**27 November 2025** | National Cyber Security Centre (NCSC)

# NCSC Open Source Strategy

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence,
Civil Protection and Sport DDPS
**National Cyber Security Centre NCSC**

# Contents


**Management summary** ..... **3**

**1 Initial situation, context and need for action** ..... **4**

*1.1 Scope and publication logic* 4

*1.2 Principles of implementation* 5

**2 NCSC open source strategy** ..... **6**

*2.1 Objectives and added value* 6

*2.2 Guiding principles* 7

*2.3 Recommendations for existing software, scripts and new developments* 8

**3 Governance and decision-making processes** ..... **9**

*3.1 Open Source Programme Office (OSPO)* 9

*3.1.1 Roles in the OSPO* ..... 9

*3.1.2 OSPO RACI* ..... 10

*3.2 Decision logic* 10

*3.2.1 Open source release process* ..... 10

*3.2.2 Coordination of enterprise architecture* ..... 11

*3.3 Security and data protection* 11

*3.3.1 Moral rights and attribution* ..... 12

*3.3.2 Classification procedure* ..... 12

*3.4 Reporting* 12

*3.5 Licensing* 12

*3.6 Open source expertise* 13

*3.7 Process and tools* 13

*3.8 NCSC open source process* 14

**4 Procurement and contracts** ..... **14**

*4.1 EMOTA application by procurement type ('make or buy')* 14

*4.2 Contract drafting* 15

*4.2.1 Core elements for EMOTA compliance as mandatory criteria* ..... 15

*4.2.2 Tools* ..... 15

*4.2.3 Free use ≠ procurement* ..... 15

*4.3 Dealing with legacy software* 15

**5 Risks and standards at the NCSC** ..... **17**

**6 Annex** ..... **18**

*6.1 Sources* 18

*6.2 Article 9 EMOTA* 19

# Management summary

The National Cyber Security Centre (NCSC) is implementing 'open source by default' under EMOTA. All new software developments will be published as open source. Exceptions require justification, documentation and periodic review. Existing applications will be systematically reviewed on a voluntary basis and progressively opened up where proportionate and feasible.

Note: This key decision implements Article 9 of the Federal Act on the Use of Electronic Means to Carry Out Official Tasks (EMOTA; SR 172.19, available in de, fr, it) within the NCSC, building on guidelines, checklists and instructions published by the Federal Chancellery. The accompanying OSS guidelines set out how the strategy applies in practice.

The NCSC implements open source under EMOTA as a working principle, with clear rules and responsibilities. The objectives are digital sovereignty, quality and speed at affordable cost. Security and legal compliance are paramount. Publications are made responsibly and in stages where necessary.

## Strategic framework and licences

The NCSC pursues open source by default. Permissive licences (e.g. Apache-2.0/MIT) are standard for broad reuse; copyleft/EUPL licences are used where feedback from adaptations or dependencies points in this direction. Licence whitelisting, clean chain of title/IP assignment and inbound/outbound compliance are mandatory. Publications go into open repositories with OSPO (Open Source Programme Office) governance, defined release gates, roadmaps and changelogs. Security and data protection take top priority: all publications require prior formal approval by IT Security Officers for the organisational unit/department. Publication scope (modules/artefacts) is limited where necessary.

## Impact through contributions and co-development

Active third-party participation is central: clear contribution rules, transparent roadmaps/backlogs, stable interfaces and predictable releases facilitate contributions and accelerate further development.

## Implementation and consolidation

Implementation rests on an open source governance policy, clear responsibilities (OSPO, legal service, specialist units) and a set of guidelines with checklists, roles and templates. This creates consistency from planning and procurement through to operation and community engagement. Procurement and contracts build in open source and security requirements from the start.

# 1 Initial situation, context and need for action

### Digitalisation, sovereignty, interoperability

Internationally, open solutions that enable transparency, reusability and cooperation are gaining ground. Open source increasingly serves as a strategic lever for reducing dependence on individual vendors, ensuring interoperability and harnessing the innovative power of ecosystems. The principle of 'public money, public code' is also gaining traction in Switzerland.

Security-critical functions are increasingly shifting to software-driven processes. Source code visibility, reproducible builds and traceable supply chains (e.g. component lists/SBOM, signed releases) are becoming prerequisites for comprehensive risk management, both internally and in exchanges with partners. Open components promote reuse across administration, research and business while strengthening digital sovereignty by keeping expertise and creative freedom within the country.

### Legal basis

Since 1 January 2024, Article 9 EMOTA has provided binding legal grounds. Federal authorities must disclose the source code of software they develop or commission for fulfilling their tasks, unless third-party rights or security reasons preclude this (Art. 9 para. 1 EMOTA). Software should be released as open source whenever possible and appropriate – authorities have discretion over specific implementation. The Federal Chancellery supports uniform implementation across federal authorities through guidelines, checklists and instructions for publishing open source software.

