Open Source Software Compliance

More and more companies are relying on open-source software. However, even open-source software (OSS) is not lawless software and there are legal risks if regulations are not observed. We support you in minimising these risks in your company.

A white paper by Stefan Hessel, LL.M. and Christina Kiefer, LL.M.

Open-source software (OSS) has become an indispensable part of everyday life in many companies. In a survey from 2021, 87% of companies with more than 2,000 employees said they use open-source software in their company.[1] Every fifth company uses OSS as a component of its own products and services, which are passed on to customers with source code adaptations.[2] The cost savings, access to the source code and the ease of switching providers are particularly appreciated.[3] The areas of application are diverse. German automobile companies are also increasingly turning to OSS. Volkswagen relies partly on open source for the development of its VW.OS operating system.[4] Mercedes-Benz recently published a manifesto to encourage employees to use and promote appropriate software.[5]

However, OSS is not lawless software, and violations of the licensing provisions may result in prohibitory injunction, (fictitious) licence fees or even the obligation to destroy or take back the reproduction copies. The use of certain open-source source codes may even result in the obligation to disclose one's own programme code and thus in the disclosure of trade secrets. It is therefore essential to consider OSS compliance as part of a comprehensive Compliance Management System (CMS) in the company.

Use of the software

OSS licences aim to grant the purchaser certain rights that go beyond the rights that the purchaser of software usually receives. These include, for example, the right to further develop and distribute the software. In return, they impose certain obligations on the purchaser. This is done by concluding a licence agreement between the purchaser and the rights holder, who need not necessarily be the distributor from whom the software was purchased. The offer to conclude the licence agreement is to be seen in the licence text supplied, which is why the obligation to supply the licence text when redistributing the software is essential for the functioning of

[1] Bitkom e.V., Open-Source-Monitor, study report 2021, p. 21, available at: https://www.bitkom.org/sites/main/files/2021-12/211207-bitkom-studie-openmonitor-2021.pdf, last accessed: 10/07/2023.
[2] Ibid, p. 22.
[3] Ibid, p. 15.
[4] News report: VW wants to make car software partly open source, available at: https://www.golem.de/news/cariad-vw-will-auto-software-teils-open-source-machen-2206-166355.html, last accessed: 10/07/2023.
[5] Mercedes-Benz AG, FOSS Manifesto, available at: https://opensource.mercedes-benz.com/manifesto/, last accessed: 10/07/2023; News report: Why Mercedes-Benz relies on Open Source, available at: https://background.tagesspiegel.de/mobilitaet/warum-mercedes-benz-auf-open-source-setzt, last accessed: 10/07/2023.

the model. Acceptance of the offer is deemed to take place through modification of the software or through another act of use that requires further authorisation.[6] Due to the continuous further development of OSS by a larger group of people, there are usually several rights holders with whom corresponding contracts must be concluded.[7] This in turn can lead to a large number of contractual partners that may be difficult to handle in individual cases and who may be entitled to claims in the event of breaches of contract, thus significantly increasing the risk of legal disputes in the event of non-compliance.

There are a variety of different OSS licences. The crucial points that are common to all of them in order to be considered open source are:

- They allow the unrestricted redistribution of the software;
- The software must be available in source code; if it is redistributed in compiled form, the source code must be accessible;
- It must allow the modification and further development of the software.

Detailed knowledge of the licence terms is crucial: the licence agreement is regularly subject to dissolution by the breach of the contractual conditions. A breach then automatically leads to the loss of the right of use.[8] In order to avoid this drastic consequence, a thorough examination of the licences used is necessary, which can be a considerable challenge, especially for larger projects.

