Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Chancellery FCh
Digital Transformation and ICT Steering DTI

14.09.2026

Em002-6 FAQ on OSS and Art. 9 EMOTA

Version 2.0-f544937

Table of Contents

1. Background and purpose 3
1.1. Background and purpose of the FAQs 3
1.2. Structure and organisation 3
2. Terms and definitions 3
2.1. Open source software 3
2.2. Software and licences 3
2.3. Legal basis in EMOTA 4
3. Roles and responsibilities 6
3.1. Role of the Federal Chancellery 6
3.2. Role of administrative units 6
3.3. Collaborations with third-party providers 6
3.4. Disclosure of personal data 7
3.5. Procurement 7
4. Process 7
4.1. Guidance 7
4.2. Licence selection 9
4.3. Quality criteria for OSS 9
4.4. Documentation 10
4.5. Contributions to projects by the Federal Administration 10
4.6. Support 10
5. Tools 11
5.1. Guidance 11
5.2. Checklists 11
5.3. Security matters 11
6. Legal matters 13
6.1. Use of English 13
6.2. Liability disclaimer 13
6.3. Permissive software 14
6.4. Licence provisions 14

6.5. Relationship between the FoIA and EMOTA 14

6.6. OSS and data protection 15

7. General 15

8. Annex 17

8.1. Abbreviations 17

8.2. Glossary 18

> **NOTE** This document is an evolving draft and part of the guidelines and tools designed to support the Federal Administration in publishing open source code. For more information, see the main README.

1. Background and purpose

1.1. Background and purpose of the FAQs

A number of questions frequently arise in connection with the tools available for publishing OSS. The following compilation answers the most common questions and aims to provide a better understanding of individual topics and aspects.

1.2. Structure and organisation

The FAQs are organised by subject, as follows:

2. Terms and definitions
3. Roles and responsibilities
4. Process
5. Tools
6. Legal matters
7. General

2. Terms and definitions

2.1. Open source software

What is meant by open source software?

This is defined in Em002-1 Practical Guidelines for Open Source Software in the Federal Administration

2.2. Software and licences

What is meant by software?

This is defined in Em002-1 Practical Guidelines for Open Source Software in the Federal Administration. For licences, see Em002-3 OSS Licensing Guidelines.

What is meant by licences?

Here we are referring to software licences. Further information can be found in Em002-3 OSS Licensing Guidelines.

Should custom-built AI models be considered as software and thus subject to the legal requirements of Art. 9 EMOTA? What about the training data?

Open source refers to software whose source code is freely accessible and modifiable under minimum conditions. This also includes custom-trained AI models (including the algorithm, training procedure, and code).

AI models are trained on the basis of data, possibly Open (Government) Data. Open Data refers to datasets that are free to use, share and process. AI models with underlying training data based on

Open (Government) Data are considered software subject to EMOTA and therefore must also be published.

However, if the training data contains (sensitive) personal data or classified information, publication can be waived on security-relevant grounds. When open-sourcing an AI model, the training data does not necessarily have to be published; however, this is in keeping with the open source ethos and is strongly encouraged by the open source community. For further information regarding AI, we refer to the Competence Network for Artificial Intelligence (CNAI).[1]

Must tools with generative AI capabilities (e.g. GitHub Copilot) be checked before use to ensure that no intellectual property belonging to third parties or the federal government is violated?

Content generated by an AI model itself cannot be protected by copyright because there is no creative activity behind it. However, AI-generated content that draws on copyrighted works of third parties may infringe the rights of these third parties. Also, given that AI outputs are notoriously unreliable, they should only be used after careful examination in each case.

Furthermore, the operators of AI systems may reserve the right in their terms and conditions to use inputs to train the system. This, in turn, can lead to inputs or parts thereof being displayed to third parties. Where this cannot be ruled out, it must be ensured that inputs do not violate the rights of the Confederation or third parties.

It is recommended to examine and approve the use of AI tools individually. Unapproved tools may not be used, but employees can apply for approval of a tool. Often it makes sense to resolve such issues by contract with the supplier, or some suppliers may offer special subscriptions by which they respect third-party rights, e.g. DeepL.

2.3. Legal basis in EMOTA

What is the legal basis for the publication of OSS?

According to Art. 9 EMOTA[2], federal authorities of the central Federal Administration must disclose the source code of software they develop or commission. Any person is allowed to use, further develop or modify the software without being charged fees of any kind.

