Switzerland

Source Code Transparency through Public Procurement: The New Swiss Open Source Software Obligation

*Désirée Klingler and Rika Koch**

The digital transformation of the public sector is an ongoing phenomenon across countries worldwide, leading to an increased demand for digital technologies by public administrations. Typically, these administrations do not develop the software themselves but rely on private companies.[1] The public procurement of 'public administration software'[2] faces several challenges, such as the failure to protect personal data or ensure cybersecurity.[3] Equally critical, though often overlooked, are challenges related to service quality, information asymmetry, vendor lock-in, transparency and accountability.

To tackle these challenges, a few jurisdictions have started to adopt legislation to regulate the disclosure of the source code of public administration software.[4] Switzerland is one of these countries:[5] The new law on public sector digitalisation, the Federal Act on the Use of Electronic Means to Carry Out Official Tasks (EMOTA),[6] contains an obligation for Open Source Software (OSS), which is discussed in this report.

I. What is OSS and Why Bother?

1. Open Source Software and Its Properties

In contrast to proprietary (or closed source) software, open source software, also referred to as 'free software' is defined by four criteria: it is software that a user can (1) use for any purpose, (2) study, by examining the source code, (3) modify and improve and (4) distribute, with or without modifications.[7]

Generally, a developer holds the intellectual property (IP) rights to their work (i.e., their software, including its source code) and thus may decide who can use it and under which conditions. In the case of proprietary software, the right to use the software is

DOI: 10.21552/epppl/2025/2/14

* Désirée Klingler, Attorney at Law, LL.M. (Yale), Assistant Professor of Public Law at University of St. Gallen. Rika Koch, Professor of Public Procurement Law at Bern University of Applied Science.

1 See Albert Sanchez-Graells, *Digital Technologies and Public Procurement. Gatekeeping and experimentation in digital public governance* (Oxford University Press 2024) 34, Hongfei Gu, 'Data, Big Tech, and the New Concept of Sovereignty' (Journal of Political Science, 2023) 592, Sayed Jahed Hussini and Wolfgang F. Finke (eds), 'Creating Awareness for the Use of Open Source Systems in the Public Sector in Afghanistan' (Wirtschaftswissenschaftliche Schriften, No. 02/2013) 4.

2 Examples range from software used by the police to report theft or fraud, software used by local authorities to allocate children to schools or software used by administrative authorities to run a chatbot. Other examples are applications for everyday life, such as weather apps by meteorological authorities or applications used in circumstances of crisis, such as COVID apps.

3 Switzerland faced a series of cyberattacks in recent years, which highlighted the vulnerability of government IT infrastructure. The most notable was the May 2023 attack on Xplain, a private IT contractor, which resulted in the release of 400 gigabytes of data on the darknet, a significant portion of which belonged to federal and cantonal authorities, including the Federal Office of Police. For details, see National Cyber Security Center (NCSC), Data analysis report of the hacker attack on Xplain, report from March 7, 2024.

4 See for Brazil, Guskow Cardoso, 'Digital Government, Public Procurement, and Contracting in Brazil: A Technological Perspective on Procurement' (2025). See for France, Nina Lasbleiz & Liliane Obrecht, 'Le droit d'accès aux codes sources des systèmes algorithmiques utilisés par l'administration publique' (2025) *Sui Generis* 38. In Italy, courts have issued rulings on the disclosure of source code used in public administrations' software, see Fabio Bravo, 'Access to Source Code of Proprietary Software Used by Public Administrations for Automated Decision-making. What Proportional Balancing of Interests?' (2020) *European Review of Digital Administration & Law* 159.

5 As pointed out by Sanchez-Graells, these OSS initiatives are just emerging and far from being mainstream policy, see Sanchez-Graells (n 2) 205.

6 Unofficial English translation provided by the Federal Chancellery <https://www.bk.admin.ch/bk/en/home/digitale-transformation-ikt-lenkung/bundesarchitektur/open_source_software/hilfsmittel_oss.html> accessed 11 June 2025.

7 Referred to as 'the four freedoms of software,' see amongst others European Commission, Guideline on public procurement of Open Source Software (2010) 9 and 10.

usually granted in the form of a license, which must be purchased by users. Since licenses generate profit, private companies often have a commercial interest in creating proprietary software.

By offering OSS, developers waive the use of their IP rights and make the source code publicly available for contributors[8] to modify, improve, or redistribute the software. This community-driven approach encourages innovation and continuous improvement, as a broad range of developers can support each other to solve issues (such as 'bug fixing') and enhance the functionality of the software at issue.