Software development

In the course of the modularisation of software development, entire programme libraries or smaller parts are increasingly being reused. Almost all newer development projects therefore contain at least traces of open-source code. Besides the many advantages, however, there are also considerable risks. Many OSS licences contain more or less strict so-called copyleft clauses. These stipulate that adaptations, when redistributed, must be subjected to the original licence. In the case of software without a corresponding protection clause, embedding of this software into proprietary software is possible in principle. If a copyleft clause exists, it should be noted that some licences provide that in this case the terms of use of the software can spread virally to the other parts - with the consequence that the source code of the proprietary software may have to be disclosed.[9]

The uncertainties are increased by the fact that the question of when a further development ("derivative work") exists has not yet been answered by the courts.[10] In the absence of supreme court rulings, it therefore depends on the interpretation of the licence texts and the circumstances of the individual case. With regard to the interpretation of the contract, the OSS licences themselves may already contain certain interpretation aids. Furthermore, it must be taken into account that due to the mostly international use of OSS, the respective interpretation in the individual case must also be reviewed with regard to

---

[6] *Jaeger/Metzger*, Open Source Software, 5th ed. 2020, para. 249.
[7] Ibid, para. 250.
[8] *Frank/Schulz*, in: Berger/Wündisch, Urhebervertragsrecht, 3rd ed. 2022, § 22 para. 105.
[9] *Huppertz*, in: Leupold/Wiebe/Glossner, IT-Recht, 4th ed. 2021, part 2.4.2. open source software licences, para. 51 et seqq.
[10] *Jaeger/Metzger*, Open Source Software, 5th ed. 2020, para. 52; *Lehmann/Spindler* in: Loewenheim, Handbuch des Urheberrechts, 3rd ed. 2021, § 82 para. 99 et seq.

the understanding of the relevant legal terms in the US legal sphere.[11]

Cloud services

Many of the common licences were already formulated in the 1990s. At that time, the network infrastructure was not yet powerful enough to enable models such as application service providing (ASP) or software as a service (SaaS). That is why there are usually no explicit regulations relating to this in the licences. With both ASP and SaaS, software and infrastructure are operated by external IT service providers. The users, e.g. the employees of a company, access these services via the internet.

But how is it to be assessed in legal terms when service providers offer the use of OSS in the cloud? This question cannot be answered uniformly and requires a thorough examination of the specific licence to see whether there are indications that the transfer of corresponding rights of use was actually intended. Generally, SaaS providers, for making the cloud services available to the customers for use, require the right of making the OSS available to the public. It is legally disputed whether the providers also need a right of use for reproduction. Although the prevailing opinion denies this, this point should be examined in any individual case. Particular problems arise if the software used includes hundreds of different licences, which is often the case with larger projects.[12] In these cases in particular, a careful examination is required, if necessary with the help of technical aids such as OSS scanners, as to whether and to what extent the software can be offered as a service in the cloud with a reasonable legal risk.

Legal risks for users of cloud services can arise in particular with regard to the passing on of cloud services. While the pure enjoyment of works is not subject to licensing requirements, the transfer of cloud services in the sense of distribution may be subject to strict licensing requirements. Among other things, it is important to distinguish between internal, group-wide and external transfer of the services. While in the first case, depending on the interpretation of the contract, there is no distribution in terms of licensing law, in the other two cases, depending on the licensing system, there are strict obligations that require OSS compliance measures.[13]

Embedded Systems

Increasingly, open-source code is finding its way into embedded systems. This poses particular problems in terms of compliance with certain requirements of the licence terms. Most licences require that a copy of the licence text be supplied with the licensed software when it is redistributed. It is in principle thinkable to supply the licence text in hard copy form, but software today often contains components that are subject to dozens of licences, quickly resulting in documents with hundreds of pages of text.[14] If the device has a display, it is conceivable to show the licence text there. If such a display is missing in the individual case, according to a liberal view, the reproduction of the licence texts via the interface used by the device and thus also e.g. via the integration of a suitable interface should be sufficient.[15] Whether

[11] *Schöttle*, MMR 2020, 801, 804; *Redeker*, IT-Recht, 7th ed. 2020, A.II.1. para. 101.
[12] *Schöttle*, MMR 2020, 801, 803 et seqq.
[13] *Redeker*, IT-Recht, 7th ed. 2020, A.II.1. para. 101.
[14] *Schöttle*, DSRITB 2017, 463, 467.
[15] *Free Software Foundation*, Frequently Asked Questions about the GNU Licenses, available at: https://www.gnu.org/licenses/gpl-

such "reproduction" is sufficient for the "transfer" in terms of licensing law is, however, disputed and requires examination in each individual case. In practice, it is also problematic to find out which licence texts must be supplied. The components used often contain sub-components for which it is not immediately clear which terms of use they are subject to.[16] Further problems result from the inclusion of a disclaimer, the representation of copyright notices and the supply of the source code. In particular, the requirements for the reproduction of copyright notices are controversial.[17] In some cases, stricter formal requirements are imposed for the provision of copyright notices than for the reproduction of licence texts. In order to meet the strict requirements in any individual case and to avoid licence infringements, the relevant requirements must be checked in advance and already taken into account during the product design (keyword: OSS compliance by design).