Publication of source code can only be avoided in relation to third-party rights or for security-relevant reasons.

More information can be found in Em002-2 Instructions for Publishing Open Source Software.

What is meant by security-relevant reasons?

The security-relevant reasons permitted under Art. 9 EMOTA and how to deal with them are defined in Section 3.2 of Em002-2 Instructions for Publishing Open Source Software.

What are third-party rights?

Third-party rights under Art. 9 EMOTA and how to deal with them are defined in Section 3.3 of Em002-2 Instructions for Publishing Open Source Software.

Is it possible for exceptions to be time-limited?

The grounds for an exception under Art. 9 EMOTA (third-party rights and security-relevant reasons) may cease to apply over time.

If that happens, the source code of the software must be released.

1. CNAI and also Art. 10 EMOTA
2. SR 172.019

What legal consequences should be considered in case of a violation of Art. 9 EMOTA?

There are two types of violations:

1. Third-party rights are violated
2. A federal authority refuses to publish OSS (e.g. citing security-relevant reasons that are not valid)

Answer to 1:

This will regularly be a breach of contract and claims for damages may be asserted in accordance with the Swiss Code of Obligations.

Answer to 2:

This has no direct consequence. If a third party wants to be able to use the source code of a federal authority, they have to submit a request under the Freedom of Information Act (FoIA; SR 152.3) to the responsible authority.

If there is a high level of interest, it may make sense to consider publication in the interest of both parties. There is no obligation to publish retroactively, although this can be done voluntarily.

Can liability claims be asserted in the case of damage caused by OSS?

In principle, liability claims should be excluded in the contracts. However, it is not possible to exclude liability for gross negligence or culpable negligence. In such cases, a federal authority could be held liable under the Government Liability Act (GLA; SR 170.32).

From which date must software be published?

According to Art. 9 para. 1 EMOTA, software that is or has been developed after 1 January 2024 must be published.

For software developed before 1 January 2024, release should be considered when major changes are pending.

If there is considerable interest from third parties, existing software may also be released voluntarily (possibly with cost sharing). In this case, a community (see Em002-4) should also be considered.

For smaller scripts, publication is usually not the best option. There may be repositories for tools that then go through the release process at the same time.

For administrative units of the decentralised Federal Administration that are subject to EMOTA, the publication requirement has applied since 1 May 2025. Exceptions to the publication requirement exist for software developed without federal funding and research software (Art. 3 para. 1 DigiO).

Is it possible to demand retroactive publication for software developed before 1 January 2024?

The law does not provide for retroactive publication.

Furthermore, contracts concluded before 1 January 2024 may contain third-party rights that preclude publication.

If a new major version is pending (major according to Semantic Versioning[3]), a release of the entire software should be considered. Otherwise, the source code of the new functionalities would at least have to be released.

3. Version control — Wikipedia

On what basis would a third party have to request the release of source code?

A third party would have to submit a request under the FoIA to the competent authority.

3. Roles and responsibilities

3.1. Role of the Federal Chancellery

Who makes the basic implementation tools available?

The DTI Sector of the Federal Chancellery provides tools for the federal authorities as a document set accompanying Em002. This includes the strategic guidelines and other practical guidelines including FAQs, as well as checklists to ensure legally compliant implementation.

The OSS tools are updated by DTI.

Is the Federal Chancellery responsible for granting exemptions (e.g. for security-relevant reasons)?

There is no central body that rules on exemptions to the publication obligation under Art. 9 EMOTA. Each federal authority is responsible for its own legally compliant implementation.

The federal departments may establish regulations.

The Checklist for Art. 9 EMOTA Blanket Exception [BBL-CL] from the FOBL should be completed.

3.2. Role of administrative units

Who is responsible for operational implementation of OSS releases?

Each federal authority (e.g. office, administrative unit) that develops or commissions software is independently responsible for the entire publication process.

The federal departments may establish binding regulations and control mechanisms within their area of responsibility, e.g. to prevent reputational damage.

It is recommended to appoint a person responsible for OSS per federal office, e.g. IT Manager (IM), Enterprise Architect, ISBO or DSBO, to ensure uniform and efficient processes. If this is not specified, the federal office management is generally responsible for compliant implementation.

This officer could then also be consulted for granting exemptions to the publication obligation.

3.3. Collaborations with third-party providers

How should a federal authority's in-house developments be published?

