27. November 2025 | Bundesamt für Cybersicherheit BACS

Open-Source-Strategie BACS

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS
Bundesamt für Cybersicherheit BACS

Übersicht / Inhalt

Management Summary

Das Bundesamt für Cybersicherheit (BACS) setzt EMBAG-konform «Open Source by default » um. Neuentwicklungen werden grundsätzlich als Open Source-Software veröffentlicht. Ausnahmen sind zu begründen, zu dokumentieren und periodisch zu überprüfen. Bestehende Anwendungen werden auf freiwilliger Basis systematisch geprüft und – wo verhältnismässig und machbar – stufenweise geöffnet.

Hinweis: Dieser Leitentscheid setzt Art. 9 des Bundesgesetzes über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBAG; SR 172.19) im BACS um und richtet sich nach den von der Bundeskanzlei publizierten Leitfäden, Checklisten und Wegleitungen. Zusätzlich zu dieser Strategie besteht ein Open-Source-Leitfaden, welcher die Details der Anwendung regelt.

Das BACS setzt Open Source gemäss EMBAG als Arbeitsprinzip um, mit klaren Regeln und Verantwortlichkeiten. Ziel sind digitale Souveränität, Qualität und Tempo bei tragbaren Kosten. Sicherheit und Rechtskonformität haben Vorrang. Publikationen erfolgen verantwortet und wo nötig gestaffelt.

Strategischer Rahmen und Lizenzen

Das BACS verfolgt Open Source by default. Permissive Lizenzen (z. B. Apache-2.0/MIT) sind Standard für breite Wiederverwendung, Copyleft/EUPL wird eingesetzt, wenn Rückfluss von Anpassungen oder Abhängigkeiten dies nahelegen. Lizenz-Whitelist, saubere Rechtekette/IP-Abtretung und Inbound/Outbound-Compliance sind verbindlich. Veröffentlichungen erfolgen in offenen Repositories mit OSPO- (Open Source Program Office) Governance, definierten Release-Gates, Roadmap und Changelogs. Sicherheit und Datenschutz haben Priorität: ein formeller Freigabeschritt durch die Informationssicherheitsbeauftragten (ISBO) und die Datenschutzbeauftragten (DSBO) geht jeder Publikation voraus. Wo nötig, wird der Publikationsumfang (Module/Artefakte) begrenzt.

Wirkung durch Beiträge und Co-Entwicklung

Im Zentrum steht die aktive Mitarbeit von Dritten: klare Beitragsregeln, transparente Roadmaps/Backlogs, stabile Schnittstellen und planbare Releases erleichtern Beiträge und beschleunigen die Weiterentwicklung.

Umsetzung und Verankerung

Die Umsetzung stützt sich auf eine Open Source Governance Richtlinie, klare Zuständigkeiten (OSPO, Rechtsdienst, Fach) und einen Leitfaden mit Checklisten, Rollen und Templates. So entsteht ein einheitliches Vorgehen von der Planung über die Beschaffung bis zu Betrieb und Community-Arbeit. Beschaffungen und Verträge berücksichtigen Open Source- und Sicherheitsanforderungen von Beginn an.

1 Ausgangslage, Kontext und Handlungsbedarf

Digitalisierung, Souveränität, Interoperabilität

International wächst der Trend zu offenen Lösungen, welche Transparenz, Wiederverwendbarkeit und Kooperation ermöglichen. Open Source wird zunehmend als strategischer Hebel verstanden, um Abhängigkeiten von einzelnen Anbietern zu reduzieren, Interoperabilität sicherzustellen und die Innovationskraft von Ökosystemen zu nutzen. Der Grundsatz «Public Money, Public Code» gewinnt auch in der Schweiz an Bedeutung.

Gleichzeitig verlagern sich sicherheitsrelevante Funktionen immer stärker in softwaregetriebene Prozesse. Sichtbarkeit des Quellcodes, reproduzierbare Builds und nachvollziehbare Lieferketten (z. B. Komponentenlisten/SBOM, signierte Releases) werden zu Voraussetzungen, um Risiken in der Breite bewältigen zu können. Das gilt sowohl intern als auch im Austausch mit Partnern. Offene Komponenten fördern zudem die Wiederverwendung in Verwaltung, Forschung und Wirtschaft und stärken die digitale Souveränität, weil Know-how und Gestaltungsfreiheit im Land bleiben.

Rechtsgrundlagen

Mit Art. 9 EMBAG verfügt der Bund seit dem 1. Januar 2024 über eine verbindliche Rechtsgrundlage. Die 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 (Art. 9 Abs. 1 EMBAG). Software soll immer dann als Open Source freigegeben werden, wenn dies möglich und sinnvoll ist – die Behörde entscheidet nach pflichtgemässem Ermessen über die konkrete Umsetzung. Die Bundeskanzlei unterstützt alle Bundesbehörden bei der einheitlichen Umsetzung, indem sie Hilfsmittel wie Leitfäden, Checklisten und Wegleitungen für die Veröffentlichung von Open-Source-Software bereitstellt.

Welche Software ist betroffen?

Art. 9 EMBAG umfasst jede Software, die Bundesbehörden zur Erfüllung ihrer Aufgaben entwickeln oder entwickeln lassen. Die Definition ist bewusst weit gefasst und umfasst beim BACS etwa:

- Anwendungen, Module und Plattformen (z. B. Cyber Security Hub [CSH]);
- Bibliotheken und Komponenten;
- Skripte, Automatisierungen und Konfigurationen;
- Algorithmen und Modelle (soweit selbst erstellt).

Nicht betroffen sind unverändert erworbene Software-Produkte Dritter sowie reine Datenbestände, Konfigurationsdateien und Design-Elemente.

1.1 Geltungsbereich und Publikationslogik

Geltungsbereich Open-Source-Strategie

Die Open Source Strategie ist für alle Bereiche und Projekte des BACS verbindlich. Sie gilt für alle individuellen Software-Lösungen, die das BACS entwickelt, beauftragt oder betreibt - für Neuentwicklungen ebenso wie für bestehende Anwendungen. Die Strategie bildet die Grundlage für Projektentscheide, Architekturvorgaben und Beschaffungsprozesse.

