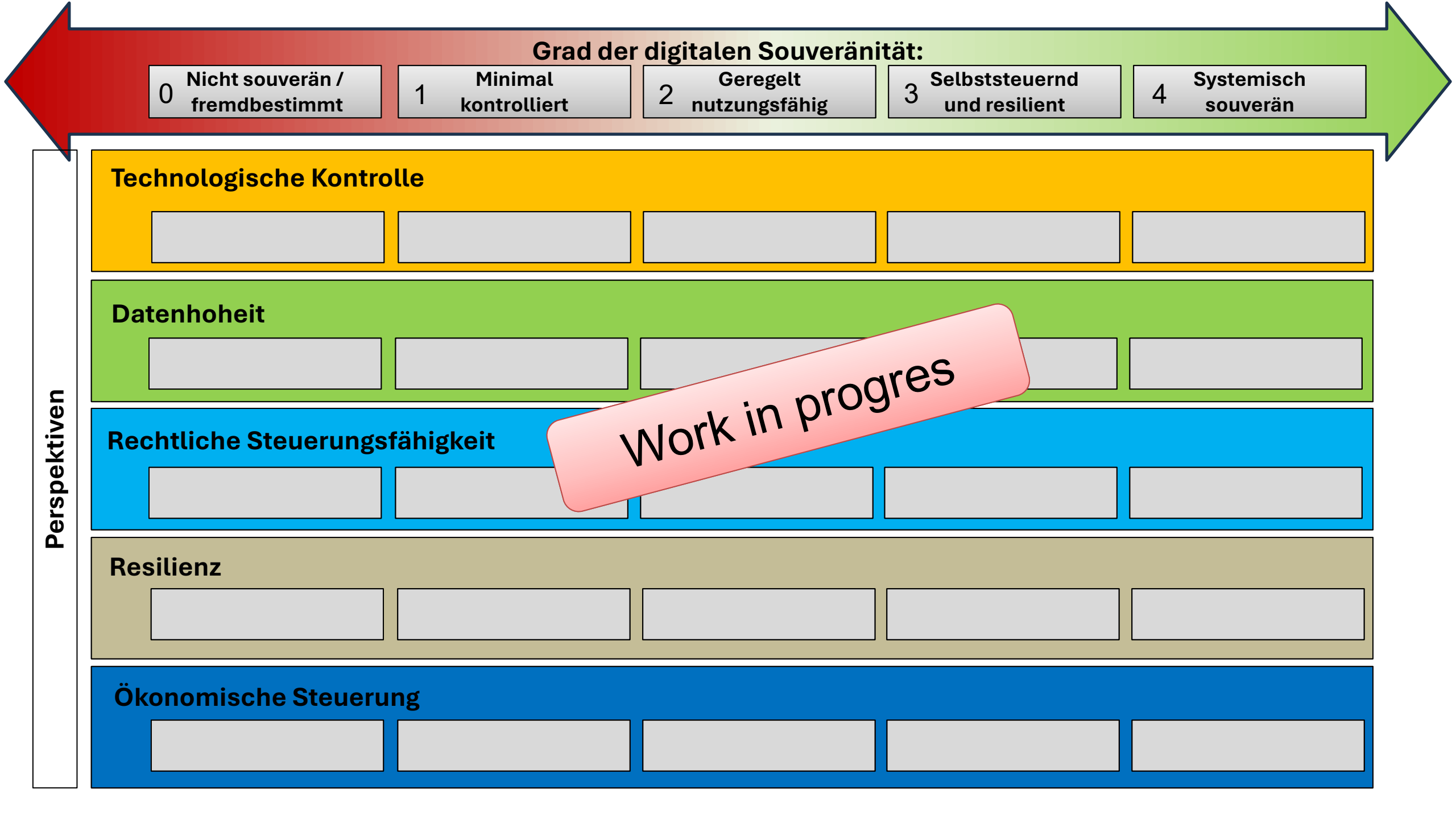
➔ Ein möglicher Ansatz ist ein **Souveränitätsindex** oder ein **Framework digitale Souveränität**