Copyright arises with the respective natural persons who developed the source code, although this is usually transferred to the employer by way of the employment contract. In contracts with external service providers, it is important to clearly delineate new developments and to agree on the contractual assignment/transfer of copyright. Ultimately, for joint in-house developments, the parties involved must agree on the open source licence for the source code under which the software is published as an independent open source project. Publication under an open source licence does not mean waiving copyright: this remains with the respective rights holders. Only on the basis of their copyright can they legally defend against licence violations or grant more extensive licences in parallel to OSS licences.

3.4. Disclosure of personal data

Under what conditions may personal data, such as that of developers, be published as part of OSS?

There is no general rule for this. The decision lies with the project.

In any case, the applicable data protection regulations must be complied with. According to Article 36 para. 1 FADP, federal bodies may only disclose personal data if they have a legal basis for doing so.

Article 36 para. 2 FADP specifies the following exceptions, among others:

(b) The data subject has consented to the disclosure.

(e) The data subject has made their data generally accessible and has not explicitly prohibited processing.

In most cases, it is advisable to obtain the consent of the persons concerned in advance, as they usually also have an interest in their work being publicly visible. If consent is not given, or if there are other reasons against publication, the source code should be published without personal data, referring only to the federal authority concerned.

This consent should be obtained from suppliers and employees as part of the procurement and hiring processes.

3.5. Procurement

Where can I find the documentation for OSS procurement?

With Version 2.0, a tool Em002-7 Strategic Aspects of Procurement and Open Source Software was made available.

The Competence Centre for Federal Public Procurement (CCPP) has published a new information sheet entitled Software Procurement and Art. 9 EMOTA [KBB-MB] as well as two documents 'Sample criteria – EMOTA procurement and open source.docx' and 'Sample contract texts – software development.docx'.

Further resources can be found on the public procurement learning and template platform (www.perimap.admin.ch).

Further assistance is available on the FOBL intranet (accessible only on the federal network) with the Open Source in Procurement Guidelines [BBL-WL] and the Checklist for Art. 9 EMOTA Blanket Exception [BBL-CL].

The relevant information can be found on the FOBL intranet pages (only available within the Confederation).

Links: FOBL IT procurement toolbox

4. Process

4.1. Guidance

Is there central guidance on how OSS is handled in the Federal Administration?

Yes, the DTI Sector of the Federal Chancellery provides comprehensive materials for this purpose.

Note that these tools are an ICT recommendation and not a binding requirement.

Link to OSS tools

How should a federal authority's in-house developments that were created in collaborations be published? How should existing rights be handled?

When developing software, copyright arises with the respective natural persons who developed the source code.

If the developer is in an employment relationship, the developments belong to the employer (Art. 332 CO).

For contracts with external service providers, it is therefore important to clearly delineate new developments and to agree on the contractual assignment/transfer of copyright. Ultimately, for joint in-house developments, the parties involved must agree on the open source licence for the source code under which the software is published as an independent open source project.

Publication under an open source licence does not mean waiving copyright: this remains with the respective rights holders.

Only on the basis of their copyright can they legally defend against licence violations or grant more extensive licences in parallel to OSS licences.

The original rights should therefore always lie with the federal government for new or further developments, if possible. Contributor Licence Agreements (CLA) or Developer Certificate of Origin (DCO) should be used for other participants. Instructions for this can be found in Em002-3 OSS Licensing Guidelines, Em002-2 Instructions for Publishing Open Source Software and Em002-4 OSS Community Guidelines.

Do changes have to be published?

According to Art. 9 EMOTA: yes, if they were developed after 1 January 2024.

However, this should be done in a way that also provides benefit. The document Em002-2 Instructions for Publishing Open Source Software provides information on the process.

When is the publication 'sufficient' according to EMOTA?

Art. 9 EMOTA is not specific in this regard and there is a great deal of room for manoeuvre. The source code must be publicly accessible.

For example, the requirements of the law are satisfied by simply publishing the source code in a zip file on a website.

In order to achieve a benefit, including through the publication of documentation etc., this should be done on a code repository according to best practices. Information on this can be found in Em002-2 Instructions for Publishing Open Source Software.

In the future, will service procurers be telling service providers how the software should be published and how to ensure quality?

The rules of the individual federal authority apply to both service providers and service procurers.

However, it makes sense to include the corresponding tools at suitable points in the existing processes and quality gates.