Abgrenzung

Im Umgang mit Open Source ist zwischen Bezug bestehender Komponenten und der Erstellung bzw. Weiterentwicklung mit anschliessender Publikation von Software durch den Bund zu unterscheiden. Art. 9 EMBAG regelt ausschliesslich Letzteres. Bezug/Verwendung (out → in): fällt nicht unter Art. 9 EMBAG; es besteht keine Pflicht zur Code-Publikation. Im Fokus stehen Beschaffung, Einsatz und Lizenzkonformität.

Erstellung/Weiterentwicklung (in → out)

Fällt unter Art. 9; der Quellcode ist grundsätzlich zu veröffentlichen. Ausnahmen bestehen nur bei Rechten Dritter oder sicherheitsrelevanten Gründen. Die Publikation erfolgt unter einer geeigneten Open-Source-Lizenz; Leistungen wie Integration, Betrieb oder Support können weiterhin kostendeckend erbracht werden.

Konsequenz für die Praxis

Der blosse Einsatz bestehender Software löst keine Pflichten nach Art. 9 EMBAG aus. Entsteht eigener Code oder wird bestehender Code substanziell weiterentwickelt (auch in Teilpaketen), gilt Art. 9 EMBAG. Ausnahmen sind stets zu begründen und dokumentieren.

Publikationslogik

Verschiedene Involvierungslevel bei einer Open-Source-Publikation:

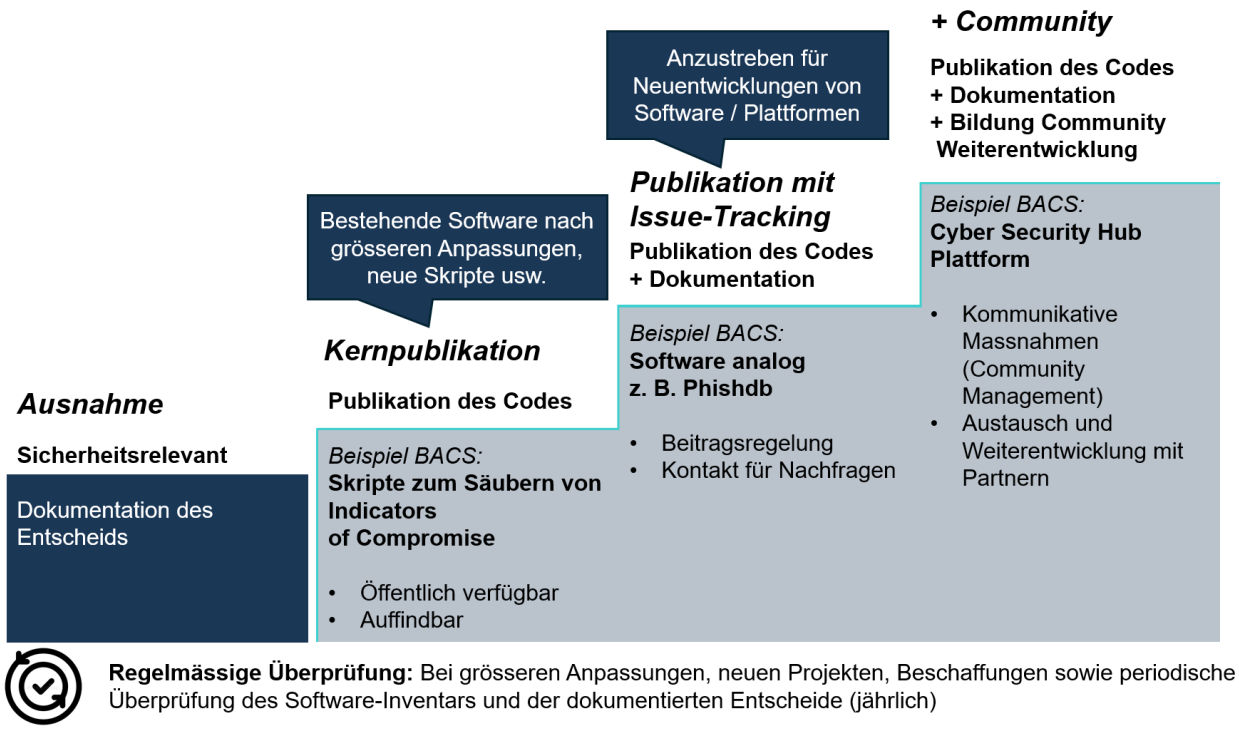

Abbildung 1: Open Source Stufenmodell BACS

1.2 Grundsätze der Umsetzung

Zweckmässigkeit und Verhältnismässigkeit

Die Veröffentlichung gemäss EMBAG erfolgt nur dann, wo sie möglich und sinnvoll ist. Sie kann ausgelassen werden, wenn:

- Rechte Dritter nicht zu angemessenen Bedingungen erworben werden können;
- Geheimhaltungsgründe dagegensprechen.

Die Publikation folgt dem Grundsatz «so offen wie möglich, so restriktiv wie nötig». Das bedeutet:

- Kernpublikation – Minimumvariante Publikation des Codes;
- Publikation mit Issue-Tracking: Fehler oder Mängel können gemeldet werden und werden behandelt;
- Publikation mit geförderten Community-Beiträgen;
- Keine Publikation – begründete Ausnahme.

Damit wird sichergestellt, dass Offenheit und Sicherheit im Einklang stehen und die Veröffentlichung stets zweckmässig und nachhaltig erfolgt.

Lizenzierung und Rechtsverhältnisse

Die Rechte werden in Form privatrechtlicher Lizenzen erteilt (Art. 9 Abs. 3 EMBAG). Soweit möglich und sinnvoll sind international etablierte Lizenztexte zu verwenden (Art. 9 Abs. 4 EMBAG). Haftungsansprüche von Lizenznehmern sind, soweit rechtlich möglich, auszuschliessen.

Verantwortlichkeiten und Umsetzung

Das BACS ist für die Umsetzung von Art. 9 EMBAG selbst verantwortlich. Es ist explizit keine zentrale Zuständigkeit innerhalb des Bundes vorgesehen - die dezentrale Umsetzung liegt bei den einzelnen Verwaltungseinheiten. Software, die neu erstellt wird oder einen grösseren Release erfährt, ist grundsätzlich zu veröffentlichen.