What to expect in case of infringements

Pursuant to § 130 (1) of the German Regulatory Offences Act (OWiG), the management has a personal duty of supervision to avoid punishable illegal acts in the company. Such acts may also occur in the case of copyright infringements relating to OSS. They may, for example, represent criminal offences under §§ 106, 108 of the German Copyright Act (UrhG).[18] In addition, there is a threat of prohibitory injunctions and claims for removal. Even in the case of free software, there is a threat of claims for damages.[19] As a consequence of the copyleft clause, non-compliance with the terms of use can lead to the obligation to disclose the source code of proprietary software and thus to the loss of trade secrets. The consequences of non-compliance with the terms of a licence can also be drastic in the case of embedded systems. Here, in extreme cases, there is a threat of recall of the entire device (§ 98 (2) UrhG), even if only the software is affected.

Step by step to OSS compliance

To avoid these consequences, which may be drastic from time to time, companies should implement OSS compliance as part of a holistic CMS.

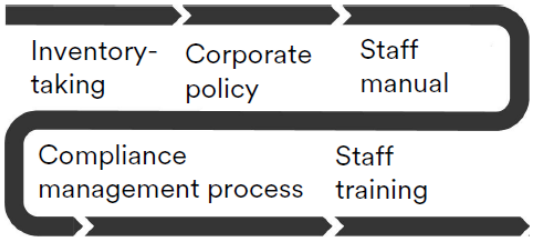

Figure 1: Steps towards OSS compliance
© reuschlaw, 2023

As a first step, an open-source policy should be developed and adopted. For this purpose, it is advisable to create a manual that contains the typically used licences with the most important related information and application instructions and is intended to facilitate the employees' daily work.

Furthermore, it is essential to get an overview of the OSS(s) used in the company. In many cases, this is a demanding task that should be carried out with technical aids such as OSS scanners, especially in the context of software development. It should be noted that OSS can also enter the company via

faq.html#NonvisualLegalNotices, last accessed: 10/07/2023.
[16] *Schöttle*, DSRITB 2017, 463, 467 et seq.
[17] Ibid, 469 et seq.
[18] *Jaeger/Metzger*, Open Source Software, 5th ed. 2020, para. 27.
[19] *Heinzke/Burke*, CCZ 2017, 56, 59.

subcontractors. Risks resulting from this should therefore be minimised through intelligent contract design. It is conceivable to oblige the subcontractors to disclose the OSS used or to carry out an OpenChain Self Certification.

In addition, processes for the introduction of new software should be established, e.g. in the form of an approval procedure by an open-source review board. Ideally, the board should be composed of representatives from the legal, engineering and product teams.

Finally, an OSS compliance officer should be appointed in the company and the employees concerned should be sensitised to the legal framework through training.

A functioning CMS can not only help to ensure compliance. If breaches occur, it can also help to invalidate accusations of negligence on the part of the company's management. Preventive measures must also be taken into account in the context of proportionality checks, which may prevent claims for recall, destruction or surrender (§ 98 (4) 1 UrhG).

Our support to you

We help you to use the advantages and potential of OSS in your company and to minimise legal risks. Our services cover all necessary steps to build a reliable OSS CMS. These include:

- Taking an inventory of OSS used and their licence terms;
- Corporate policies on the use of OSS;
- Staff manuals with key licensing requirements and recommended actions;
- Designing processes to comply with licensing requirements, e.g. when introducing new OSS;
- Staff training to raise awareness.

Next step: Get in touch

We are looking forward to supporting you on your way to OSS compliance. We would be pleased to explain the details of our approach to you in a personal meeting. Get in touch with us without obligation!

T + 49 681 / 859 160 0

E info@reuschlaw.de