### Which software is affected?

Article 9 EMOTA covers all software that federal authorities develop or commission for fulfilling their duties. The definition is deliberately broad. For the NCSC, this includes:

- Applications, modules and platforms (e.g. Cyber Security Hub [CSH])
- Libraries and components
- Scripts, automations and configurations
- Algorithms and models (if created in-house)

Third-party software products acquired unchanged are excluded, as are pure datasets, configuration files and design elements.

## 1.1 Scope and publication logic

### Scope of application of the open source strategy

The open source strategy binds all NCSC areas and projects. It applies to all software solutions the NCSC develops, commissions or operates – both new developments and existing applications. The strategy underpins project decisions, architectural specifications and procurement processes.

### Boundary

Open source work divides into two categories: procurement of existing components as opposed to software creation/development followed by publication by the federal government. Article 9 EMOTA covers only the latter. Purchase/use (out → in): Not covered by Article 9 EMOTA; no obligation to publish code. Focus is on procurement, deployment and licence compliance.

### Creation/further development (in → out)

Covered by Article 9; source code must always be published. Exceptions apply only for third-party rights or security-critical reasons. Publication uses a suitable open source licence; services such as integration, operation or support can continue on a cost-covering basis.

### Practical consequences

Simply using existing software does not trigger any obligations under Article 9 EMOTA. Where proprietary code is created or existing code substantially developed (including in partial packages), Article 9 EMOTA applies. Exceptions always require justification and documentation.

### Publication logic

Different levels of involvement in open source publication:

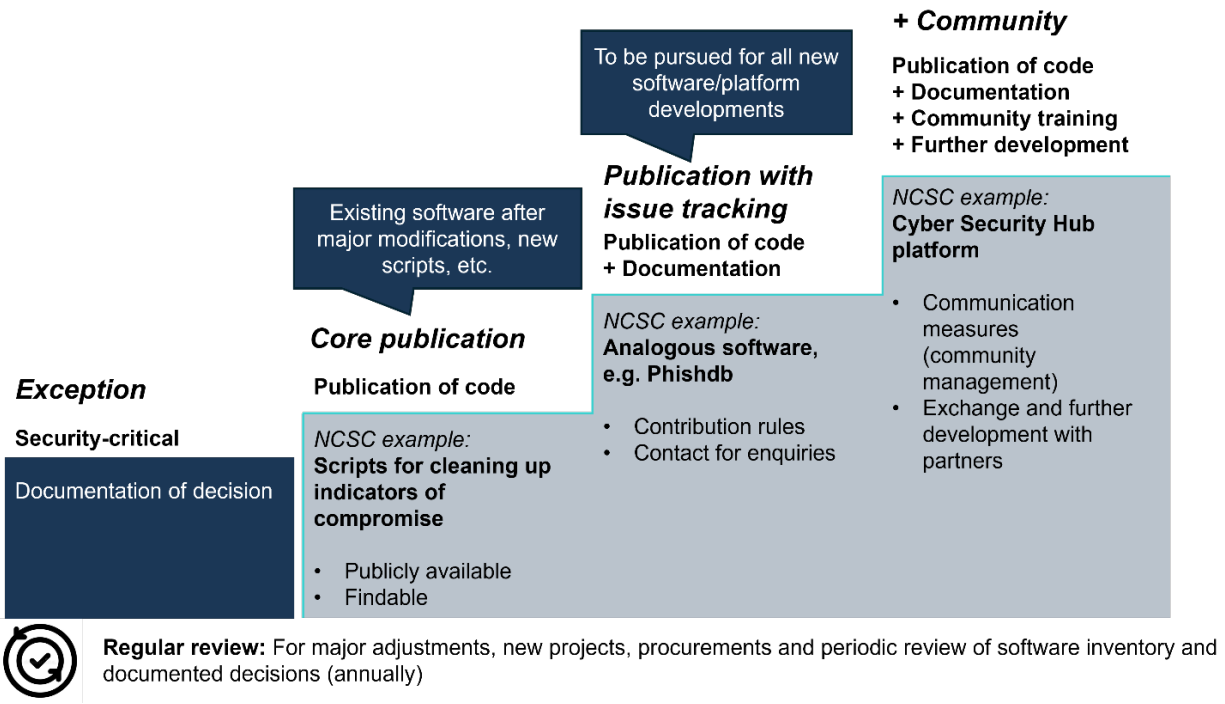


Figure 1: NCSC step-by-step open source model

## 1.2 Principles of implementation

### Appropriateness and proportionality

Publication under EMOTA occurs only where possible and appropriate. It may be omitted if:

- Third-party rights cannot be acquired on reasonable terms;
- Confidentiality considerations argue against it.

Publication follows the principle 'as open as possible, as restrictive as necessary':

- Core publication – minimum variant: publication of the code;
- Publication with issue tracking: errors or defects can be reported and addressed;
- Publication with sponsored community contributions;
- No publication – justified exception.

This keeps openness and security in balance while ensuring publication remains appropriate and sustainable.