Based on its development experience, the service provider can make suggestions for its service procurer here and treat this uniformly (just as the development process is treated uniformly).

4.2. Licence selection

Under which open source licence should software be developed?

There are no strict requirements regarding the choice of licence as long as the licence terms of the software components used in the software to be developed are adhered to.

For completely new developments, a licence type should be chosen that enables a broad and sustainable basis for further developments.

For this, it is important that the licence in question should be widely accepted in the relevant developer community.

The use of AGPL (with copyleft) and MIT is therefore recommended.

These two licences represent the two extremes of the licence spectrum, so to speak.

AGPL with a very strong copyleft permanently enforces the principle of 'public money – public code'. In the case of further developments, namely proprietary solutions, this will weaken towards LGPL.

MIT, on the other hand, is a very liberal licence where almost anything is possible.

The two licences cover the entire spectrum. If particular importance is attached to not naming the federal government in the case of permissive licences, BSD-3 is to be preferred over MIT.

For a more detailed selection of licences, please refer to Em002-3 OSS Licensing Guidelines.

4.3. Quality criteria for OSS

Does open source software have to meet certain quality criteria?

As a rule, all quality criteria for any other software also applies. Open source primarily makes everything more transparent. To comply with the licence, the criteria for a 'good' release, and any community rules in place, some additional points are necessary. These are outlined in Em002-2.2 OSS Analysis and Preparation Checklist and Em002-4.1 OSS Community Checklist.

What are the requirements planned for quality gates?

No central requirements are planned. The rules of the federal authority (administrative units) developing the software are applicable.

Apart from the general requirements, there are no special requirements for OSS quality. However, Hermes will be updated to incorporate Art. 9 EMOTA.

Publication is the Federal Administration’s way of going public. If this is not done carefully and professionally, the public image of a federal authority can quickly suffer.

How are development guidelines regulated?

Apart from the general requirements set out in the tools, there are no special requirements regarding the development of open source software. Guidance is provided in Em002-2.2 OSS Analysis and Preparation Checklist and Em002-4 OSS Community Guidelines.

Does OSS have to be published in a specific location?

The Confederation does not currently operate its own central repository. The federal authorities are therefore basically free in their publication. As many federal authorities already use GitHub, this platform is currently the preferred choice. There is also a central GitHub account (swiss) that can be used.

GitHub - swiss/index: An overview of current repository organisations.

This is especially the case if a federal authority does not yet have a GitHub account ('organisation') or does not use another platform such as GitLab or BitBucket.

Please contact the responsible unit in the DTI (opensource@bk.admin.ch) to check whether publication via the central GitHub account (swiss) is appropriate and possible.

Federal authorities should in all cases maintain a local copy of the code. It is also advisable for each federal authority to have a corresponding strategy and corresponding internal rules in place.

Further recommendations are given in Em002-2 Instructions for Publishing Open Source Software.

4.4. Documentation

What are the documentation requirements for OSS publication?

The tools made available by the Federal Chancellery's DTI Sector provide information on the legal requirements; see OSS tools.

It is recommended that the OSS checklists be completed and stored centrally in each federal authority (administrative unit).

4.5. Contributions to projects by the Federal Administration

Can and should an administrative unit contribute code to an 'upstream' project and does it thereby meet the requirements of Art. 9 EMOTA?

- If the projects are open source, then Art. 9 EMOTA is fulfilled. However, the projects must also remain open source. If they fail to do so, the code must be published again.
- Upstream contributions have the advantage that maintenance takes place within the upstream project and the benefit for the community is maximised.

  The following disadvantages exist: less control and influence, a CLA may have to be signed or a DCO (see Em002-4 Section 3.3). The contributions also do not appear in the publiccode.yml and the federal directories. A completely different advantage is that with such contributions, the developers continue to develop within the ecosystem.
- As long as the risks and effort remain manageable (CLA content, collection of the code), upstream contributions are to be welcomed.
- The licence of the upstream project then applies to the contribution. This corresponds to the procedure in Em002-3.
- **Forking of upstream projects should be avoided:** The entire maintenance and update burden then falls to the federal authority. Inadequate maintenance of the fork also represents a security risk. There is hardly any benefit for the community.
- Contributions to upstream projects should generally be viewed positively and actively discussed by the federal authorities' project managers.
- If the upstream project belongs to the Federal Administration and involves third-party contributions, Em002-7 Section 9 will help.

