EDITOR DIRK RIEHLE
Friedrich Alexander-University of Erlangen Nürnberg;
dirk.riehle@fau.de

Open Source License Compliance— Why and How?

Hendrik Schöttle, Osborne Clarke

Compliance with open source software (OSS) license requirements is necessary but often overlooked. This article explains how OSS license compliance differs from compliance with commercial software licenses, why it is necessary even though OSS is generally free, and what requirements have to be met with OSS.

W hen distributing open source software (OSS) components as standalone software or as part of one's own software projects, an essential step to ensure compliance with the respective license requirements is often neglected, and its complexity is often underestimated.

DIFFERENCES BETWEEN COMMERCIAL LICENSES AND OSS LICENSES

Why is OSS license compliance so complex? The difficulties become evident when comparing OSS licenses with commercial ones. With most commercial licenses, the main obligation of the licensee consists of only a payment for the right to use or distribute the software. Commercial licenses may come with specific restrictions concerning the license metrics in the form of concurrent-user licenses or special requirements for the indirect use of software or its distribution; however, the main obligation (also in these just-mentioned cases) is the payment of remuneration for the use of the software.

Most OSS licenses work differently than commercial licenses. They do not involve payments. However, many require the provision of license texts or other information along with provision of the software. Some licenses require the provision or offer of the OSS component's source code in cases when the software is provided in binary form only.

Besides purely commercial and purely open source-licensed projects, many intermediate forms exist. Almost every larger piece of software these days contains OSS components. Some commercial software is also licensed in a dual licensing model, where the same component is available under an OSS license and under a commercial license that exempts the recipient from the OSS license's requirements. Another common licensing model is the open core model, which offers the basic technology under an OSS license and additional functionality or add-ons as proprietary software under a commercial license.

WHY COMPLIANCE?

Why is open source compliance so essential? Isn't it all about free software? If there are no companies behind such licenses, do you really have to fear any enforcement in case of noncompliance?

First, as already mentioned, OSS-licensed software may be part of a dual licensing strategy, with a company, and thus commercial aims, behind it. Second, some efforts are being made within the community to enforce OSS licenses so as to raise awareness about compliance, resulting in court claims.[1] Third, some software developers have established a business model by attacking companies in cases of noncompliance with OSS licenses. It is said that one of them has earned millions of euros as a result.[2] In the case of some OSS licenses, such as the GNU General Public License v2.0 (GPL-2.0), the usage and distribution rights terminate upon breach of the license obligations. As a consequence, a licensor may request a software producer to refrain from future distribution of his or her components. Especially under German law, it is rather easy to get a cease and desist order from a competent court in such cases, which has led in the recent past to what has been called *open source trolling*.[3]

MAIN OBLIGATIONS OF OSS LICENSES

The main obligations that come with OSS licenses can be separated into two categories: organizational requirements concerning the handling of the OSS and obligations concerning information and documentation.

Organizational requirements

Copyleft effect. Regarding the handling of OSS components, some OSS licenses, such as the GPL, the GNU Lesser GPL (LGPL), and the GNU Affero GPL (AGPL) contain a so-called copyleft effect: derivative works of such OSS components have to be licensed under the same OSS license (see, e.g., section 2b of GPL-2.0).[4] This effect can be triggered by, for example, statically linking an LGPL-licensed library to proprietary code. To avoid the copyleft effect, one has to either link dynamically, in the case of the LGPL, or, if this is not sufficient (as with GPL-licensed software, under which any linking triggers the effect), refrain from using the respective OSS component. Ensuring the avoidance of such copyleft effect can become an essential element of an open source compliance process. Assessing whether the copyleft effect applies is not easy in practice, as it does not depend only on technical requirements that can be evaluated automatically. It gets further complicated when third-party components come into play that have not been assembled by the distributor of the final software. In this case, the necessary knowledge required to answer the copyleft question is not available to the distributor, which makes it practically impossible to answer this question.