Mögliche Perspektiven «Digitale Souveränität»

Perspektive	Beschreibung	Typische Ansätze
Technologische Kontrolle	Inwieweit hat die Bundesverwaltung Kontrolle über eingesetzte Technologien und deren Weiterentwicklung?	- Zugriff auf Quellcode, Standards und Schnittstellen - Möglichkeit zur Auditierung und Anpassung - Abhängigkeit von proprietären Systemen oder Monopolanbietern - Förderung eigener technologischer Innovationskraft
Datenhoheit	Wer hat Zugriff auf, Kontrolle über und Entscheidungsgewalt bezüglich der Daten – insbesondere sensible Verwaltungsdaten?	- Standort der Datenhaltung (CH/EU/Drittstaat) - Verschlüsselung, Zugriffskontrollen, Metadatenhoheit - Datenverfügbarkeit und -portabilität - Regelungen bei Notfällen und Betriebsunterbrechungen
Rechtliche Steuerungs-fähigkeit	Wie stark kann die Schweiz bzw. die Bundesverwaltung rechtlich und politisch auf die digitalen Rahmenbedingungen Einfluss nehmen?	- Kontrolle über Governance-Modelle - Vertragsgestaltung, Exit-Klauseln, Compliance, - Politische Abhängigkeit von ausländischen Regulierungen - Fähigkeit, digitale Grundrechte sicherzustellen/durchzusetzen
Resilienz	Wie robust und krisenfest sind digitale Systeme und Prozesse der Bundesverwaltung gegenüber Störungen, Krisen und Abhängigkeiten?	- Redundanz und Failover-Konzepte - Exit-Strategien bei Ausfall oder Sanktionen - Fähigkeit zur Wiederherstellung (Disaster Recovery) - Diversifikation der Lieferketten und Anbieter - Fähigkeit, kritische Funktionen im Krisenfall autonom zu betreiben
Ökonomische Steuerung	Wie kann die Bundesverwaltung durch ökonomische Steuerung und strategisches Sourcing ihre digitale Souveränität kosteneffizient sichern und gleichzeitig Abhängigkeiten sowie Risiken in der IT-Beschaffung minimieren?	- Kosten- und Investitionsplanung - Exit- und Migrationsszenarien - Marktmacht nutzen - Total Cost of Ownership (TCO) Analysen

Mögliche Stufen der digitalen Souveränität

Stufe	Kurzbezeichnung	Beschreibung
0	**Fremdbestimmt / Nicht-souverän**	Keine Kontrolle über Systeme, Daten oder Infrastruktur; keine Trnsparenz, hohe Abhängigkeiten; keine Exit- oder Altrnativoptionen
1	**Minimal kontrolliert**	Erste Einsichten in Nutzung und Abhängigkeiten; punktuelle Kontrollmechanismen; operative, rechtliche oder technologische Lücken bestehen
2	**Geregelt nutzungsfähig**	Systeme verlässlich und teilweise steuerbar; rechtliche und technischer Rahmen etabliert; strategische Abhängigkeiten weiterhin bestehend
3	**Selbststeuernd und resilient**	Marktposition wird genutzt; Exit-Strategien und Multivendor-Konzepte implementiert; KnowHow aufgebaut; Resilienz und Krisenszenarien vorbereitet
4	**Systemisch souverän**	Souveränität in allen relevanten Dimensionen (rechtlich, technologisch, kulturell, strategisch); aktive Markt- und Standardgestaltung; geopolitische Wirkung möglich


Grad der digitalen Souveränität:
0 Nicht souverän / fremdbestimmt
1 Minimal kontrolliert
2 Geregelt nutzungsfähig
3 Selbststeuernd und resilient
4 Systemisch souverän
Perspektiven
Technologische Kontrolle
Datenhoheit
Rechtliche Steuerungsfähigkeit
Work in progres
Resilienz
Ökonomische Steuerung

Grad der digitalen Souveränität:

	0 Nicht souverän / fremdbestimmt	1 Minimal kontrolliert	2 Geregelt nutzungsfähig	3 Selbststeuernd und resilient	4 Systemisch souverän
Technologische Kontrolle	Technologische Abhängigkeit von externen Anbietern; Quellcode, Plattformen und Betriebsmodelle vollständig in fremder Hand. Kein aktiver Eingriff möglich. Keine Kontrolle über Updates, Standards oder Schnittstellen.	Einzelne Konfigurationen möglich, vor allem durch Dienstleister. Eingeschränkte API-Nutzung erlaubt Automatisierung, aber keine tiefgreifende Architekturkontrolle.	Kontrolle über Konfigurationen wird gezielt ausgeweitet; Quellcode-Einsicht für zentrale Komponenten wird eingefordert, strategische Governance etabliert sich	Technologische Roadmaps werden aktiv entwickelt. Anbieterwahl orientiert sich an Interoperabilität, Modularität und Open-Source-Optionen. Entwicklung eigener Komponenten wird vorbereitet, aber nicht abgeschlossen.	Technologische Eigenständigkeit ist etabliert. Es bestehen offene Schnittstellen, eigene IP, Betrieb im souveränen Raum. Internationale Kompatibilität und digitale Diplomatie werden aktiv gestaltet.
Datenhoheit	Datenhaltung erfolgt ausschliesslich durch externe Akteure. Metadaten, Speicherorte und Zugriffsrechte sind nicht kontrollierbar. Es besteht ein systematischer Kontrollverlust.	Lesender Zugriff auf Datenbestände ist gegeben, aber Export- und Aggregationsmöglichkeiten sind eingeschränkt. Datenschutz kann durchgesetzt werden, aber nicht bei Metadaten oder Datenübermittlung an Drittländer.	Datenflüsse sind nachvollziehbar; Interoperabilität wird aktiv gefordert; Datenschutz und Zugriffskontrolle werden als Kriterien in Beschaff… integriert	Speicherorte, Klassifizierung und Zugriffsk…llen sind definiert. …den systematisch …n oder vertraglich …reign-Cloud-Szenarien …tern vorbereitet.	Datenverarbeitung erfolgt vollständig im kontrollierten Raum. Metadatenkontrolle, Auditierung und Verschlüsselung unter eigenem Schlüsselbesitz. Drittländer ausgeschlossen.
Rechtl. Steuerungsfähigkeit	Nutzung basiert auf Standardverträgen ("Click-Through"), ohne verhandelte Bedingungen. Juristische Bindung vollständig auf Seiten der Anbieter.	Nutzung EU-basierter Dien… teilweiser CH-Vertra… Regulatorische Grau… Exit- oder Second-So… Rechtlicher Rahmen … ist aber nicht strategis…	…r Exit, …bilität; rechtliche …gen werden strategisch …rmonisiert.	Verhandlungsstrategie enthält Escrow-Klauseln, SLA-Standards, Exit-Bedingungen und Aufgabenteilung mit Zweitanbietern. Vertragsgestaltung wird zunehmend strategisch.	Standardisierte Exit-Szenarien, Mandantenfähigkeit, Escrow & Second-Source sind in allen Verträgen operationalisiert. Rechtliche Risiken können aktiv minimiert werden.
Resilienz	Es bestehen Single Points of Failure auf allen Ebenen. Keine Notfallpläne, keine Redundanzen, kein Zugriff im Krisenfall.	Erste technische Massnahmen zur Resilienz (z.B. lokale Backups, Failover-Testfälle). Ausfallszenarien sind skizziert, aber noch nicht durchgehend durchgeplant. Kein koordiniertes Notfallkonzept.	Teils redundante Systeme, Second-Source-Strategien initialisiert; erste Massnahmen zur strukturellen Resilienz erkennbar, Szenarien werden geübt.	Krisen- und Resilienzmanagement ist Bestandteil der Betriebsstrategie. Cyber-Resilienz, nationale Backup-Strukturen (insbes. Verbund-RZ) und Cloud-Exit-Optionen werden getestet. Pläne sind dokumentiert und mit Partnern abgestimmt.	Redundanz-, Backup- und Krisenmechanismen sind automatisiert. Kritische Applikationen haben physische und logische Schutzebenen. Sofortige Handlungsfähigkeit bei Ausfall oder Angriff (Prämisse 2).
Ökonomische Steuerung	Kostenkontrolle liegt beim Anbieter. Es existieren keine Exit-Szenarien. Preismodell ist beliebig anpassbar durch den Anbieter.	Kosten-Transparenz entsteht. Betriebskosten sind kalkulierbar, aber Migrationskosten bleiben schwer planbar.	Multivendor-Strategien geplant aber noch nicht umgesetzt; Exit wird einkalkuliert, Investitionen werden steuerungsfähig gemacht	Lifecycle-Kostenmodelle werden erstellt, Gesamtbetriebskosten (TCO) bewertet. Investitionsstrategien setzen gezielte Souveränitätsakzente. Anbietersteuerung erfolgt zunehmend auch über Verhandlungsposition der BVerw (Marktmacht als Hebel).	Steuerung erfolgt nach TCO, Lebenszyklus und strategischen Investitionsprioritäten (Prämisse 1). Souveränitätskosten sind transparent und begründet. Die Bverw nutzt ihre Matkstellung auch mit Wirkung auf geopolitischer Ebene (Prämisse 4)