Ergänzende Dienstleistungen

Das BACS kann ergänzende Dienstleistungen erbringen (Integration, Wartung, Support), soweit diese der Erfüllung von Behördenaufgaben dienen und mit verhältnismässigem Aufwand erbracht werden können (Art. 9 Abs. 5 EMBAG). Für diese Leistungen ist grundsätzlich ein kostendeckendes Entgelt zu verlangen (Art. 9 Abs. 6 EMBAG).

Handlungsbedarf für das BACS

«Open Source by Default» wird zur Regel. Ausnahmen müssen klar begründet, dokumentiert und regelmässig überprüft werden. Der Ansatz verlangt strukturierte Governance statt Ad-hoc-Entscheide: transparente Rollen, definierte Entscheidungswege und klare Zuständigkeiten für Sicherheit und Qualität. So lässt sich die gesetzliche Verpflichtung zur Offenlegung mit den Sicherheits- und Effizienzzielen des BACS in Einklang bringen.

2 Open-Source-Strategie BACS

2.1 Ziele und Mehrwerte

Das BACS setzt «Open Source by Default» gemäss Art. 9 EMBAG konsequent um: Neuentwicklungen werden grundsätzlich offen publiziert. Ausnahmen sind begründet, dokumentiert und periodisch überprüft. Bestehende Anwendungen werden systematisch auf Öffnung geprüft und schrittweise geöffnet, wo dies verhältnismässig und machbar ist. Bevorzugt werden bestehende Open-Source-Bausteine. Partnerschaften werden genutzt, Kompetenzen gezielt ausgebaut und aktive Beiträge in genutzte Projekte geleistet. Transparente Architekturentscheide, Roadmaps und Changelogs sichern Qualität, Mehrwert und Wiederverwendung.

Folgende Ziele und Mehrwerte werden verfolgt:

Für das BACS

- Verlässliche Umsetzung der EMBAG-Vorgaben, Ausbau digitaler Souveränität sowie Qualitäts- und Effizienzgewinne in der Software-Entwicklung.
- Einheitliche Prozesse, klare Governance und professionelles Auftreten im Bereich Open Source schaffen Rechtssicherheit und ermöglichen nachhaltige Zusammenarbeit mit öffentlichen wie privaten Partnern.

Für die Schweiz

- «Public Money, Public Code»: Mit öffentlichen Mitteln entwickelte Software kann mehrfach genutzt werden.
- Wiederverwendung spart Kosten, reduziert Doppelentwicklungen und fördert eine gemeinsame digitale Infrastruktur über Verwaltungsebenen hinweg.

Für Partner

- Gebührenfreie Lizenzen (Art. 9 Abs. 2 EMBAG), transparente Entwicklungsprozesse und niedrige Eintrittshürden eröffnen neue Möglichkeiten zur Mitgestaltung und Weiterentwicklung.
- Es entsteht ein Ökosystem wiederverwendbarer Digital Public Goods, das Innovation und Wissenstransfer beschleunigt.

2.2 Leitprinzipen

Die Leitprinzipien konkretisieren die Vision «Open Source by Default». Sie geben eine verbindliche Orientierung für Entscheidungen, Umsetzung und Priorisierung - von Architekturentscheiden bis zur Publikation. Die Leitprinzipien berücksichtigen auch die Architekturprinzipien der Referenzarchitektur VBS.

Sicherheit, Datenschutz und nachhaltiger Betrieb

Sicherheit und Datenschutz sind nicht verhandelbar. Das BACS integriert dieses Prinzip von Beginn an und veröffentlichen erst nach sauberer Prüfung. Sensible Informationen werden nicht publiziert. Schwachstellen werden verantwortungsvoll behandelt und - sobald vertretbar - offen kommuniziert. Damit die Veröffentlichung tragfähig bleibt, berücksichtigt das BACS Wartung, Sicherheitskorrekturen, Dokumentation und wo nötig Community-Arbeit, baut technische Schulden ab und geht schrittweise vor. Das BACS beginnt erst mit dem Ausbau des Publikationsumfangs und mit Community-Tätigkeiten, wenn Bedarf oder Nutzen identifizierbar sind.

Zielgerichtete Publikation

Für sicherheitskritische Komponenten gilt entweder Minimalpublikation oder begründeten Ausnahme. Für nicht-kritische Software gilt volle Transparenz. Der Publikationsumfang richtet sich nach Vertraulichkeit allfälliger Rechten Dritter sowie dem Ziel der Wiederverwendung. Entscheide werden nachvollziehbar dokumentiert, befristet und regelmässig überprüft - stets im Einklang mit den geltenden Vorgaben.

Verbindlichkeit und Standardisierung

Ein klarer Open-Source-Prozess im BACS führt zu nachvollziehbaren Open-Source-Entscheidungen, Ausnahmen, Lizenzen und Publikationen. Ausnahmen sind befristet und begründet und werden periodisch überprüft. Entscheidungen sind revisionssicher dokumentiert. Rechtliche und regulatorische Anforderungen (Informationssicherheit, Datenschutz, Urheber-/Markenrecht) sind integriert.

Kollaboration, Reuse-first und Interoperabilität

Wiederverwendung hat Vorrang vor Neuentwicklung: Bestehende Open-Source-Bausteine werden systematisch geprüft und bevorzugt eingesetzt. Lösungen werden API-first, standardbasiert gestaltet, um Integration und Austauschbarkeit zu sichern. Externe Beiträge aus Verwaltung, Forschung und Wirtschaft werden aktiv gefördert. Zudem setzt sich das BACS zum Ziel, aktiv an für das BACS relevanten Open-Source-Projekten mitzuwirken. Internationale und industriespezifische Standards sind vorzuziehen.

2.3 Empfehlungen für bestehende Software, Skripte und Neuentwicklungen

Neuentwicklungen

Open by Default. Alle neuen Applikationen und Module, die im Auftrag oder unter Verantwortung des BACS entstehen, werden standardmässig unter einer geeigneten Open-Source-Lizenz publiziert - ausser, wenn Rechte Dritter oder überwiegende Schutzinteressen entgegenstehen.

Software, die nach dem 1. Januar 2024 entwickelt wird, fällt direkt unter Art. 9 EMBAG und ist grundsätzlich zu veröffentlichen. Für ältere Anwendungen gilt: Eine Freigabe wird geprüft, sobald grössere Änderungen oder neue Hauptversionen (Major Releases) anstehen. Wo erhebliches Interesse Dritter besteht, kann auch eine freiwillige Veröffentlichung in Betracht gezogen werden - allenfalls unter Kostenbeteiligung und mit Aufbau einer Community.