4.6. Support

Is the federal authority required to provide support for published software?

No, but it can if it so wishes.

According to Art. 9 paras 5 and 6 EMOTA, it may also charge fees for support.

How should an authority proceed if it wishes to charge for support?

For resource reasons, this is not part of the current project to provide tools. If required, this could be included in the tools in a subsequent stage. For the time being, each federal authority regulates this itself. (See also Em002-4 OSS Community Guidelines)

5. Tools

5.1. Guidance

Is there any central guidance on working with open source software in the Federal Administration?

Yes, the DTI Sector of the Federal Chancellery provides comprehensive materials for this as part of Em002 Strategic Guidelines for Open Source Software in the Federal Administration.

OSS is discussed in general terms in Em002-1 Practical Guidelines for Open Source Software in the Federal Administration. Release under Art. 9 EMOTA is addressed in Em002-2 Instructions for Publishing Open Source Software.

5.2. Checklists

Do the tools also include checklists for releasing open source software?

Yes, the DTI Sector of the Federal Chancellery provides the following checklists for free use:

- Em002-2.1 OSS Preliminary Assessment Checklist
- Em002-2.2 OSS Analysis and Preparation Checklist
- Em002-2.3 OSS Release and Publication Checklist
- Em002-4.1 OSS Community Checklist

See the **Checklist for Art. 9 EMOTA Blanket Exception** [BBL-CL] from the FOBL.

5.3. Security matters

Are there special OSS security risks?

In this context, supply chain attacks, zero-day vulnerabilities and typosquatting attacks are mentioned, for example.

Such security issues must be taken into account in OSS and in its procurement, but also generally in the development of software and in the procurement of commercial software. At best, they can be somewhat amplified if the OSS project used was careless when integrating libraries and containers.

In the medium term, a general strategy is needed to mitigate these risks (through the NCSC/SEPOS). If necessary, secure sources for containers and libraries must be made available.

In general, all those responsible in the IT environment must be aware of these possible attack vectors. Possible attempts include:

- Supply chain attacks: `XZ_Utils_backdoor` (https://en.wikipedia.org/wiki/XZ_Utils_backdoor), Codecov (https://blog.gitguardian.com/codecov-supply-chain-breach/)
- Zero-day vulnerabilities: Log4Shell (https://www.ibm.com/de-de/think/topics/log4j)

- Typosquatting: https://en.wikipedia.org/wiki/Typosquatting

Does publishing source code increase the risk of a malicious copy of an app? (e.g. a phishing or fake app)

No. Withholding source code offers no effective protection against fake apps and is moreover incompatible with Article 9 EMOTA, which establishes the open source principle for the Federal Administration.

The risk of a third party building a visually identical app to harvest data exists regardless of whether the source code is published. Since the Confederation's design systems are publicly available, the look and feel of an app can be replicated by an attacker without access to the source code. Apps can also be decompiled to extract assets such as logos from the published version.

Security and trust are therefore ensured not through obscurity, but through verification and cryptographic security:

- **Digital signatures:** Official apps must be cryptographically signed, providing technical assurance that an app is an unmodified original from the Confederation. The smartphone operating system verifies this signature.
- **App store verification:** The Apple and Google app stores offer processes to verify publishers as official government bodies. Google, for example, explicitly labels Federal Chancellery (FCh) apps as government apps, giving users confidence in their authenticity.
- **Reproducible builds:** Through independent, reproducible builds, it can be technically demonstrated that the published source code corresponds exactly to the app available in the store.

A blanket exemption for security-related reasons under Article 9 of EMOTA is therefore not applicable to apps.

Recommendation:
Rather than withholding source code, the focus should be on app store processes and monitoring. Official channels must be kept up to date and fake apps reported promptly for removal by the platform operators (Apple and Google).

Does it make sense for requisitioners within the Federal Administration to join forces to procure OSS?

Yes, definitely. This can be done directly and informally between administrative units.

The problem is rather that the administrative units do not know much about each other's needs.

One solution could be for administrative units to keep a 'most wanted' list of OSS tools (or libraries) to be developed or made available and to share this list.

Such a centrally managed list could also help to better analyse the need for OSS components and better assess the maturity level of the administrative unit. Ultimately, an artifact repository would make sense.

Maintaining such a list would then be the task of an OSPO, should one be introduced. At best, this could also be done via Digital Public Services Switzerland for the entire federal structure.