2. The Benefits of 'Public Money, Public Code'

While the free publication of OSS has long been perceived as a potential market distortion,[9] it is now acknowledged that the benefits of OSS outweigh these concerns. There is now a prevailing view that OSS should be the default option for software used by public administrations, in line with the principle of 'public money, public code.'[10]

The first benefit is that OSS improves efficiency, leading to cost reduction. The free publication of source code and the community-driven collaborative approach enhance software quality through synergy effects, adding value from an economic perspective. This is particularly important in the context of public-public cooperation. In this context, OSS's openness allows proven software solutions developed by one public authority to be adopted, used, and adapted by another authority ('develop once, use many times').[11]

Another benefit is that OSS helps to overcome vendor lock-ins,[12] where public authorities (or other users) become dependent on one vendor, due to system- and knowledge-based constraints. Switching the vendor comes with high transaction costs, such as acquiring expertise to operate a new IT solution.[13] Legal dependencies, like End User License Agreements, exacerbate this problem by locking authorities into specific software, institutionalising path dependencies. This vendor-lock in can also be observed in Swiss public procurement practice, where a multitude of public tenders invoke the exception of Article 21(2)(e) of the Federal Act on Public Procurement (FAPP)[14] that allows a contracting authority to award a contract directly to a previous supplier 'for economic or technical reasons, due to considerable difficulties [to change the supplier] or due to substantial additional costs.' In Swiss IT procurement, figures for direct awards are twice as high as in other sectors.[15]

II. The Swiss OSS Obligation: Article 9 EMOTA

Swiss OSS proponents have demanded the publication of the source code of 'government software' for years, until their efforts have finally led to the adoption of a legal base for OSS,[16] the EMOTA, also broadly referred to as 'Digitalisation Law.'

The law entered into force in January 2024 and covers various aspects of public sector digitalisation, such as open data and interoperability of standards. Article 9 focuses on OSS, stating that: 'The federal authorities subject to this law shall disclose the source code of the software they develop or have commissioned [by third parties] to fulfil their tasks, unless the rights of third parties or security-related reasons would exclude or limit this.' Paragraph 2 further

8 This could be private individuals, companies or even public authorities, see for example European Commission (n 8) 28.

9 See Rika Koch and Simon Schlauri, 'Open Source Software im EMBAG - Analyse des neuen Art. 9 des Bundesgesetzes über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben', in Rika Koch and Lara Biehl and Thomas Fischer (eds), *Alles neu?, Beschaffungswelt im Wandel, Konferenzband 2024* (Weblaw 2024), 22 and 23.

10 For details on this principle and an explanatory video, see webpage 'Public Money Public Code' provided by the Free Software Foundation Europe FSFE, available at <https://publiccode.eu/en/> accessed 11 June 2025.

11 See Koch and Schlauri (n10) 24, see also Sanchez-Graells in the context of AI and 'buy once, use many times' (n 2) 205.

12 Also referred to as technological lock-in, for details see also Sanchez-Graells (n 2) 205.

13 Matthias Stürmer, 'Technologische Perspektive der digitalen Souveränität – Bericht zuhanden des Eidgenössischen Departements für auswärtige Angelegenheiten' (2024) 8, available at <www.bfh.ch/de/aktuell/news/2024/neue-studie-digitale-souveraenitaet/> accessed 11 June 2025.

14 The Intercantonal Agreement on Public Procurement (IAPP) that regulates the sub-federal level contains an analogous clause.

15 Matthias Stürmer and Oliver Krancher and Thomas Myrach, 'When the Exception Becomes the Norm: Direct Awards to IT Vendors by the Swiss Public Sector' in Rehema Baguma and Rahula De' and Tomasz Janowski (eds), *ICEGOV '17: Proceedings of the 10th International Conference on Theory and Practice of Electronic Governance (*Association for Computing Machinery 2017*)*.

16 For an overview of the negotiation history of the EMOTA, see Koch and Schlauri (n 10) 22 and 23.

www.lexxion.eu

states that: '[The federal authorities] allow anyone to use, further develop, and distribute the software, and do not charge any licensing fees.'

This provision nicely outlines the key obligations for software to be defined as 'open source' in the Swiss government context: (1) the obligation to disclose and allow free use, development, and distribution, (2) the scope that covers software developed or commissioned by the respective authority, and (3) two grounds for exceptions. These three elements will be briefly assessed in the following.

1. Scope and Content of the Swiss OSS Obligation

The first element of the OSS obligation is the obligation to disclose the source code of the software. Neither the EMOTA nor its implementing ordinance encompass a legal definition of the term 'source code.'

In common language, source code is referred to as the program code, which is the centrepiece of any software.[17] The OSS obligation also contains the obligation to allow the use, further development and redistribution of the respective software free of charge. As opposed to proprietary software that operates with restricted usage rights, OSS cannot restrict usage rights to specific users or usages.[18] Disclosure of the source code should take place on a widely known open-source platform, such as GitHub.[19]

The second element of Article 9, the reference to 'software they develop or have commissioned', means that the OSS obligation applies to software that is developed in-house,[20] or whose development is procured (ie, commissioned) by third-party software developers. Given that most digital technologies are not developed in-house, the second scenario presumably covers the majority of cases of software used by public administrations.[21] Noteworthy is that the law only applies to the procurement of software that was newly developed for the public administration (as opposed to already developed software that is procured 'off-the-shelf'). In other words, public authorities must comply with the OSS obligation only when they decide that their needs cannot be met by existing software (standard software) and a new software must be developed (specialised application). This can be illustrated by the example of the Swiss COVID certificate application, where the COVID-19 pandemic created the need for a novel digital solution, namely an application to prove that Swiss citizens have been vaccinated (see table below).[22]

2. Exceptions from the Swiss OSS Obligation

Article 9(1) EMOTA states two grounds of exceptions that can be invoked by public authorities to derogate from the OSS obligation: (1) Third party rights and (2) security-related reasons.