Skripte und Kleinstcode zur täglichen Unterstützung

Für kleinere Skripte ist eine eigenständige Publikation in der Regel nicht zielführend. Bei dieser Kategorie ist das Prinzip der Verhältnismässigkeit zu beachten. Solche Skripts können gebündelt in dedizierten Repositories (digitaler Speicher) bereitgestellt werden, die einmalig den Freigabeprozess durchlaufen. Das BACS oder GS-VBS können für kleinere Skripte ein Sammel-Repository zur Verfügung stellen.

Umgang mit bestehender Software

Vorhandene Anwendungen werden systematisch überprüft - initial im Rahmen der Erarbeitung der Open-Source-Strategie und danach regelmässig. Massgebend sind die Kriterien Verhältnismässigkeit, Sicherheit, Sinn für Anwendung bei Dritten, Rechte Dritter sowie verfügbare

Ressourcen. Wo sinnvoll und tragbar, werden bestehende Anwendungen schrittweise für eine Veröffentlichung vorbereitet oder in Teilen publiziert (z. B. Schnittstellen, Dokumentation, nicht-sicherheitskritische Module).

Für ältere Anwendungen sieht das Gesetz keine rückwirkende Publikationspflicht vor. Dennoch wird bei neuen Hauptversionen jeweils geprüft, ob eine vollständige Freigabe möglich ist. Ansonsten ist mindestens eine Minimalpublikation oder eine dokumentierte Ausnahme vorzusehen.

3 Governance und Entscheidungsprozesse

Im Folgenden werden die Governance und die Entscheidungsprozesse der Open-Source-Strategie aufgezeigt. Die Prozesse sind vertieft im Leitfaden zur Open-Source-Strategie festgehalten.

3.1 Open Source Programm Office (OSPO)

Zur Umsetzung der Open-Source-Strategie richtet das BACS ein Open Source Program Office (OSPO) ein. Dieses ist keine eigenständige Abteilung, sondern ein virtuelles Konstrukt, koordiniert durch Planung und Steuerung, ein Team innerhalb des BACS. Es bündelt bedarfsgerecht Kompetenzen aus Technik, Recht, Informationssicherheit und Community und ist auf die Bedürfnisse einer schlanken, kleinen Organisation wie dem BACS zugeschnitten. Anstelle eines komplexen Gremienmodells setzt das OSPO auf ein handlungsfähiges Kernteam mit klarer Verantwortung und kurzen Entscheidungswegen.

Planung und Steuerung führt den Vorsitz, koordiniert die Abläufe und stellt die Verbindung in die Direktion sicher, einschliesslich der Traktandierung grösserer Publikationen und der Diskussion von Ausnahmen.

3.1.1 Rollen im OSPO

Product Owner (Projektleitung / PO der Applikation)

Führt die operative Umsetzung; stellt die Erstellung einer Dokumentation, die Aufbereitung, Checklisten und erste Sicherheits-/Lizenzprüfungen sicher; meldet Publikationsvorschläge an das OSPO.

Entwicklungsteams / Lieferanten (Know-How-Träger)

Stellen Code-Qualität, Security-Standards und Lizenzkonformität sicher; liefern Komponenten- und Lizenzinformationen; erstellen eine Dokumentation gemäss den Vorgaben des PO.

Community Manager

Externe Kommunikation, Contribution-Guidelines, Issue-Handling und Transparenz (README, SECURITY.md, Roadmap je nach Stufe); Interagiert mit der Community und stellt einen regelmässigen Austausch sicher.

Rechtsdienst und ISBO

Rechte Dritter, Datenschutz, Lizenzwahl, Sicherheitsfreigaben. Werden vom OSPO beigezogen.

OSPO-Vorsitz koordiniert durch Planung und Steuerung

Prüft Unterlagen, entscheidet über Publikationen (Fast-Track) und bringt Ausnahmen direkt in die Direktion. Dokumentiert Entscheidungen (Publikation, Ausnahme, Lizenzwahl) und liefert ein konsolidiertes Halbjahres-Reporting an die Direktion. Wenn nötig, liefert der OSPO-Vorsitz ad-hoc-Reportings an die Direktion. Pflegt die Open-Source-Strategie, den Leitfaden und die Hilfsmittel. Stellt Kontakt zu weiteren Stellen im Bereich Open Source wie BK und GS-VBS usw. sicher.

3.1.2 OSPO RACI

Die Rollen und Verantwortlichkeiten der am OSPO teilnehmenden Stellen werden in folgender RACI-Matrix dargestellt (RACI Responsible, Accountable, Consulted, Informed).

Aufgabe / Rolle	Product Owner	Entwicklung	Community Manager	Rechtsdienst / ISBO	OSPO
Dokumentation und Aufbereitung	**C**	**R**	**I**	**I**	**A**
Lizenz- und Komponentenprüfung	**R**	**C**	**I**	**C**	**A**
Security-Checks	**C**	**R**	**I**	**C**	**A**
Publikationsentscheidung (Fast-Track)	**I**	**I**	**I**	**C**	**R/A**
Publikationsentscheidung (Ausnahme)	**I**	**I**	**I**	**C**	**R/A Direktion**
Community-Management	**I**	**I**	**R/A**	**I**	**C**
OKR-Konsolidierung und Portfolio-Sync	**I**	**I**	**I**	**I**	**R/A**
Reporting an Direktion	**I**	**I**	**I**	**I**	**R/A**

R = Responsible, A = Accountable, C = Consulted, I = Informed, Direktion = Entscheidung wird über den Vorsitz direkt in der Direktion traktandiert.

3.2 Entscheidungslogik

Standardverfahren Fast-Track

Dezentrale Entscheidung im Fachbereich/Product Owner nach Em002-Checklisten der Bundeskanzlei; OSPO entscheidet abschliessend und informiert die Direktion summarisch.

Ausnahmen

Prüfung im OSPO (inkl. Recht/ISBO); Entscheidungsvorlage wird über Planung und Steuerung direkt in die Direktion gebracht.