6. Legal matters

6.1. Use of English

Is the Confederation allowed to use licences in the original language English?

According to Art. 9 para. 4 EMOTA, internationally established licence texts should be used wherever possible and practical.

Insisting on German-language OSS licences would largely negate the purpose of Art. 9 para. 4 EMOTA as there are very few internationally established licence texts where a version in one of Switzerland's official languages (German, French and Italian as specified in Art. 70 para. 1 Cst.) is recognised as authoritative for interpretation.

This situation parallels English-language courses at higher education institutions such as ETH, where English as the teaching language is permitted – subject to the three conditions under Article 36 of the Federal Constitution (St Gallen Commentary on the Federal Constitution, 4th ed. 2023, Art. 70 N 29; namely a legal basis, public interest, and proportionality must exist for English to be permitted).

Based on the above, Art. 9 para. 4 EMOTA should be interpreted as providing the legal basis for using English-language licences, since international licences are predominantly in English. The provision must therefore refer to these.

The public interest in Art. 9 EMOTA lies, among other things, in the exchange with the respective developer communities.[4] In the computing industry, these communities are typically international and use English as their working language. Restricting licences to German-language ones would at the very least make cooperation with international communities difficult, if not impossible, because software licensed in this way would hardly be used internationally. This would also conflict with the intended purpose of Article 9 EMOTA.

Moreover, internationally established OSS licences are, by definition, valid worldwide. The legislator evidently intended to enable international use of the released software. Restricting OSS releases to German-language licences would severely limit the international usability of the released software.

Additionally, English is firmly established as the standard language in the computing industry's commercial sphere, which includes OSS releases. Using English-language licences therefore represents a reasonable and proportionate limitation on the contractual partners' rights. Moreover, English-language licences are both appropriate and necessary to achieve the intended objectives.

6.2. Liability disclaimer

Most OSS licences include liability disclaimers. Is this adequate, or are additional measures needed? What is the position regarding defective software? (including consideration of the Government Liability Act)

The applicable licences exclude liability for slight negligence. **Liability cannot be excluded for gross negligence or intentional acts**. However, the practical liability risks are minimal.

Distributing modified software under a licence incompatible with the original software's licence (for instance, using an MIT licence without copyleft where the code originally used was under a GPL licence with copyleft) breaches the original licence. Due to the absence of good faith protection in intellectual property law, this neither allows other users to suddenly use the original software under the new licence, nor creates an enforceable obligation to offer the new licence under the original

4. BBl 2022 804, p. 66

software's licence terms. The sole consequence is breach of the original licence, potentially resulting in damages claims (licence analogy) against a federal authority.

However, this risk can be managed through systematic checking according to the guidelines, as is now standard practice in the software industry. Specifically, licensing requires creating a bill of materials listing all pre-existing software incorporated into the new software, which must be strictly adhered to during licensing.

Where third-party rights exist, Art. 9 para. 1 EMOTA anyway does not require publication of the software in any case (or potentially only its newly written portions; this should be clarified in the guidelines).

Under Article 11 of the Government Liability Act, the Confederation's liability is governed by civil law when it acts as a civil law entity. This is the case under Art. 9 para. 2 EMOTA; consequently, additional liability under the Government Liability Act is excluded.

6.3. Permissive software

If software is based on a library/program component published under a permissive licence, can the main software (excluding the library) be published under a non-permissive licence?

Yes, this is unproblematic. See the information provided in the guidelines Em002-3.

6.4. Licence provisions

Can software be used by several different offices? What licence provisions apply within the Federal Administration? Is the Federal Administration considered a corporate group? (This applies to unmodified open source software from third parties.)

Distributing software under permissive licences is generally straightforward.

However, with copyleft licences, the question arises whether distribution within the central or decentralised Federal Administration triggers copyleft obligations and thus risks compromising the confidentiality of the Confederation's own developments. When distributing to institutions of the decentralised Federal Administration that have their own legal personality, this is indeed the case, whereas it does not apply within the central Federal Administration, as all departments operate under the same legal entity.

Corporate group companies are legally independent but remain under the economic control of the parent company. Legal literature considers the distribution of copyleft-licensed code to a group company as triggering copyleft obligations. Since group companies often receive open-source software during software development, they require their own right of use, meaning that distribution to a group company triggers copyleft obligations.