### Licensing and legal relationships

Rights are granted through private-law licences (Art. 9 para. 3 EMOTA). Internationally established licence texts should be used where possible and appropriate (Art. 9 para. 4 EMOTA). Liability claims by licensees are excluded to the extent legally permissible.

### Responsibilities and implementation

The NCSC is responsible for implementing Article 9 EMOTA itself. There is explicitly no central federal responsibility – implementation is decentralised to individual administrative units. Newly created software or software undergoing major releases must always be published.

### Supplementary services

The NCSC may provide supplementary services (integration, maintenance, support) where these fulfil official tasks and can be provided at reasonable cost (Art. 9 para. 5 EMOTA). These services are charged at cost-covering rates (Art. 9 para. 6 EMOTA).

### Need for action for the NCSC

'Open source by default' is now standard. Exceptions must be clearly justified, documented and regularly reviewed. The approach requires structured governance rather than ad hoc decisions: transparent roles, defined processes and clear responsibilities for security and quality. This reconciles the legal disclosure obligation with the NCSC's security and efficiency objectives.

# 2 NCSC open source strategy

## 2.1 Objectives and added value

The NCSC consistently implements 'open source by default' under Article 9 EMOTA: new developments are always published openly. Exceptions are justified, documented and periodically reviewed. Existing applications are systematically assessed for openness and gradually opened up where proportionate and feasible. Existing open source components take preference. Partnerships are utilised, skills developed strategically, and active contributions made to projects in use. Transparent architectural decisions, roadmaps and changelogs ensure quality, added value and reuse.

### Objectives and added value:

#### For the NCSC

- Reliable EMOTA implementation, expanded digital sovereignty, and quality and efficiency gains in software development.
- Uniform processes, clear governance and a professional open source approach create legal certainty and enable sustainable cooperation with public and private partners.

#### For Switzerland

- 'Public money, public code': software developed with public funds becomes reusable.
- Reuse saves costs, reduces duplication and promotes shared digital infrastructure across administrative levels.

#### For partners

- Fee-free licences (Art. 9 para. 2 EMOTA), transparent development processes and low barriers to entry create new opportunities for participation and further development.
- This builds an ecosystem of reusable digital public goods that accelerates innovation and knowledge transfer.

## 2.2 Guiding principles

These principles make 'open source by default' concrete. They provide binding guidance for decisions, implementation and prioritisation – from architectural decisions through to publication. They also align with DDPS reference architecture principles.

#### Security, data protection and sustainable operation

Security and data protection are non-negotiable. The NCSC builds these in from the start and publishes only after thorough verification. Sensitive information stays unpublished. Vulnerabilities are handled responsibly and communicated openly when reasonable. To keep releases viable, the NCSC factors in maintenance, security fixes, documentation and, where necessary, community engagement, reduces technical debt and proceeds step by step. The NCSC will expand publications and community activities only once need or benefit is identified.

#### Targeted publication

Security-critical components get either minimal publication or justified exceptions. Non-critical software gets full transparency. Publication scope depends on confidentiality, third-party rights and reuse purpose. Decisions are documented clearly, time-limited and reviewed regularly – always under applicable regulations.

#### Commitment and standardisation

A clear NCSC open source process produces transparent decisions on open source, exceptions, licences and publications. Exceptions are temporary and justified, reviewed periodically. Decisions get audit-proof documentation. Legal and regulatory requirements (information security, data protection, copyright/trademark law) are integrated throughout.

### Collaboration, reuse-first and interoperability

Reuse takes priority over new development: existing open source components are systematically reviewed and preferred. Solutions are designed API-first and standards-based to ensure integration and interchangeability. External contributions from administration, research and industry are actively encouraged. The NCSC also participates actively in relevant open source projects. International and industry-specific standards are preferred.

## 2.3 Recommendations for existing software, scripts and new developments

### New developments

Open by default. All new applications and modules developed on behalf of or under NCSC responsibility are published under suitable open source licences as standard, unless third-party rights or overriding protection interests conflict.

Software developed after 1 January 2024 falls directly under Article 9 EMOTA and must in principle be published. For older applications: release is reviewed when major changes or new major releases are pending. Where significant third-party interest exists, voluntary publication may be considered – possibly with cost sharing and community establishment.

### Scripts and microcode for daily support

Separate publication is generally not worthwhile for smaller scripts. Proportionality applies in this category. Such scripts can be bundled in dedicated repositories undergoing one-time approval. The NCSC or GS-DDPS can provide a collective repository for smaller scripts.

### Dealing with existing software

Existing applications get systematic review – initially during open source strategy development, then regularly. Decisive factors are proportionality, security, third-party usability, third-party rights and available resources. Where appropriate and feasible, existing applications will be gradually prepared for publication or published in parts (e.g. interfaces, documentation, non-security-critical modules).

The legislation does not require retroactive publication of older applications. Nevertheless, each new major version is assessed for full release possibility. Otherwise, at least minimal publication or documented exception must be provided.