3.2.1 Open-Source-Freigabe-Prozess

Die Open-Source-Freigabe erfolgt erst nach bestandenem Security-Gate:

- Der ISBO der Organisationseinheit bestätigt die Schutzbedarfsanalyse und den IT-Grundschutz;
- Bei erhöhtem Schutzbedarf: Überprüfung der ISDS-Massnahmen und deren Umsetzung;
- Prüfung auf sicherheitsrelevante Ausschlussgründe gemäss Art. 9 EMBAG;
- Dokumentation der Prüfung und Entscheidung.

Vereinfachtes Verfahren: Kleine Skripte werden in einem speziellen Repository zusammengefasst und durchlaufen als Sammlung einen einmaligen Freigabeprozess.

Datenschutz

Bei der Open-Source-Publikation sind die datenschutzrechtlichen Bestimmungen zwingend einzuhalten.

Code-Bereinigung vor Publikation

- Systematische Prüfung auf Personendaten in Quellcode, Konfigurationsdateien und Dokumentation;
- Entfernung von Testdaten, Logs und Kommentaren mit Personenbezug;
- Überprüfung von Datenbank-Schemas und API-Definitionen.

Besondere Vorsicht ist geboten bei

- besonders schützenswerten Personendaten (Gesundheit, Religion, usw.);
- Profiling-Algorithmen oder -Logik;
- Datenverarbeitungslogik mit Personenbezug;
- Hardcoded Credentials (z. B. im Code enthaltene Passwörter).

Verantwortlichkeiten

- Entwicklungsteams: Erstprüfung und Code-Bereinigung;
- Rechtsdienst: Datenschutzrechtliche Beurteilung;
- Freigabe durch OSPO nur nach Freigabe der Datenschutzprüfung.

Verbindliche Standards

- Coding-Guidelines und API-Guidelines sind einzuhalten. Code, der diese verletzt, wird nicht publiziert.
- Zusätzlich gelten Security Baselines (z. B. Secrets-Handling, Least Privilege) und Privacy by Design (Datenminimierung, Pseudonymisierung/Anonymisierung).

Alle datenschutzrechtlichen Prüfungen werden nachvollziehbar dokumentiert und bei Bedarf der zuständigen Datenschutzstelle vorgelegt.

3.2.2 Abstimmung Unternehmensarchitektur

Das OSPO stellt sicher, dass die Prüfungsprozesse, welche in der Unternehmensarchitektur VBS definiert sind, eingehalten werden. Insbesondere wird sichergestellt, dass die Freigabe mit der Architektursteuerung des Departements abgestimmt ist.

Die Konformitätsprüfung werden im Leitfaden zur Open-Source-Strategie näher erläutert.

3.3 Sicherheit und Datenschutz

Jeder Release durchläuft ein Security-Gate. Automatisierte Lizenz-/Dependency-Scans (z. B. FOSSology, OWASP Dependency-Check, Dependabot) werden genutzt. Der ISBO wird bei erhöhtem Schutzbedarf beigezogen. Eine verbindliche Datenschutz-Prüfung vor jeder Publikation ist durchzuführen. Alle Software-Lösungen müssen die bestehenden Informatiksicherheitsvorgaben des Bundes einhalten. Für jedes Schutzobjekt wird systematisch vorgegangen:

1. Schutzbedarfsanalyse P041 für jede Software-Lösung respektive pro Sammelrepository;
2. IT-Grundschutz Si001 sicherstellen;
3. Bei erhöhtem Schutzbedarf: Risikoreduktion durch geeignete technische und organisatorische Massnahmen;
4. Dokumentation in ISDS-Konzept P042 bei besonderen Sicherheitsanforderungen.

3.3.1 Urheberpersönlichkeitsrecht und Namensnennung

Das Urheberpersönlichkeitsrecht von Personen, die zu Open Source Software des BACS beitragen, bleibt unabhängig von der gewählten Lizenz vollumfänglich bestehen. Dies gilt sowohl für BACS-Mitarbeitende als auch für externe Contributors. Konkret bedeutet dies für das BACS, dass die Urheber intern erkennbar sind, jedoch gegen extern (Publikation) nicht mit Klarnamen erkennt werden können. Dabei wird ein Anonymsierungsverfahren eingesetzt.

3.3.2 Einstufungsverfahren

Open Source Community Building ist für das BACS ein strategisches Mittel, kein Selbstzweck. Das BACS orientiert sich am Stufenmodell mit den Ebenen Ausnahme, Minimalpublikation, Issue-Tracking und Community. Je höher die Stufe, desto grösser die Transparenz und die mögliche Interaktion - aber auch der damit verbundene Aufwand. Die Wahl der Stufe erfolgt nutzenorientiert entlang des Nutzens für das BACS, den Staat und die Öffentlichkeit, dem Reifegrad der Software, den verfügbaren Ressourcen und letztendlich auch der erwarteten Adoption. Open-Source-Entscheide werden dokumentiert, regelmässig überprüft und können jederzeit hoch- oder heruntergestuft werden - es besteht keine Pflicht zur aktiven Community, und eine Rückzugsmöglichkeit auf Minimalpublikation ist explizit vorgesehen. Ebenfalls kann die Software im Rahmen einer regelmässigen Überprüfung auch auf «Ausnahme» zurückgestuft werden.

Die Ausrichtung möglicher Unterstützung wird pro Publikation festgelegt: None, Best-Effort, Community oder gar Support gegen Kostendeckung. Das BACS definieret vorwiegend qualitative Reaktions- und Fix-Ziele ohne Rechtsanspruch (keine SLA). Als Transparenz-Mindeststandard gelten LICENSE, README, SECURITY.md und Hinweise zur Mitarbeit. Höhere Publikationsstufen werden mit Roadmap, Release-Politik und klarer Ansprechstelle publiziert. Insgesamt stellet das BACS sicher, dass Community-Aufwand, Sicherheitsanforderungen und öffentlicher Mehrwert in einem vernünftigen Gleichgewicht bleiben.

3.4 Reporting

Das OSPO berichtet der Direktion ein bis zwei Mal pro Jahr. Die Ergebnisse fliessen in den Jahresbericht des BACS ein. Zusätzlich dokumentiert das OSPO Kennzahlen (Publikationen, Wiederverwendung, Security-Advisories, Community-Aktivität) und leitet daraus Massnahmen ab.

3.5 Lizenzierung

Lizenzauswahl nach EMBAG-Vorgaben

Die Auswahl der Lizenz erfolgt gemäss Art. 9 Abs. 4 EMBAG und orientiert sich an international etablierten Lizenztexten. Für jede Software-Lösung wird die Lizenz nach fachlichen und rechtlichen Kriterien gemäss der Lizenzstrategie des BACS bestimmt.