As for the first category, third-party rights primarily refer to IP rights held by software developers. Since these IP rights are usually transferred from the supplier to the procuring authorities,[23] this typically does not create an issue for OSS. However, there are cases where software is not developed 'from scratch' but based on pre-existing software modules.[24] If pre-existing modules used in the development of new software are already licensed under a proprietary license, a disclosure of the source code can be difficult. If consent of the developer cannot be obtained, at least the newly developed components of the software should be released under OSS.[25] If this is not

17 The auxiliary documents (referred to as 'OSS tools') by the Swiss Federal Chancellery specify that the obligation of disclosure also refers to 'libraries', as well as 'plug-ins' and 'add-ons', see Federal Chancellery, ' EM002-2: Instructions for Publishing Open Source Software, Recommendation for Federal Administration IT' (2025) 6, available at <www.bk.admin.ch/bk/en/home/digitale-transformation-ikt- lenkung/bundesarchitektur/open_source_software/hilfsmittel_oss.html> accessed 11 June 2025.

18 Koch and Schlauri (n 1012) 26.

19 The website provides an overview of organisations and authorities that are active on GitHub see <https://ossbenchmark.com> accessed 11 June 2025. The OSS tool 'EM002-2' contains a list of other conceivable platforms, see Federal Chancellery (n 18) 17.

20 In this context, it is unclear to what extent this obligation applies only to services developed strictly within the same entity (in-house) or also to those developed by other public sector entities at the same federal level (referred to in the Swiss context as 'instate' procurement, see Rika Koch and Caroline Lehner, 'The In-State Exception in Swiss Public Procurement Law: A Largely Unregulated Regulation', in *European Yearbook of International Economic Law 2023* (Springer 2024).

21 Sanchez-Graells (n 2) 34.

22 In this use case, the authority (the Federal Office of Information Technology, Systems and Telecommunications, FOITT) decided to commission the development of the COVID software as open source, even though there was not yet a legal mandate to do so.

23 This is stated in para 25 of the 'General terms and conditions for IT work contracts and contracts for the maintenance of individual software packages' (status as of January 2024) that apply in IT contracts with federal procuring authorities.

24 See for example Wolfgang Straub, *Softwareschutz - Urheberrecht, Patentrecht, Open Source* (Dike 2024), 9.

25 Koch and Schlauri (n 10) 30.

Type of software	OSS Obligation	Public Procurement Law
In-house development of software	✓	X (make)
Procurement of development services for special software	✓	✓ (buy)
Procurement of standard-software	X	✓ (buy)

Table 1.

possible, due to a proprietary license stipulating that any further developments of the modules must be licensed under proprietary terms, a conflict arises with the OSS obligation set out in the EMOTA. To avoid such a problem and to increase legal certainty, procurement authorities should include the OSS obligation of new tenders in the tender documents. Authorities can make compliance with the OSS obligation a mandatory selection criterion or specify acceptable licenses as a technical specification.

The second category of security-related reasons remains vague, as the term is not specified in the law or its legislative materials. The auxiliary documents of the Swiss Chancellery state that the term relates to confidentiality, integrity or traceability and that certain algorithms and procedures visible in the source code should not become public (such as offensive cyber capabilities or details of fraud detection).[26]

France, for example, exempts the disclosure of the source code of systems used to detect tax fraud from its obligation to render algorithmic systems transparent.[27] The Swiss auxiliary documents further point out the fact that the security-related purpose of the software itself cannot be a general ground for exclusion. For example, software used by the federal police must be published as open source, unless reasons relating to the structure of the source code speak against it.

Even when security-related reasons limit the disclosure of the source code, authorities should not entirely disregard the OSS obligation but should instead explore ways to delimit sensitive information and disclose non-sensitive information. The policy implication of this exception remains unclear, as it is usually not the disclosure of source code that jeopardises security, but factors like the quality of the source code and regular updates and patches.[28]

III. Conclusion

Switzerland is usually not a first mover when it comes to the modernisation of public procurement laws.[29] However, in 2024, Switzerland introduced the thus far broadest OSS obligation that impacts the procurement of public administration software.

The new Swiss rule highlights that the decision between purchasing standard software or developing tailor-made software for the public sector has become increasingly important. This decision is not only crucial in determining whether the OSS obligation applies - it is also decisive for the question of how much transparency should be granted to citizens and how much a country is willing to accept dependency from IT-suppliers, typically 'big tech' companies.

Although the policy implications of this new regulation remain to be seen, in particular when it comes to the application of security-related exceptions, the OSS obligation can be viewed as a big step towards efficiency, service quality, transparency and accountability of the public sector.

26 Federal Chancellery (n 18) 10.

27 Lasbleiz and Obrecht (n 5) 38.

28 Koch and Schlauri (n 10) 31.

29 Switzerland was the last country to ratify the revised Government Procurement Agreement (GPA) of 2012.