# 3 Governance and decision-making processes

The governance and decision-making processes are outlined below. The OSS Strategic Guidelines provide further details.

## 3.1 Open Source Programme Office (OSPO)

The NCSC has established an Open Source Programme Office (OSPO) to deliver its open source strategy. This is a virtual structure, not a separate division, coordinated by Planning and Control within the NCSC. It draws on expertise in technology, law, information security and community engagement as required, designed for a lean organisation like the NCSC. The OSPO operates through an effective core team with clear responsibilities and short decision-making paths, avoiding complex committee structures.

Planning and Control chairs the OSPO, coordinates procedures and maintains the liaison with Management, including scheduling major publications and discussing exceptions.

### 3.1.1 Roles in the OSPO

#### Product Owner (Project Management / PO of the application)

Leads operational implementation; prepares documentation, checklists and initial security/licence checks; submits publication proposals to the OSPO.

#### Development teams / suppliers (knowledge carriers)

Ensure code quality, security standards and licence compliance; provide component and licence information; create documentation to the PO's specifications.

#### Community Manager

Handles external communication, contribution guidelines, issue management and transparency (README, SECURITY.md, roadmap depending on stage); engages with the community and maintains regular exchange.

#### Legal Service and ISBO

Address third-party rights, data protection, licence selection and security clearances. Consulted by the OSPO as required.

#### OSPO Chair (coordinated through Planning and Control)

Reviews documents, approves publications (fast track) and escalates exceptions directly to Management. Documents all decisions (publication, exceptions, licence selection) and provides consolidated half-yearly reporting to Management, with ad hoc reporting as needed. Maintains the open source strategy, guidelines and tools. Coordinates with other organisational units working on open source matters, such as the Federal Chancellery and GS-DDPS.

### 3.1.2 OSPO RACI

The RACI matrix below sets out roles and responsibilities for OSPO participants (RACI: Responsible, Accountable, Consulted, Informed).

| Task / Role | PO | Development | Community Manager | Legal Service / ITSO | OSPO |
|---|---|---|---|---|---|
| **Documentation and processing** | **C** | **R** | **I** | **I** | **A** |
| **Licence and component check** | **R** | **C** | **I** | **C** | **A** |
| **Security checks** | **C** | **R** | **I** | **C** | **A** |
| **Publication decision (fast track)** | **I** | **I** | **I** | **C** | **R/A** |
| **Publication decision (exception)** | **I** | **I** | **I** | **C** | **R/A Management** |
| **Community management** | **I** | **I** | **R/A** | **I** | **C** |
| **OKR consolidation and portfolio synchronisation** | **I** | **I** | **I** | **I** | **R/A** |
| **Reporting to Management** | **I** | **I** | **I** | **I** | **R/A** |

R = Responsible, A = Accountable, C = Consulted, I = Informed, Management = Decision is placed on the agenda directly by the chairperson.

## 3.2 Decision logic

#### Standard procedure (fast track)

Decentralised decision at unit/PO level following Federal Chancellery Em002 checklists; OSPO makes final decision and provides summary reporting to management.

#### Exceptions

OSPO review (including Legal/IT Security Officer); decision template submitted directly to Management via Planning and Control.

### 3.2.1 Open source release process

Open source releases proceed only after passing the security gate:

- IT Security Officer of the organisational unit (ITSO-O) confirms protection needs analysis and IT baseline protection;
- For increased protection needs: ISDP measures reviewed for implementation;
- Examination for security-critical exclusion grounds under Article 9 EMOTA;
- Documentation of examination and decision.

Simplified procedure: Small scripts grouped in a dedicated repository undergo single collective approval process.

#### Data protection

Open source publications must strictly observe data protection regulations.

#### Code clean-up prior to publication

- Systematic checking for personal data in source code, configuration files and documentation;
- Removal of test data, logs and comments containing personal information;
- Review of database schemas and API definitions.

#### Particular caution required for:

- Particularly sensitive personal data (health, religion, etc.);
- Profiling algorithms or logic;
- Data processing logic relating to personal data;
- Hardcoded credentials (e.g. passwords in code).

#### Responsibilities

- Development teams: initial review and code clean-up;
- Legal service: data protection assessment;
- OSPO approval only after data protection review completed.

#### Binding standards

- All code must comply with coding and API guidelines. Non-compliant code will not be published;
- Security baselines (e.g. secrets handling, least privilege) and privacy by design principles (data minimisation, pseudonymisation/anonymisation) apply throughout.

All data protection checks require comprehensive documentation and submission to the responsible data protection authority where necessary.

### 3.2.2 Coordination of enterprise architecture

The OSPO ensures compliance with DDPS corporate architecture audit processes, particularly coordination with departmental architecture management for all releases.

The OSS Strategic Guidelines provide further details on conformity testing.

