Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK

**Digitale Transformation und IKT-Lenkung DTI**

14.09.2026

# Em002-2.2 Checkliste OSS-Analyse und -Vorbereitung

Version 2.0-85c0f18

# Inhaltsverzeichnis

Diese Checkliste ist Teil von *Em002-2 Anleitung zur Veröffentlichung von Open-Source-Software* und richtet sich an IKT-Fachpersonen.
Sie dient der Überprüfung der Dokumentation und des Quellcodes eines Projekts. Damit hilft sie sicherzustellen, dass die Qualität der Dokumentation ausreicht, um eine Anwendung als Open Source zu veröffentlichen. Zudem lässt sich damit prüfen, ob der Quellcode und alle vom Projekt verwendeten Drittkomponenten keine rechtlichen Risiken bergen. Diese Massnahmen minimieren Sicherheitsrisiken.
Informationen zu dieser Checkliste finden sich in *[Em002-2]* in Kapitel 4.

Darüber hinaus stellt diese Checkliste sicher, dass die Projektdokumentation Endnutzende und technische Fachpersonen gleichermassen anspricht.

## 1. Gegenstand

### 1.1. Name und Kurzbeschreibung der Software

Tragen Sie den Namen der Software ein.

### 1.2. Ansprechperson und Prüfung

Nennen Sie die Organisation, die Ansprechperson der Fachstelle sowie die verantwortlichen Personen (z. B. ISBO/DSBO), welche die Einhaltung der Veröffentlichungsvorgaben geprüft haben.

## 2. Checkliste

☐ Die *Em002-2.1 Checkliste OSS-Vorabklärung* wurde ausgefüllt und es wurden keine problematischen Punkte festgestellt.

☐ Der zu veröffentlichende Quellcode wurde analysiert.

Prüfen, wie die bestehende Codequalität und die Richtlinien umgesetzt wurden.

Sicherstellen, dass keine sensiblen (Test-)Daten enthalten sind, z. B. Daten, die auf realen Personen oder Fällen beruhen.

Aktuelle Dokumentation (siehe [Em002-2] Anhänge D.1. und D.2.)

Unnötige Dateien oder veraltete Dokumente löschen.

Code auf Secrets/Zugangsdaten prüfen.[1]

Gezielte Sicherheitstests durchführen und anschliessend ein (öffentliches) Bug-Bounty-Programm einrichten.[2]

1. https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2022/git.html
2. https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-it-spezialisten/themen/bug-bounty-programme.html

Alle verwendeten Bibliotheken prüfen, ob die Lizenzen vorliegen und entsprechende Listen (Attributionen) erstellt wurden.

Beschreibung des Deployments (CI/CD-Pipeline[3]) und gegebenenfalls Aufbau einer Demo-Instanz.

☐ Lizenzwahl

Allfällige Abhängigkeiten von bestehenden Lizenzen prüfen.

Bei Drittcode die Nutzungsbedingungen auf Kompatibilität mit der vorgesehenen Lizenz prüfen und den Code nötigenfalls ersetzen.

Die passende Lizenz anhand des Leitfadens «Em002-3 Leitfaden OSS-Lizenzierung» auswählen (primäre Empfehlungen sind AGPL für Copyleft und MIT für permissiv).

Gewählte Lizenz und Begründung

☐ Die Dokumentation wird zusammen mit dem Quellcode abgelegt (siehe [Em002-2] Anhang D.1.)

Begründung/Ablageort

☐ Die Dokumentation spricht sowohl Endnutzende als auch technische Fachpersonen an.

Liste der zentralen Dokumentation

☐ Ausführliche Dokumentation des Quellcodes (OSS-spezifisch)

Wichtige Standarddokumentation (README, LICENSE, CONTRIBUTING usw.) ist vorhanden.

☐ Der Quellcode enthält einschliesslich Historie keine sensiblen, geschützten oder vertraulichen Personendaten. Oder die Historie wurde vollständig gelöscht. (siehe [Em002-2] Anhang E.2.)

Erläuterung der Prüfung (falls nicht als separates Dokument abgelegt)

☐ Mit dem Lieferanten und allen beteiligten Entwicklerinnen und Entwicklern innerhalb der Bundesverwaltung wurde geklärt, ob Autorenangaben (Namen, E-Mail-Adressen) veröffentlicht werden dürfen.
Alternativ wurde der Quellcode einschliesslich Historie bereinigt/anonymisiert.

☐ Die vom Projekt verwendeten Bibliotheken sind mit der Lizenz des Projekts kompatibel.

Erläuterung der Prüfung (falls nicht als separates Dokument abgelegt)

☐ Das Projekt verwendet einen Paketmanager zur Verwaltung seiner Abhängigkeiten.

☐ Das Projekt deklariert seine Lizenz im entsprechenden Deskriptor des Paketmanagers. Erstellung einer Software Bill of Materials (SBOM), die alle verwendeten Open-Source-Komponenten auflistet.

☐ Der Quellcode enthält eine Datei *THIRD-PARTY-LICENSES.md*, die für jede verwendete Bibliothek aufführt: den Projektnamen der Bibliothek, die Homepage der Bibliothek, den SPDX-Identifikator der Lizenz der Bibliothek sowie einen Link auf die Lizenz der Bibliothek.

☐ Bei Anwendungen steht ein «Über»-Dialog zur Verfügung, der auf die Datei *THIRD-PARTY-LICENSES.md* verweist.

3. https://de.wikipedia.org/wiki/CI/CD

☐ Im Rahmen des Code-Review-Prozesses wird sichergestellt, dass die Datei *THIRD-PARTY-LICENSES.md* bei jeder Änderung an den Bibliotheken nachgeführt wird.

## 3. Schlussbemerkungen

Bemerkungen und Verweise auf weitere relevante Dokumente

| |
|---|
| |

**Ablage des Formulars**

Legen Sie dieses Formular bei der Projektdokumentation und/oder gemäss den Vorgaben Ihrer Behörde (Organisationseinheit) ab.