Lizenzstrategie des BACS

Die Auswahl der Lizenz erfolgt gemäss dem Leitfaden Em002-3 für Open-Source-Lizenzen individuell für jede Softwarelösung.

Grundsätzlich wird die permissive MIT-Lizenz bevorzugt, um grösstmögliche Offenheit, Wiederverwendbarkeit und Integration in bestehende sowie zukünftige Systeme sicherzustellen.

Copyleft-Lizenzen (z.B. GPL (General Public License), AGPL (Affero General Public License)) werden bei Bedarf gezielt eingesetzt, wenn:

- gemeinschaftlich entwickelte Kernkomponenten vor proprietärer Vereinnahmung geschützt werden sollen;
- ein nachhaltiges Open-Source-Ökosystem gefördert werden soll;
- Reciprocity (Rückfluss von Verbesserungen) gewünscht ist.

Bei Cloud- und Web-Services wird die AGPL-Lizenz bevorzugt, um den Copyleft-Effekt auch bei netzwerkbasierter Nutzung sicherzustellen.

Lizenzkompatibilität und -Management

In jeder Software-Lösung muss sichergestellt werden, dass ausschliesslich Open-Source-Komponenten mit kompatiblen Lizenzen integriert werden. Dies wird systematisch dokumentiert:

- Lizenzregister pro Applikation mit allen verwendeten Komponenten oder Dokumentation als SBOM (Software Bill of Materials);
- Kompatibilitätsprüfung vor Integration neuer Abhängigkeiten.

Lizenzänderungen

Lizenzänderungen bedürfen einer Überprüfung durch das OSPO, um Konsistenz, Rechtssicherheit und Nachhaltigkeit zu gewährleisten. Dabei werden insbesondere die Auswirkungen auf bestehende Nutzerinnen und Nutzer und die Community-Entwicklung bewertet.

3.6 Open Source Know-How

Das BACS orientiert sich konsequent an den Open-Source-Hilfsmitteln der Bundeskanzlei (BK). Die Em002-Leitfäden, Checklisten und Vorlagen bilden den Open-Source-Leitfaden für Planung, Entwicklung, Freigabe und Publikation. Prozesse, Artefakte und Entscheide des BACS werden damit kompatibel gestaltet; Abweichungen sind zu begründen und zu dokumentieren. Erkenntnisse aus Pilotvorhaben (u. a. CSH) speist das BACS gezielt in die Weiterentwicklung der Hilfsmittel ein - inklusive Feedback zu Zentralisierungsfragen (z. B. gemeinsames Repository, Meldestellen, Standardbausteine).

Das BACS nimmt aktiv an der bundesweiten Open Source Community of Practice (CoP) teil. Ziele sind der systematische Wissensaustausch über Verwaltungsgrenzen hinweg, das Teilen von Best Practices und die gemeinsame Klärung von Rechts-, Sicherheits- und Betriebsfragen. Das BACS bringt eigene Erfahrungen, Fallbeispiele und Vorlagen ein, knüpft Kontakte zu Forschung und Wirtschaft und meldet Publikationen sowie relevante Erkenntnisse an die zentrale Stelle.

3.7 Prozess und Hilfsmittel

Der Leitfaden zusätzlich zur Open-Source-Strategie beschreibt den Open-Source-Prozess des BACS (Vorabklärung → Analyse/Aufbereitung → Freigabe/Publikation → Betrieb) und wird vom Open Source Program Office verantwortet und laufend gepflegt. Die EMBAG-Hilfsmittel (Em002, Wegleitungen, Checklisten) sind darin konsolidiert und verbindlich referenziert. Für jedes Projekt gelten Open Source Gates mit klaren Artefakten und definierter Ablage von Code und Dokumentation.

3.8 BACS Open-Source-Prozess

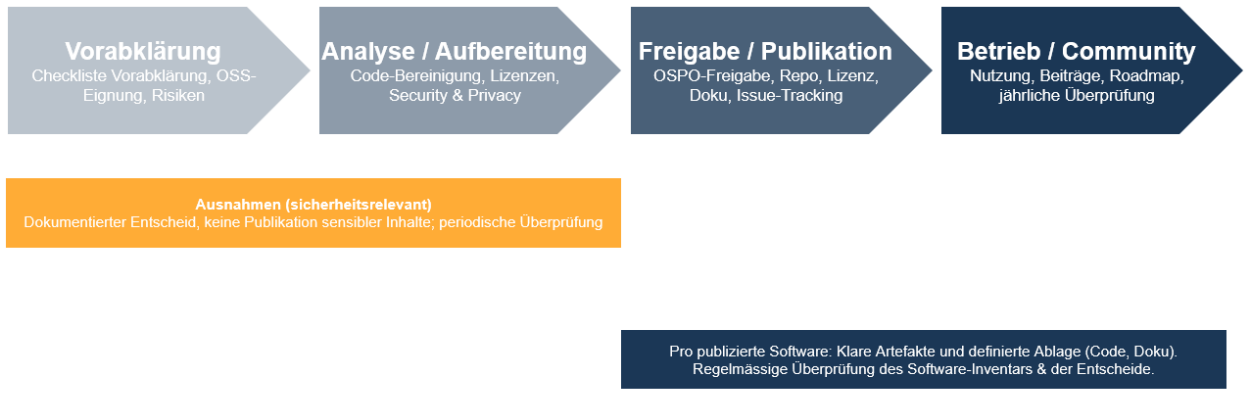

Abbildung 2: Open-Source-Prozess des BACS

4 Beschaffung und Verträge

Das BACS beschafft lizenz- und modelloffen mit Fokus auf digitale Souveränität, Lebenszykluskosten und Interoperabilität. Funktionale Ausschreibungen sind der Normalfall; Produkt-/Herstellerbindungen bleiben die Ausnahme.

Open Source kann explizit gefordert werden, wenn dies sachlich begründbar ist:

- digitale Souveränität;
- Vermeidung von Lock-ins;
- erwartete Anpassungen mit EMBAG-Publikationspflicht;
- Interoperabilität und offene Standards.

Die Regelung von Art. 9 EMBAG müssen stets mitberücksichtigt werden, sobald Eigen- oder Zusatzentwicklungen beabsichtigt werden.