## 3.3 Security and data protection

Every release passes through a security gate. Automated licence/dependency scans (e.g. FOSSology, OWASP Dependency Check, Dependabot) support this. ITSO engagement is required for increased protection needs. Mandatory data protection checks precede every publication. All software solutions must meet federal government IT security requirements. Each protected object follows a systematic approach:

1. Protection needs analysis P041 for each software solution or collective repository;
2. IT baseline protection Si001;
3. For increased protection needs: risk reduction through appropriate technical and organisational measures;
4. Documentation in ISDP concept P042 for special security needs.

### 3.3.1 Moral rights and attribution

Contributors to NCSC open source software retain full moral rights, regardless of licence. This applies equally to NCSC employees and external contributors. In practice, authors remain identifiable internally but are anonymised in external publications. An anonymisation process handles this.

### 3.3.2 Classification procedure

Open source community building serves as a strategic tool for the NCSC, not an end in itself. The NCSC operates a tiered model: exception, minimal publication, issue tracking and community. Higher levels bring greater transparency and interaction potential – but also greater resource requirements. Level selection weighs the benefits for the NCSC, state and public against software maturity, available resources and expected adoption. Open source decisions are documented and regularly reviewed, with flexibility to upgrade or downgrade. Active community management is not mandatory; reverting to minimal publication remains an explicit option. Regular review may also result in downgrading to 'exception' status.

Support focus is determined per publication: none, best effort, community or cost-based support. The NCSC sets qualitative response targets without legal entitlement (no SLA). Minimum transparency standards comprise LICENSE, README, SECURITY.md and collaboration instructions. Higher publication levels include roadmaps, release policies and clear points of contact. The NCSC maintains reasonable balance between community effort, security requirements and public value.

## 3.4 Reporting

The OSPO reports to Management once or twice annually. Results feed into the NCSC Annual Report. The OSPO tracks key metrics (publications, reuse, security advisories, community activity) and derives action points accordingly.

## 3.5 Licensing

#### Licence selection under EMOTA

Licence selection follows Article 9 paragraph 4 EMOTA, using internationally established licence texts. Each software solution's licence is determined by technical and legal criteria according to the NCSC licensing strategy.

#### NCSC licensing strategy

Licences are selected individually per software solution following Em002-3 guidelines for open source licences.

**The permissive MIT licence is preferred by default** to maximise openness, reusability and integration into existing and future systems.

Copyleft licences (e.g. GPL (General Public Licence), AGPL (Affero General Public Licence)) are deployed where necessary when:

- Jointly developed core components require protection from proprietary appropriation;
- A sustainable open source ecosystem needs promotion;
- Reciprocity (return flow of improvements) is desired.

For cloud and web services, AGPL licensing is preferred to maintain copyleft effect in network-based use.

### Licence compatibility and management

Every software solution must integrate only open source components with compatible licences. Documentation is systematic:

- Licence register per application listing all components used, or SBOM (Software Bill of Materials) documentation;
- Compatibility check before integrating new dependencies.

### Licence changes

Licence changes require OSPO review to ensure consistency, legal certainty and sustainability. Assessment particularly considers impact on existing users and community development.

## 3.6 Open source expertise

The NCSC uses the Federal Chancellery's open source tools as its foundation. The Em002 guidelines, checklists and templates provide the framework for planning, development, approval and publication. NCSC processes, artefacts and decisions are designed to align with these tools; any deviations require justification and documentation. Findings from pilot projects (including CSH) feed directly into tool development – particularly on centralisation issues such as shared repositories, reporting centres and standard modules.

The NCSC takes an active role in the nationwide open source Community of Practice (CoP), which facilitates knowledge exchange across administrative boundaries, shares best practices and addresses legal, security and operational challenges collectively. The NCSC contributes case studies, templates and practical experience, builds links with research and industry partners, and keeps the central office informed of publications and relevant developments.

## 3.7 Process and tools

The set of guidelines accompanying this strategy sets out the NCSC open source process (preliminary assessment → analysis/preparation → release/publication → operation). The Open Source Programme Office manages and continuously updates these guidelines. EMOTA tools (Em002, guidelines, checklists) are consolidated and referenced as binding standards. Every project follows open source gates with clearly defined artefacts and documented storage for code and documentation.