Modification of OSS. Other organizational requirements cover the modification of OSS. In distributions of modified versions, some licenses require that such changes be formally highlighted together with accompanying information on the date and scope of changes made, or they require that modified components be renamed to avoid confusion with the original version (see, e.g., section 2a of GPL-2.0).[4]

Digital rights management-protected environment. Some licenses require that the user be able to install modified versions of the OSS components on a device (see, e.g., section 6, paragraph 5 of GPL-3.0).[5] In practice, this prohibits the use of such software in a digital-rights-management-protected environment. As a consequence, software distributed under such licenses cannot be used on any device that uses cryptographic protection and executes only respectively signed

binary files. (This prohibits, e.g., the use of GPL-3.0-licensed software on an iPhone.)

Information and documentation requirements

License text. Besides the organizational requirements, most open source licenses contain specific obligations concerning information and documentation. In many cases, licenses require that the respective license text be delivered together with the software when it is distributed.

Let's take a look at the obligations of the GPL-2.0, one of the most common open source licenses found in the field. According to section 1 of GPL-2.0, a copy of the license conditions must be delivered together with each program copy. This can be done in physical form as a printout or nonphysically by adding a corresponding text file. According to German case law, the mere provision of a link to the license text is not sufficient.[6]

In practice, the applicable licenses for OSS components contained in proprietary software are often simply copied together as one large text file without specifying which component the respective licenses are applicable to. This likely does not meet the requirements of the licenses. Rather, the respective texts have to be assigned with the corresponding licensed software packages so that the correct license texts are assigned to each individual component.

Missing license texts are a classic case of license infringement, which can lead to the loss of all usage rights in the case of some licenses (see section 4 of GPL-2.0)[4], and that, in practice, sometimes entails enforcement actions such as an interim injunction.

Copyright notices. Besides the license text, in many cases the provision of a copyright notice mentioning the name of the author is also required. Section 1 of GPL-2.0 requires the distributor to "conspicuously and appropriately publish on each copy an appropriate copyright notice."

The copyright notices can usually be found in several locations within software. Some of them are contained in the file with the license texts. Furthermore, the source files can also contain copyright notices, often distributed over hundreds or thousands of files. The notices will not be found in the binary code of the software, however, as a compiler regards them only as comments that are removed when compiling the source files.

In case of GPL-2.0, there is controversy over whether it is sufficient to simply provide the copyright notices from the license texts or necessary to additionally extract the copyright notices from the individual source files for the distribution of the binary files, which involves considerable effort for larger components. The wording of section 1 of GPL-2.0 permits an interpretation in such a way that an extraction of the copyright notices is required.[7,8]

Special notices. Some licenses require special notices or notices in a special form, such as the Berkeley Source Distribution (BSD)-4 Clause, which requires that an acknowledgment be displayed in advertisements mentioning features or use of the licensed software. In this case, the OSS licenses can affect marketing materials or other elements that are not usually taken into consideration when dealing with OSS.

Bill of materials. Probably the best way to fulfill the foregoing information and documentation requirements is to create and maintain a bill of materials as one central document in which all necessary texts, notes, and information are contained in a structured manner.

This bill of materials should be delivered together with the software and additionally be made part of the contract concluded with the recipient of the software (who generally requires information prior to conclusion of such a contract). The latter can be achieved by making the bill of materials available on the Internet and referring in the terms and conditions to the use of third-party components and to a landing page via which the user can access the applicable documents for the components. However, one should keep in mind that this is not sufficient with regard to many licenses' obligations.

Provision of the source code

Some OSS licenses require the provision of the source code in cases in which the software package is provided in binary form only. In some cases, a written offer to provide the source code upon request is sufficient (see section 3b of GPL-2.0).[4] In other cases, such an offer is not sufficient, and the source code has to be made available in a certain form, e.g., as a download from a server when the binary file is made available in the same way (see section 6d of GPL-3.0).[5]

In the previous examples, the source code provided has to be exactly the same source code that is the basis of the respective binaries. It is not sufficient to refer to the official project's website or to an online repository for the unmodified source files of the official branch. This would be sufficient only in cases in which the OSS is used without any modification; even in such cases, the distributor remains responsible for the availability of the website or repository.