In contrast, distribution within the central Federal Administration does not trigger copyleft obligations. However, for the decentralised Federal Administration, where separate legal entities exist, the above applies: distribution triggers copyleft obligations, and the software must be offered in source code form under the same licence terms as the original software. An instruction not to distribute the software to third parties would violate the licence and could also breach Art. 9 EMOTA.

6.5. Relationship between the FoIA and EMOTA

How do the Freedom of Information Act (FoIA) and EMOTA relate to each other?

According to Art. 6 FoIA, official documents must be issued. An official document under Art. 5 para. 1 FoIA is defined as any information recorded on any medium that is in the possession of an authority and relates to the performance of a public task. OSS fundamentally falls under the FoIA. The FoIA applies when an individual requests source code from a department or office for their own

use. The office must disclose the source code to the person concerned unless exceptions under Article 7 FoIA apply. If the office refuses to disclose the source code, the FoIA procedure applies. A different case arises when someone demands that the office publish the source code on its website. Then the procedure would not follow the FoIA but EMOTA. Since EMOTA itself does not specify a procedure, general administrative law must suffice. This provides either the option of an administrative decision, a real act, or a general declaratory decision from the office concerned. This decision can then be appealed to the Federal Administrative Court.

While disclosure obligations for software developed by a federal authority under the FoIA are conceivable (if the relevant conditions are met), it should be noted that disclosure of software under the FoIA does not automatically grant an OSS licence. The use of software disclosed under the FoIA is thus limited to the purposes set by the FoIA, such as viewing the code or executing it for observation purposes. However, FoIA disclosure does not include a licence for regular use of the software or as a basis for further software development (details in T. Poledna/S. Schlauri/S. Schweizer, Rechtliche Voraussetzungen der Nutzung von Open-Source-Software in der öffentlichen Verwaltung, insbesondere des Kantons Bern [tr: Legal Requirements for the Use of Open Source Software in Public Administration, particularly in the Canton of Bern], Zurich 2017, https://carlgrossmann.com/?ddownload=11748, N 393 ff.).

The decision to license software as OSS, even if it falls under the FoIA, continues to follow EMOTA; there remains no entitlement to the granting of a licence.

Importantly, software developed before 1 January 2024, while not subject to EMOTA, must still be released according to the FoIA.

6.6. OSS and data protection

Can developers' personal data be published without further consideration? What data protection aspects need to be considered?

From a data protection perspective, publishing personal data (e.g. names or email addresses) is problematic unless employees have given prior consent. This is because the disclosure of personal data can, in principle, be avoided through pseudonymisation or anonymisation of repository entries, which would be required according to the principle of data minimisation and proportionality (Art. 6 para. 2 FADP).

However, such consent should generally be easy to obtain, as employees often have an interest in publicly demonstrating their capabilities (as noted in Poledna/Schlauri/Schweizer, N 68, with references). Consent may also be implied through the use of names in the repository, at least where no employer directive exists to the contrary.

Nevertheless, it is advisable to address the provider’s responsibility for their employees' personal data in the contracts.

7. General

Does it matter whether OSS is used commercially or non-commercially?

Open source licences generally do not distinguish between commercial and non-commercial use. Therefore, OSS can be used for any purpose, including commercial applications. Commercial suppliers often try to integrate OSS components into proprietary products. This is only permissible if the OSS components are not under a licence with copyleft effects (see also Em002-3 OSS Licensing Guidelines).

Are there restrictions on which organisations are permitted for communities?

Ultimately, each case must always be considered individually: who is behind it, and what commitments are being made?

As long as no money changes hands and no formal commitments are made, the situation is relatively straightforward and unproblematic.

Association memberships are possible, as is informal collaboration.

It is possible to delegate memberships to eOperations or similar organisations.

See also Em002-4 OSS Community Guidelines, Section 3.1

How does ISO Standard 5230 relate to the guidelines?

ISO Standard 5230:2020 was reviewed and taken into account during the drafting of the guidelines. The list below sets out the requirements of the standard and how these have been addressed in the guidelines:

3.1 Programme foundation

- The 'Em002 Strategic Guidelines for Open Source Software in the Federal Administration' and the referenced strategies provide the framework. The respective federal departments and offices are responsible for implementation.

3.2 Relevant tasks defined and supported

- The guide 'Em002-2 Instructions for Publishing OSS' and the checklists define specific tasks for publication. There is currently no central body within the Federal Administration.