## 3.8 NCSC open source process

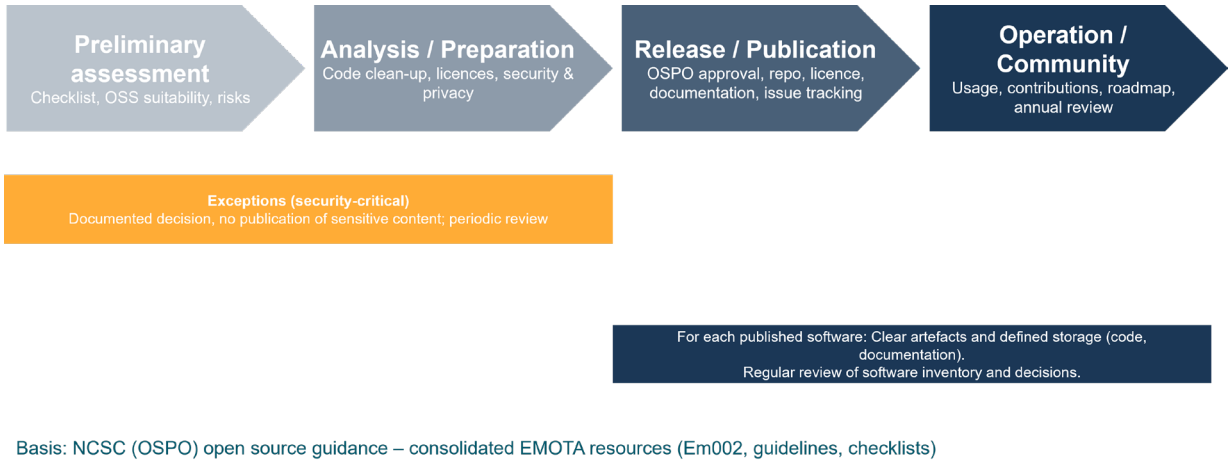


Figure 2: NCSC open source process

# 4 Procurement and contracts

The NCSC takes a licence- and model-neutral approach to procurement, prioritising digital sovereignty, life cycle costs and interoperability. Functional specifications are standard; only in exceptional cases is procurement tied to specific products or manufacturers.

Open source can be explicitly required where objectively justified:

- Digital sovereignty;
- Avoiding vendor lock-in;
- Expected modifications triggering EMOTA publication requirements;
- Interoperability and open standards.

Article 9 EMOTA must be considered when planning any proprietary or additional developments.

## 4.1 EMOTA application by procurement type ('make or buy')

| Procurement type | Open source obligation | Particularities |
|---|---|---|
| **Developing software in-house** | Yes (Art. 9 EMOTA) | Applies also to further developments |
| **Commissioning software development** | Yes (Art. 9 EMOTA) | Ensure approval rights in contracts |
| **Purchasing software externally** | Where adjustments made | Include approval rights in tender |
| **Software 'rent' (SaaS)** | No | No adjustments = no obligation |
| **Acquiring software from another federal agency** | For NCSC adjustments | Assumption: Original usually already published |
| **Purchasing development resources** | Yes (Art. 9 EMOTA) | Contract must cover ability to publish |
| **Co-production with public authorities** | Yes for new creations | Unpaid contributions permitted |

#### Strategic procurement – equal treatment with open source focus

All licence and business models are permitted in tenders. Open source can serve as an eligibility or evaluation criterion (covering digital sovereignty and expected modifications with publication requirements).

#### Digital sovereignty as a criterion

Procurement puts adaptability, creativity and influence first.

#### Integrate EMOTA early

Decide early on licence family (permissive vs. copyleft). Clarify market conditions, upstream options and community setup during planning before tendering. Use provisional EMOTA checklists (e.g. Em002 2.1–2.3) for compliance.

#### Life cycle management

Require SLAs covering security fix policy and update capability. Document SBOM obligations. Treat subscription/support models as evaluation criteria.

#### Open standards and portability

Demand open standards to minimise lock-in and ensure interoperability.

## 4.2 Contract drafting

### 4.2.1 Core elements for EMOTA compliance as mandatory criteria

- Ensure IP transfer to the federal government;
- Define licence selection and publication rights;
- Specify contribution rules and community standards;
- Guarantee long-term availability in provider-independent repositories.

### 4.2.2 Tools

- Criteria and framework agreement sections of the Competence Centre for Federal Public Procurement (CCPP);
- Open source procurement guidelines from the Federal Office for Buildings and Logistics (FBL);
- Em002 contract modules for publishability.

### 4.2.3 Free use ≠ procurement

Downloading and using open source software at no charge does not constitute procurement. Services can be procured later under standard regulations.

The open source guidelines provide further procurement details and links.

## 4.3 Dealing with legacy software

Orderly transfer: we publish what is legally and technically sound from a security perspective – everything else is excluded pending clarification.