Work in progres

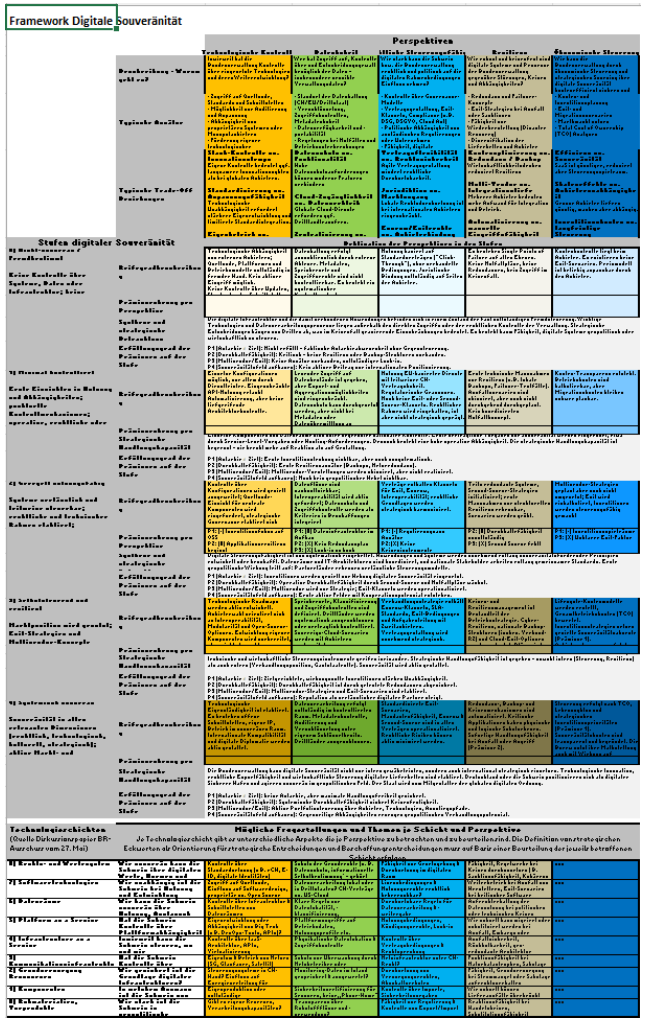
Grad der digitalen Souveränität:

	0 Nicht souverän / fremdbestimmt	1 Minimal kontrolliert	2 Geregelt nutzungsfähig	3 Selbststeuernd und resilient	4 Systemisch souverän
Technologische Kontrolle	Technologische Abhängigkeit von externen Anbietern; Quellcode, Plattformen und Betriebsmodelle vollständig in fremder Hand. Kein aktiver Eingriff möglich. Keine Kontrolle über Updates, Standards oder Schnittstellen.	Einzelne Konfigurationen möglich, vor allem durch Dienstleister. Eingeschränkte API-Nutzung erlaubt Automatisierung, aber keine tiefgreifende Architekturkontrolle.	Kontrolle über Konfigurationen wird gezielt ausgeweitet; Quellcode-Einsicht für zentrale Komponenten wird eingefordert, strategische Governance etabliert sich	Technologische Roadmaps werden aktiv entwickelt. Anbieterwahl orientiert sich an Interoperabilität, Modularität und Open-Source-Optionen. Entwicklung eigener Komponenten wird vorbereitet, aber nicht abgeschlossen.	Technologische Eigenständigkeit ist etabliert. Es bestehen offene Schnittstellen, eigene IP, Betrieb im souveränen Raum. Internationale Kompatibilität und digitale Diplomatie werden aktiv gestaltet.
Datenhoheit	Datenhaltung erfolgt ausschliesslich durch externe Akteure. Metadaten, Speicherorte und Zugriffsrechte sind nicht kontrollierbar. Es besteht ein systematischer Kontrollverlust.	Lesender Zugriff auf Datenbestände ist gegeben, aber Export- und Aggregationsmöglichkeiten sind eingeschränkt. Datenschutz kann durchgesetzt werden, aber nicht bei Metadaten oder Datenübermittlung an Drittländer.	Datenflüsse sind nachvollziehbar; Interoperabilität wird aktiv gefordert; Datenschutz und Zugriffskontrolle werden als Kriterien in Beschaf integriert	Speicherorte, Klassifi Zugriffsk	gt vollständig im tierung und enem er
Rechtl.Steuerungsfähigkeit	Nutzung basiert auf Standardverträgen ("Click-Through"), ohne verhandelte Bedingungen. Juristische Bindung vollständig auf Seiten der Anbieter.	Nutzung EU-basierter Dienste mit teilweiser CH-Vertragshoheit. Regulatorische Grauzonen. Noch keine Exit- oder Second-Source-Klauseln. Rechtlicher Rahmen wird eingehalten, ist aber nicht strategisch geprägt.	Verträge enthalten Klauseln für E Escrow, Interoperabilität; rechtlic Grundlagen werden strategisch harmonisiert.	Escrow- dards, Exit- gungen und Aufgabenteilung mit Zweitanbietern. Vertragsgestaltung wird zunehmend strategisch.	Standardisierte Exit-Szenarien, Mandantenfähigkeit, Escrow & Second-Source sind in allen Verträgen operationalisiert. Rechtliche Risiken können aktiv minimiert werden.
Resilienz	Es bestehen Single Points of Failure auf allen Ebenen. Keine Notfallpläne, keine Redundanzen, kein Zugriff im Krisenfall.	Erste technische Massnahmen zur Resilienz (z.B. lokale Backups, Failover-Testfälle). Ausfallszenarien sind skizziert, aber noch nicht durchgehend durchgeplant. Kein koordiniertes Notfallkonzept.	Teils redundante Systeme, Second-Source-Strategien initialisiert; erste Massnahmen zur strukturellen Resilienz erkennbar, Szenarien werden geübt.	Krisen- und Resilienzmanagement ist Bestandteil der Betriebsstrategie. Cyber-Resilienz, nationale Backup-Strukturen (insbes. Verbund-RZ) und Cloud-Exit-Optionen werden getestet. Pläne sind dokumentiert und mit Partnern abgestimmt.	Redundanz-, Backup- und Krisenmechanismen sind automatisiert. Kritische Applikationen haben physische und logische Schutzebenen. Sofortige Handlungsfähigkeit bei Ausfall oder Angriff (Prämisse 2).
Okonomische Steuerung	Kostenkontrolle liegt beim Anbieter. Es existieren keine Exit-Szenarien. Preismodell ist beliebig anpassbar durch den Anbieter.	Kosten-Transparenz entsteht. Betriebskosten sind kalkulierbar, aber Migrationskosten bleiben schwer planbar.	Multivendor-Strategien geplant aber noch nicht umgesetzt; Exit wird einkalkuliert, Investitionen werden steuerungsfähig gemacht	Lifecycle-Kostenmodelle werden erstellt, Gesamtbetriebskosten (TCO) bewertet. Investitionsstrategien setzen gezielte Souveränitätsakzente. Anbietersteuerung erfolgt zunehmend auch über Verhandlungsposition der BVerw (Marktmacht als Hebel).	Steuerung erfolgt nach TCO, Lebenszyklus und strategischen Investitionsprioritäten (Prämisse 1). Souveränitätskosten sind transparent und begründet. Die Bverw nutzt ihre Matkstellung auch mit Wirkung auf geopolitischer Ebene (Prämisse 4)