3.3 Open source content review and approval

- The publication process is described in the resource 'Em002-2 Instructions for Publishing OSS'. This also refers to the existence of a Software Bill of Materials (SBOM).
- The resource 'Em002-3 OSS Licensing Guidelines' provides comprehensive information on licensing.

3.4 Compliance artifact creation and delivery

- The publication process is described in the resource 'Em002-2 Instructions for Publishing OSS'. This also refers to the existence of a Software Bill of Materials (SBOM).
- Implementation is not described in further detail and takes place within the federal departments or offices.

3.5 Understanding open source community engagements

- The resource 'Em002-4 OSS Community Guidelines' describes how to set up and maintain a community. A concept must be defined and implemented for each project.

3.6 Adherence to the specification requirements

- The final chapter sets out requirements for organisations or projects wishing to explicitly confirm compliance with the OpenChain requirements.

The ISO standard outlines further areas of responsibility for an Open Source Programme Office (OSPO) which are not covered by the guidance documents.

8. Annex

8.1. Abbreviations

AI
Artificial intelligence

AO
Application owner

CCPP
Competence Centre for Federal Public Procurement

CLA
Contributor Licence Agreement

DCO
Developer Certificate of Origin

DPSS
Digital Public Services Switzerland (www.digital-public-services-switzerland.ch/strategy)

EMOTA
Federal Act on the Use of Electronic Means to Carry Out Official Tasks

FITSU
Federal IT Steering Unit (until 2021)

FOBL
Federal Office for Buildings and Logistics

FoIA
Freedom of Information Act

FSF
Free Software Foundation

HERMES
Handbuch der Elektronischen Rechenzentren des Bundes, a method for system development (www.hermes.admin.ch)

OSI
Open Source Initiative

OSPO
Open Source Programme Office

OSS
Open source software

OSSD
Open source software development

OU
Organisational unit (usually a federal office)

SPc
Service procurer

SPDX
Software Package Data Exchange

SPv
Service provider

8.2. Glossary

Further terms can be found in TERMDAT, the Federal Administration's terminology database.

Application area
This refers to the categories of office automation (OA) software as defined in [A029] and other classifications.

Branch
A development branch of an OSS.

Collaboration
The term 'collaboration' derives from the Latin word 'collaborare', which means 'to work together'. It describes a way of working in which several people or teams work together towards a common goal, contributing their skills and resources. The focus is on mutual exchange, transparency and the sharing of knowledge.
According to the Gabler Business Dictionary, collaboration also refers to 'cooperation between a company and its customers and suppliers, using modern information technologies to integrate internal and cross-company business processes.'

Contribution
OSS contribution refers to the contribution to the development and improvement of open source software (OSS). This can take the form of providing code, documentation, tests, feedback or other types of contributions. (Google AI)

Contributor Licence Agreement (CLA)
A Contributor Licence Agreement (CLA), also known as a Contributor Agreement, is a document that sets out the terms under which intellectual property may be contributed to a project or initiative. This usually refers to a software project under an open-source licence (Wikipedia).

Core developer
Developer of an OSS project who has committer access rights to the repository.

Market analysis
A specific market analysis is used to identify and process information on the current and potential procurement market. The purpose of the market analysis is to identify and understand market structures and, in particular, the supplier structure with regard to all relevant characteristics: price situation (high, low, fluctuations); market size; geographical distribution of potential suppliers and key players, etc. (see https://perimap.admin.ch/goto_perimap_file_38221_download.html).
Possible sources of OSS software can be found in Em002-1 Practical Guidelines for OSS in Section 7.

OSS
Open source software

Product
Used here as a synonym for 'application'.

The term originates from ITIL. In ITIL (Information Technology Infrastructure Library), a product is a configuration of resources designed to deliver value to a customer or organisation. Unlike a service, which is typically an ongoing, interactive process, a product is a static entity.

Products can be software, hardware, data or other resources provided by the organisation. (Google AI)

Product standardisation

In this document, standardisation primarily refers to SD120, the ICT standard service for office automation, and other standardisations by DTI.

Subscription

When subscribing to software, a subscription is taken out. This means that the software is not purchased.
In most cases, this involves not only permission to use the software, but also includes all relevant services and support.

Upstream project

Upstream is a term used in distributed software development (often open source) and refers to the direction of a patch to its origin (upstream), i.e. to the original developers or maintainers of the software, or to the original project. These can also be software libraries.