### Procedure:

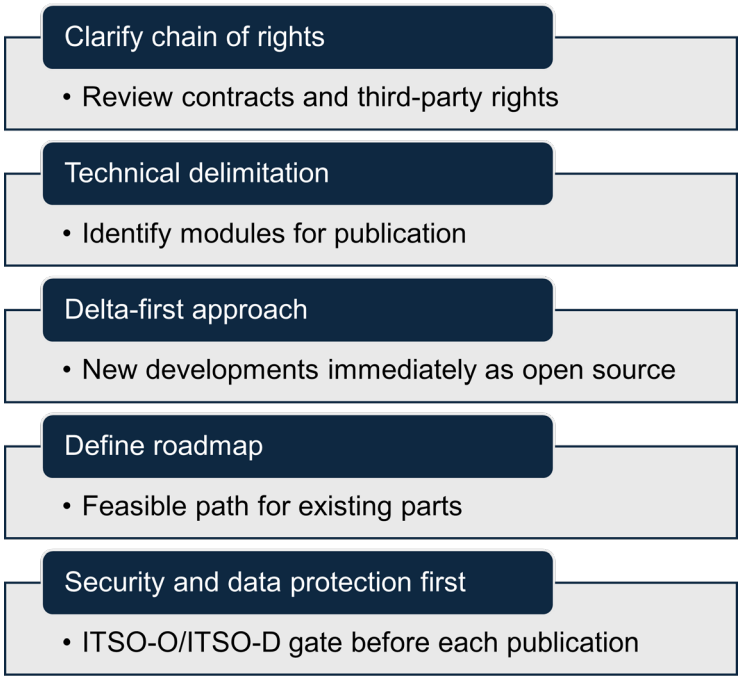


Figure 3: Approach to legacy software

### Governance for legacy cases:

- Open Source Programme Office decides;
- Exceptions time-limited and documented;
- Annual review of legacy cases.

# 5 Risks and standards at the NCSC

| Risk | NCSC standard | Possible mitigation measures |
|---|---|---|
| **R01 Legitimacy and compliance**<br>Tension between 'open source by default' and exceptions produces inconsistent decisions. | Exceptions limited, temporary, documented; annual review against clear criteria. | • Uniform exemption procedure;<br>• OSPO + Legal Service + ITSO-O/ITSO-D decide;<br>• Central exception register and KPIs;<br>• Project manager training. |
| **R02 Security**<br>Openness increases attack surface/probability. | Security before features; publication only after security review. | • ITSO-O/ITSO-D gate before each release;<br>• SAST/DAST/dependency scanning and SBOM;<br>• Vulnerability disclosure policy;<br>• Patch/backport process;<br>• Security champions per team. |
| **R03 Digital sovereignty and vendor independence**<br>Dependencies (cloud/CI/repos/build chains) strategic goals. | Open standards, portability, and exit planning as standard. | • Reproducible builds;<br>• Repo mirrors and backups;<br>• Data/artefact egress in SLAs;<br>• Licence/data escrow;<br>• Open tools and formats. |
| **R04 Ecosystem and reuse**<br>Forks/fragmentation or low adoption weaken impact. | API stability, clear roadmaps, active community management; compatibility before features. | • Regular release cadence;<br>•<br>• Contribution and governance models;<br>• Early partner involvement. |
| **R05 Reputation and trust**<br>Security incidents or false support expectations; use of unmaintained software. | Transparent communication; clear support scope and response channels; flag as 'unmaintained'. | • Incident response playbook;<br>• SECURITY.md and SUPPORT.md;<br>• Status badges (build, coverage, maintained);<br>• EOL policy;<br>• SLA classes and contact channels. |
| **R06 Rights and IP clarity**<br>Unclear rights chains or licence incompatibilities block publication. | Upfront legal and data protection analysis; contract compliance; licence whitelist; IP assignment; OSS specifications in procurement. | • Automated licence scans and third-party notices;<br>• Inbound/outbound licence guidelines;<br>• Provenance evidence in SBOM. |
| **R07 Execution capability and resources**<br>Open source by default clashes with project/operational load → delays. | Dedicated capacity for processing, documentation and community; clear prioritisation. | • MVP publication with gradual expansion;<br>• RACI matrix for roles;<br>• Release calendar and buffer;<br>• Separate 'publish hardening' backlog;<br>• Fixed budget and time blocks. |
| **R08 Financing and sustainability**<br>Ongoing costs (security, maintenance, documentation, community) underestimated; OpEx/SLAs insufficiently mapped. | Lifecycle financing (CapEx + OpEx); explicit maintenance/security/documentation/community requirements; TCO and benefit basis for prioritisation. | • Multi-year contracts and SLAs;<br>• Co-financing and partnerships;<br>• Contribution programmes;<br>• Minimal publication with expansion roadmap. |
| **R09 Data and privacy**<br>Leaks in code, tickets, logs or documentation. | Privacy by design; editorial rules; confidential artefact separation; data minimisation. | • Private issue queues for sensitive tickets;<br>• Anonymised demo data;<br>• Pre-publish privacy checklist. |
| **R10 Interoperability and quality**<br>Unclear standards and fluctuating code quality hinder reuse. | Architectural principles; Definition of Ready/Done; SemVer compliance; compatibility as default. | • Coding and API guidelines;<br>• CI quality gates (linting, tests, coverage thresholds);<br>• Contract/compatibility tests. |