ergibt hier eine Souveränitäts-Kennzahl von 5 (von 20)

- Das Framework ist bei BK-DTI «work in progres» im Rahmen der Strategie-Massnahme 4 «Digitale Souveränität stärken»

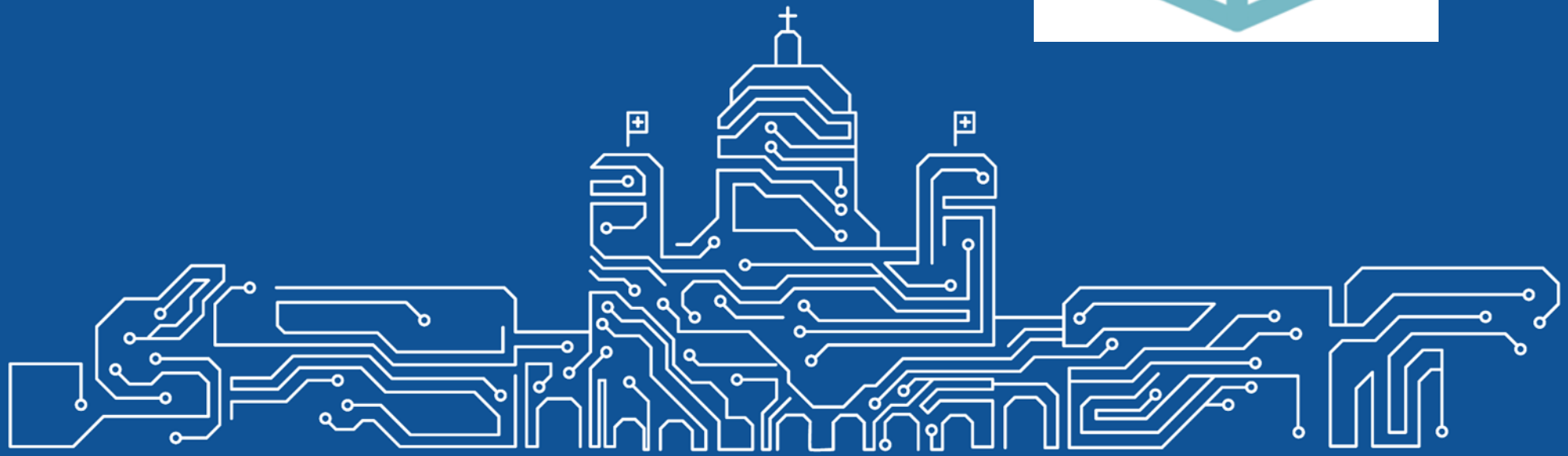
- Was halten Sie vom Ansatz eines solchen Frameworks?