4.1 EMBAG-Anwendung nach Beschaffungsart («Make or Buy»)

Beschaffungsart	Open-Source-Pflicht	Besonderheiten
Software selbst entwickeln	Ja (Art. 9 EMBAG)	gilt auch bei Weiterentwicklungen
Software entwickeln lassen	Ja (Art. 9 EMBAG)	Freigabe in Verträgen sicherstellen
Software extern kaufen	Bei Anpassungen	Freigabe in Ausschreibung vorsehen
Software «mieten« (SaaS)	Nein	keine Anpassungen = keine Pflicht
Übernahme von Software von anderer Bundesstelle	Bei BACS-Anpas-sungen	Annahme: Original meist schon publiziert
Entwicklungsressourcen einkaufen	Ja (Art. 9 EMBAG)	Vertragsbausteine für Publizierbarkeit
Koproduktion mit Behörden	Ja für neue Kreationen	Unentgeltliche Beiträge unproblematisch

Strategische Beschaffung – Gleichbehandlung mit Open-Source-Fokus

Bei Ausschreibungen sind alle Lizenz- und Geschäftsmodelle zulässig. Open Source kann als Eignungs- bzw. Bewertungskriterium dienen (u. a. digitale Souveränität sowie erwartete Anpas-sungen mit Publikationspflicht).

Digitale Souveränität als Kriterium

Beschaffungen gewichten Wechselfähigkeit, Gestaltungsfähigkeit und Einflussnahme als über-geordnete Ziele.

EMBAG frühzeitig integrieren

Früh einen Grundsatzentscheid zur Lizenzfamilie (permissiv vs. Copyleft) treffen. Markt-abklärung, Upstream-Optionen und Community-Setup in der Planungsphase vor der Ausschrei-bung klären. Provisorische EMBAG-Checklisten (z. B. Em002 2.1–2.3) zur Compliance nutzen.

Lifecycle-Management

SLAs inklusive Security-Fix-Policy und Update-Fähigkeit verlangen. SBOM-Pflichten festhalten. Subskriptions-/Supportmodelle als Bewertungskriterien berücksichtigen.

Offene Standards und Portabilität

Offene Standards sollen eingefordert werden, um Lock-ins zu minimieren und Interoperabilität zu sichern.

4.2 Vertragsgestaltung

4.2.1 Kernelemente für EMBAG-Compliance als Muss-Kriterien

- IP-Übergang zum Bund sicherstellen;
- Lizenzwahl und Publikationsrechte regeln;
- Contribution-Regeln und Community-Standards;
- Langzeitverfügbarkeit in anbieterunabhängigen Repositories.

4.2.2 Hilfsmittel

- Kriterien und Rahmenvertragsteile des Kompetenzzentrums für Beschaffungswesen (KBB);
- Wegleitung für Open-Source-Beschaffung des Bundesamtes für Bauten und Logistik (BBL);
- Em002-Vertragsbausteine für Publizierbarkeit.

4.2.3 Unentgeltliche Nutzung ≠ Beschaffung

Herunterladen/Verwenden von Open Source ohne Entgelt ist kein Beschaffungsvorgang. Die Dienstleistungen können später regelkonform beschafft werden.

Details und weiterführende Links zur Beschaffung sind im Open-Source-Leitfaden zu finden.

4.3 Umgang mit Legacy Software

Grundsatz: Geordnete Überführung. Veröffentlicht wird, was rechtlich und sicherheitstechnisch möglich ist – der Rest bleibt bis zur Klärung ausgeschlossen.

Vorgehen:

Abbildung 3: Vorgehen im Umgang mit Legacy Software

Governance für Legacy-Fälle:

- Entscheid durch Open Source Program Office;
- Ausnahmen befristet und dokumentiert;
- jährlicher Review der Legacy-Fälle.

5 Risiken und Standards beim BACS

Risiko	Standard BACS	Mögliche Mitigationsmassnahmen
R01 Legitimität und Compliance Spannungsfeld «Open Source by Default» vs. Ausnahmen führt zu inkonsistenten Entscheiden.	Ausnahmen eng, befristet, dokumentiert; jährlicher Review nach klaren Kriterien.	• Einheitliches Ausnahmeverfahren; • Entscheid durch OSPO + Rechtsdienst + ISBO/DSBO; • Zentrales Ausnahmen-Register und KPIs; • Schulungen der Projektleitenden.
R02 Sicherheit Offenheit erhöht Angriffsfläche/-wahrscheinlichkeit.	Sicherheit vor Features; Publikation nur nach Security-Prüfung.	• ISBO/DSBO-Gate vor jedem Release; • SAST/DAST/Dependency-Scans und SBOM; • Vulnerability-Disclosure-Policy; • Patch-/Backport-Prozess; • Security-Champions je Team.
R03 Digitale Souveränität und Vendor-Unabhängigkeit Abhängigkeiten (Cloud/CI/Repos/Build-Chains) strategische Ziele.	Offene Standards, Portabilität und Exit-Pläne sind der Standard.	• Reproducible Builds; • Repo-Mirrors und Backups; • Daten-/Artefakt-Egress in SLAs; • Lizenz-/Daten-Escrow; • Offene Tools und Formate.
R04 Ökosystem und Wiederverwendung Forks/Fragmentierung oder geringe Adoption schwächen Wirkung.	API-Stabilität, klare Roadmaps, aktives Community-Management; Kompatibilität vor Features.	• geregelte Release-Cadence; • Contributing and Governance; • Frühe Einbindung von Partnern.
R05 Reputation und Vertrauen Sicherheitsvorfälle oder falsche Support-Erwartungen; Nutzung nicht mehr gepflegter Software.	Transparente Kommunikation; klarer Support-Scope und Reaktionswege; «Unmaintained» deklarieren.	• Incident-Response-Playbook; • SECURITY.md undSUPPORT.md • Status-Badges (Build, Coverage, Maintained); • EOL-Policy; • SLA-Klassen und Kontaktkanäle.
R06 Recht und IP-Klarheit Unsaubere Rechtekette oder Lizenzinkompatibilitäten blockieren Publikation.	Initiale Rechts- und Datenschutzanalyse; Vertrags-Compliance; Lizenz-Whitelist; IP-Abtretung; OSS-Vorgaben in Beschaffungen.	• Automatisierte Lizenz-Scans und Third-Party-Notices; • Inbound/Outbound-Lizenzleitfaden; • Provenance-Nachweise in SBOM.
R07 Ausführungsfähigkeit und Ressourcen Open Source by-Default kollidiert mit Projekt-/Betriebslast → Verzögerungen.	Verbindliche Kapazitäten für Aufbereitung, Doku und Community; klare Priorisierung.	• MVP-Publikation mit stufenweisem Ausbau; • RACI-Matrix für die beteiligten Rollen; • Release-Kalender und Puffer • Separater «Publish-Hardening»-Backlog; • Fixe Budget- und Zeitblöcke.
R08 Finanzierung und Nachhaltigkeit Laufende Aufwände (Security, Wartung, Doku, Community) werden unterschätzt; OpEx/SLAs ungenügend abgebildet.	Lifecycle-Finanzierung (CapEx + OpEx); Wartung/Security/Doku/Community explizit ausschreiben; TCO- und Nutzenbasis für Priorisierung.	• Mehrjahresverträge und SLAs; • Co-Finanzierung und Partnerschaften; • Contribution-Programme; • Minimalpublikation mit Ausbau-Roadmap.
R09 Daten und Privatsphäre Leaks über Code, Tickets, Logs oder Dokumentation.	Privacy-by-Design; Redaktionsregeln; Trennung vertraulicher Artefakte; Minimaldatenprinzip.	• Private Issue Queues für sensitive Tickets; • Anonymisierte Demo-Daten; • Pre –Publish –Privacy Checklist.
R10 Interoperabilität und Qualität Unscharfe Standards und schwankende Codequalität beeinträchtigen Wiederverwendung.	Architekturprinzipien; Definition of Ready/Done; SemVer-Konformität; Kompatibilität als Default.	• Coding- und API-Guidelines; • CI-Quality-Gates (Linting, Tests, Coverage-Schwellen); • Contract-/Kompatibilitätstests.