# 6 Annex

## 6.1 Sources

| Title | Source / Author | Link | Last updated |
|---|---|---|---|
| **BBl 2023 787 – Federal Act on the Use of Electronic Means to Carry Out Official Tasks (EMOTA)** | Federal Council / Federal Chancellery | fedlex.admin.ch | 22.11.2023 (in force: 1.1.2024). (News.admin.ch) |
| ***EMBAG macht Open Source Software zur Norm: Chance und Verpflichtung für die Bundesverwaltung*** | APP Unternehmensberatung AG (Thomas Häfliger) | app.ch | 11.07.2024. (APP Unternehmensberatung AG) |
| **Explanatory notes on the Ordinance on the Use of Electronic Means to Carry Out Official Tasks (EMOTO)** | Federal Council / Federal Chancellery | PDF | 22.11.2023. (Newsd) |
| **Em002 Strategic Guidelines for Open Source Software in the Federal Administration** | Federal Chancellery, DTI Sector | PDF | 14.03.2025. (bk.admin.ch) |
| **Em002-1 Practical Guidelines for Open Source Software in the Federal Administration** | Federal Chancellery, DTI Sector | PDF | 14.03.2025. (bk.admin.ch) |
| **Em002-2 Instructions for Publishing Open Source Software** | Federal Chancellery, DTI Sector | PDF | 14.03.2025. (bk.admin.ch) |
| **Em002-2.1 Preliminary Assessment Checklist** | Federal Chancellery, DTI Sector | DOCX | 14.03.2025. (bk.admin.ch) |
| **Em002-2.2 Analysis and Preparation Checklist** | Federal Chancellery, DTI Sector | DOCX | 14.03.2025. (bk.admin.ch) |
| **Em002-2.3 Release and Publication Checklist** | Federal Chancellery, DTI Sector | DOCX | 14.03.2025. (bk.admin.ch) |
| **Em002-3 OSS Licensing Guidelines** | Federal Chancellery, DTI Sector | PDF | 11.03.2025. (bk.admin.ch) |
| **Em002-4 OSS Community Guidelines** | Federal Chancellery, DTI Sector | PDF | 11.03.2025. (bk.admin.ch) |
| **Em002-4.1 OSS Community Checklist** | Federal Chancellery, DTI Sector | DOCX | 14.03.2025. (bk.admin.ch) |
| **Em002-5 Factsheet: Publication of Open Source Software (OSS) by the Federal Administration** | Federal Chancellery, DTI Sector | PDF | 11.03.2025. (bk.admin.ch) |
| **Em002-6 OSS-FAQ** | Federal Chancellery, DTI Sector | PDF | 14.03.2025. (bk.admin.ch) |
| **Em002-7 Factsheet: Applying the OSS Article 9 EMOTA** | Federal Chancellery, DTI Sector | PDF | 14.05.2025. (bk.admin.ch) |
| ***IT-Beschaffungen 2.0: Die Handbremse lösen!* (conference proceedings)** | Koch / Biehl / Fischer (eds.), Dike | dike.ch | 2025. (DIKE Verlag) |
| **CCPP Factsheet: Software procurement under Article 9 EMOTA (de/fr/it)** | Federal Chancellery (DTI) and Competence Centre for Federal Public Procurement (FOBL/CCPP) | PDF | 13.08.2025. (bk.admin.ch) |
| **'Open by default' (Promoting digital sustainability), v60** | Federal Chancellery, DTI Sector | (local copy) | 26.08.2025 |

| | | | |
|---|---|---|---|
| **Study: *Technologische Perspektive der digitalen Souveränität*** | Professor Matthias Stürmer (BFH) | bfh.ch (PDF) | 12.06.2024. (Bern University of Applied Sciences) |
| **DDPS EA principles** | Confluence (internal – not public) | Confluence | 26.09.2025 |
| ***Umsetzung EMBAG Art. 9 im Bund (Foliensatz HV CH-Open)*** | Bruno Schöb, Federal Chancellery DTI | ch-open.ch (PDF) | 21.03.2024. (CH Open) |
| ***Wegleitung Open Source in der Beschaffung*** | Federal Office for Buildings and Logistics (FOBL) | (local copy) | 2025 |

Relevant paragraphs from the Cybersecurity Ordinance:

- Article 8 paragraph 3: "The NCSC is responsible for the security of communication and information systems and the lawful processing of data."
- Article 11 paragraph 2: "The NCSC decides on the publication of approved information."

## 6.2 Article 9 EMOTA

**New legal basis in Article 9 EMOTA → The federal government not only may, but MUST**

**Article 9 Open source software**

[1] Federal authorities subject to this Act **shall disclose the source code of software** they develop or commission for fulfilling their tasks, unless third-party rights or security reasons preclude or restrict this.

[2] **They allow anyone to use, develop and distribute the software, charging no licence fees.**

[3] **The rights in paragraph 2 are granted through private-law licences,** unless other enactments stipulate otherwise. Disputes between licensors and licensees are settled under civil law.

[4] **Where possible and appropriate, internationally established licence texts should be used. Liability claims by licensees should be excluded** to the extent legally possible.

[5] **Federal authorities subject to this Act may provide supplementary services, particularly for integration, maintenance, information security and support, insofar as these serve official tasks** and can be provided at reasonable cost.

[6] **They charge fees covering the costs of the supplementary services.** The competent department may grant exemptions for certain services where this does not compete with the private sector.