Digitale_Souveraenitaet_Framework-Modell_x0100.xlsx

4. Open Source als Fokusthema 2025

Stand Projekt PoC BOSS



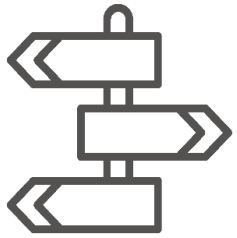
Fokusthemen Digitale Schweiz 2025 (digital.swiss)

Strategie Digitale Schweiz

➔ Entscheid BR vom 13.12.2024

Bildung & Kompetenzen

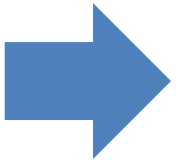
Sicherheit & Vertrauen



Rahmenbedingungen

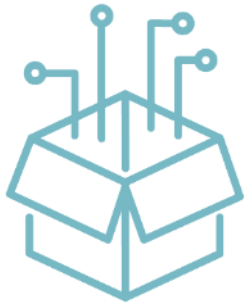
Infrastruktur

Digitale Behördenleistungen

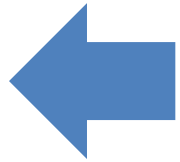


Künstliche Intelligenz

Information- und Cybersicherheit



Open Source



2-3 Fokusthemen werden jährlich neu von Bundesrat definiert (im Dezember fürs Folgejahr)

Fokusthema «Open Source in der Bundesverwaltung fördern»

Open Source in der Bundesverwaltung fördern

Die Veröffentlichung und der Einsatz von Open-Source-Software (OSS) in der Bundesverwaltung sollen aktiv gefördert werden, um Transparenz, Sicherheit und Innovationskraft in IT-Systemen zu steigern und um die digitale Souveränität der Verwaltung zu stärken. Gleichzeitig soll der Wissensaustausch sowie die Zusammenarbeit mit der nationalen und internationalen Open-Source-Community intensiviert werden, wodurch die Schweiz eine Vorreiterrolle einnehmen und ihre digitale Souveränität stärken kann.

Federführung: BK (Bereich Digitale Transformation und IKT-Lenkung)

Quelle: https://digital.swiss/de/strategie/fokusthema/open-source-in-der-bundesverwaltung-fordern

3 definierte Massnahmen

1

OSS Hilfsmittel

Weiterentwicklung V2.0 (Ressourcen dazu bereitgestellt)

Politisch auszuloten, wie viel Zentralisierung für OSS gewünscht wird und welche Ressourcen dafür erforderlich sind (z.B. auch Aufbau zentrales Repository)

2

Open Source Community of Practice (CoP)

Ziel: Wissensaustausch stärken und praktische Erfahrungen mit Open Source sammeln

→ Aufbau einer **bundesweiten CoP** (regelmässige Zusammenkünfte mit Mitgliedern aus allen Departementen und der dezentralen Bundesverwaltung

→ Lunch and Learn / Internationale Kontakte knüpfen / Teilnahme an Konferenzen usw.

→ *Viva Engage Gruppe* – schon über 700 Mitarbeitende ➔ mitmachen

→ Mailadresse: opensource@bk.admin.ch

3

Büroautomation mit OSS (→ PoC BOSS)

Proof of Concept aufgebaut: Einsatz von Open-Source-Software für grundlegende Büroanwendungen

+ Notfall-Lösung

Massnahme 3: PoC BOSS (Büroautomation mit OSS)

Ziele:

OSS Exit Strategie M365

Notfall Büroautomation

Sichere Bearbeitung

Verifikation

Ergebnisbericht als Entscheidungsgrundlage

→ Gesamtdokumentation der Ergebnisse liegt vor
→ Bericht über Erfahrungen im Aufbau, Betrieb und Benutzung der Umgebung ist erstellt
→ Empfehlung über das weitere Vorgehen liegt vor