6 Anhang

6.1 Quellenverzeichnis

Titel	Quelle / Autor	Link	Stand
BBl 2023 787 – Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBAG)	Bundesrat / Bundeskanzlei	fedlex.admin.ch	22.11.2023 (in Kraft: 01.01.2024). (News.admin.ch)
EMBAG macht Open Source Software zur Norm: Chance und Verpflichtung für die Bundesverwaltung	APP Unternehmens-beratung AG (Thomas Häfliger)	app.ch	11.07.2024. (APP Unternehmensberatung AG)
Erläuterungen zur Verordnung über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBAV)	Bundesrat / Bundeskanzlei	PDF	22.11.2023. (Newsd)
Em002 Strategischer Leitfaden Open Source Software in der Bundesverwaltung	Bundeskanzlei, Bereich DTI	PDF	14.03.2025. (bk.admin.ch)
Em002-1 Praxis-Leitfaden Open Source Software in der Bundesverwaltung	Bundeskanzlei, Bereich DTI	PDF	14.03.2025. (bk.admin.ch)
Em002-2 Anleitung zur Veröffentlichung von Open Source Software	Bundeskanzlei, Bereich DTI	PDF	14.03.2025. (bk.admin.ch)
Em002-2.1 Checkliste Vorabklärung	Bundeskanzlei, Bereich DTI	DOCX	14.03.2025. (bk.admin.ch)
Em002-2.2 Checkliste Analyse und Aufbereitung	Bundeskanzlei, Bereich DTI	DOCX	14.03.2025. (bk.admin.ch)
Em002-2.3 Checkliste Freigabe und Publikation	Bundeskanzlei, Bereich DTI	DOCX	14.03.2025. (bk.admin.ch)
Em002-3 Leitfaden Open Source-Lizenzen	Bundeskanzlei, Bereich DTI	PDF	11.03.2025. (bk.admin.ch)
Em002-4 Leitfaden Open Source-Community	Bundeskanzlei, Bereich DTI	PDF	11.03.2025. (bk.admin.ch)
Em002-4.1 Checkliste Open Source-Community	Bundeskanzlei, Bereich DTI	DOCX	14.03.2025. (bk.admin.ch)
Em002-5 Faktenblatt EMBAG und Open Source	Bundeskanzlei, Bereich DTI	PDF	11.03.2025. (bk.admin.ch)
Em002-6 Open Source-FAQ	Bundeskanzlei, Bereich DTI	PDF	14.03.2025. (bk.admin.ch)
Em002-7 Merkblatt Open Source-Hilfsmittel	Bundeskanzlei, Bereich DTI	PDF	14.05.2025. (bk.admin.ch)
IT-Beschaffungen 2.0: Die Handbremse lösen! (Konferenzband)	Koch / Biehl / Fischer (Hrsg.), Dike	dike.ch	2025. (DIKE Verlag)
Merkblatt KBB: Beschaffung Software - Artikel 9 EMBAG	Bundeskanzlei (DTI) und Kompetenzzentrum Beschaffungswesen Bund (BBL/KBB)	PDF	13.08.2025. (bk.admin.ch)
«Open-by-Default» (Förderung der digitalen Nachhaltigkeit), v60	Bundeskanzlei, Bereich DTI	– (lokale Kopie)	26.08.2025
Studie: Technologische Perspektive der digitalen Souveränität	Prof. Dr. Matthias Stürmer (BFH)	bfh.ch (PDF)	12.06.2024. (Berner Fachhochschule)
UA-Prinzipien VBS	Confluence (Intern – nicht öffentlich)	Confluence	26.09.2025

Umsetzung EMBAG Art. 9 im Bund (Folien-satz HV CH-Open)	Bruno Schöb, Bundeskanzlei DTI	ch-open.ch (PDF)	21.03.2024. (CH Open)
Wegleitung Open Source in der Beschaffung	Bundesamt für Bauten und Logistik (BBL)	– (lokale Kopie)	2025

Relevante Absätze aus der Cybersicherheitsverordnung:

- Art. 8 Abs. 4: «Das BACS ist für die Sicherheit des Kommunikations- sowie der Informationssysteme und die Rechtmässigkeit der Bearbeitung der Daten verantwortlich.»
- Art. 11 Abs. 4: «Das BACS entscheidet über die Veröffentlichung von freigegebenen Informationen.»

6.2 EMBAG Art. 9

Neue gesetzliche Grundlage im EMBAG Artikel 9 → 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.