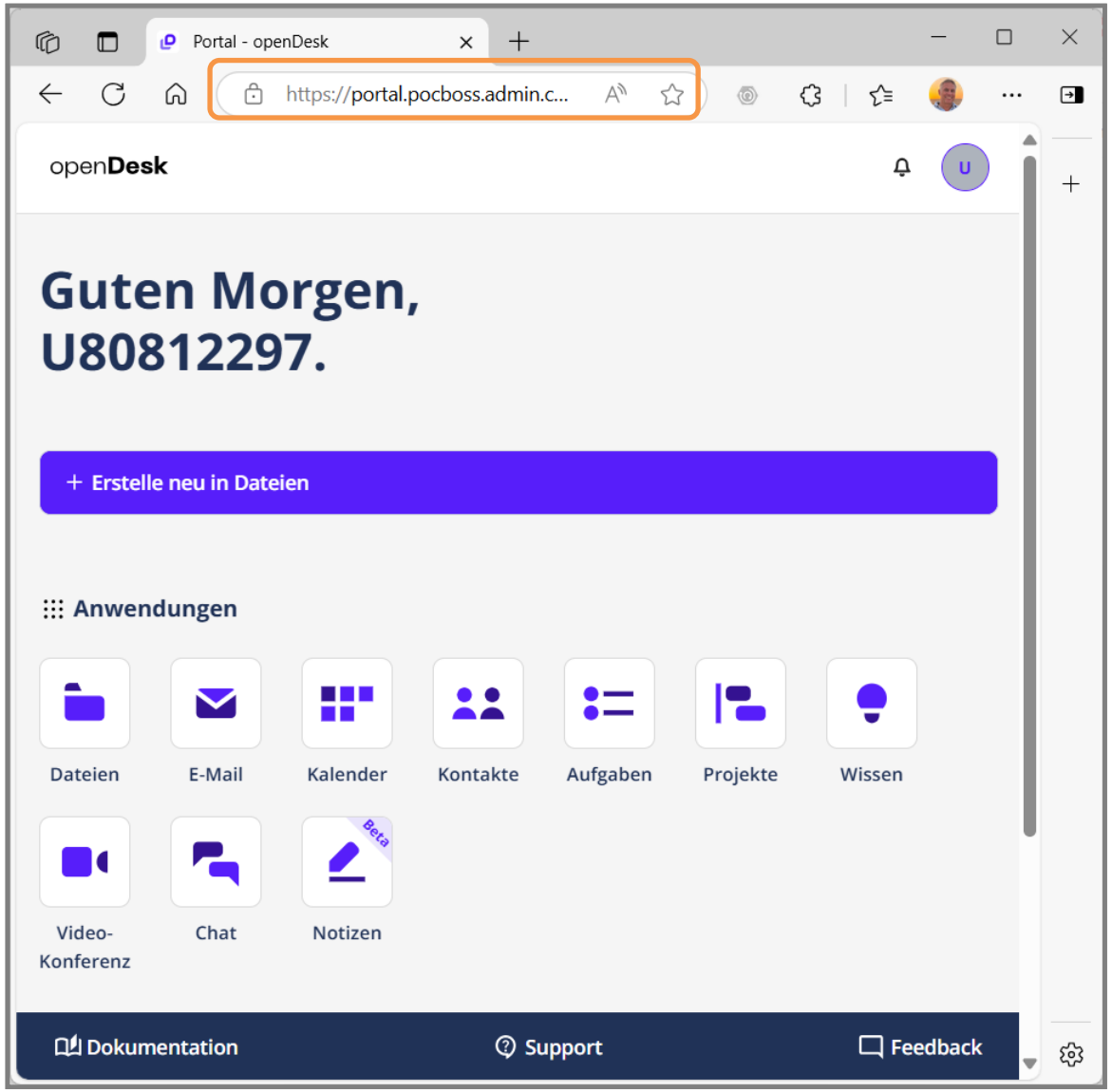
PoC BOSS mit openDesk

openDesk
Der Souveräne Arbeitsplatz

ZenDiS Zentrum Digitale Souveränität

www.opendesk.eu/

Umgebung on-premises aufgebaut:
portal.pocboss.admin.ch



Quelle: DTI

Key Takeaways

Open Standards und OSS untersützen die Digitale Souveränität

OSS-Hilfsmittel Version 2.0 erscheinen bis Ende 2025

Überlegungen **Digitale Souveränität als Beschaffungskriterium**

OSS geht auch nach dem Fokusthemenjahr 2025 weiter

PoC BOSS als konkreter Schritt Richtung Digitale Souveränität


UNUS PRO OMNIBUS
OMNES PRO UNO