In case of updates to the software, that source code also has to be made available. As a consequence, the user of an embedded system or a desktop software package has to be able to determine which version of the software is being used. Additionally, the manufacturer has to maintain a repository that archives all older versions of the software that have been distributed.

When a written offer is sufficient, it is recommended to ensure that it legally complies with the license requirements. The author of this article has supported companies that were attacked in several cases where such

a written offer was missing or considered to be insufficient.

When do the license obligations apply?

Unlike many commercial software products, most OSS licenses do not restrict the internal handling of the software, e.g., by limiting the number of concurrent users or cores or by comparable license metrics. They do require distribution of the software to trigger the license obligations. Most licenses' obligations are also not triggered when access is provided to the software as a service. However, a handful of OSS licenses also do impose specific obligations in this case, such as the AGPL or the Server Side Public License.

In practice, it is recommended to comply with OSS license requirements anyway. Even when only software as a service is provided, a customer may require an on-premise solution. In that case, a distribution of software would be issued, and the respective obligations of the OSS license would be triggered.

It is often forgotten that the provision of unmodified software as part of a bundle of software components also triggers the obligations of the underlying OSS licenses, for example, in case of provision of a Linux distribution as the basis for an embedded system. However, many OSS components still lack the information that has to be provided when they are distributed.

MISTAKES COMMONLY MADE

Even though many companies strive to achieve compliance when dealing with third-party software components, some of them fail in practice. It may help to take a closer look at mistakes that are commonly made.

Negligence of formal requirements

Many companies concentrate their efforts on the questions of whether and to what extent the copyleft effect applies. In practice, however, the licensing obligations enforced most often are formal noncompliance issues such as missing license texts or a missing written offer of the source code.

Avoiding the copyleft effect may be essential. However, it is just as important to ensure compliance with the formal requirements. These may seem less critical at first sight, but as enforcement is focused on these formal requirements, they should be an essential part of a compliance process.

No recursive scanning

Another mistake is to focus only on the main components of third-party software and ignore the subcomponents within. A developer is generally interested in the main component only and does not care about possible subcomponents. From a compliance point of view, however, it is irrelevant

> In practice, however, the licensing obligations enforced most often are formal noncompliance issues such as missing license texts or a missing written offer of the source code.

whether the distributor has included a third-party component directly or whether the third-party component has snuck into the software package as a subcomponent. Every piece of software must be distributed properly.

A good example is the Linux kernel. It is common understanding that the Linux kernel is licensed under the GPL-2.0. However, in practice, the kernel consists of hundreds of subcomponents. A source code scan reveals about 90 different licenses. Even though there may be duplicates among them, this shows that the Linux kernel is far from being one coherent piece of software licensed under one license only. Although it increases the efforts involved in OSS compliance dramatically, it is strongly recommended to recursively scan through all third-party components to ensure no subcomponent is missed.

OSS licenses are templates only, not laws

Finally, it is another common understanding that licenses are interpreted by their creators in case of doubt, for example, by the Free Software Foundation in the case of the GPL. While this is surely the best approach when no other interpretation is available, this may not be the correct way when copyright holders and licensors of software components have expressed their own understanding of such licenses.

OSS licenses are generally based on template documents. However, the basis is a template document only and not a law. Whenever such licenses are subject to interpretation, one has to take a look at the respective will and understanding of the parties involved. And if such parties express their understanding in a way that has to be considered by the other party, there are very good arguments that this understanding becomes part of the license agreement, even if it contradicts the official understanding of the creators of such licenses.

In practice, this may lead to different results. For instance, take the copyleft effect. In the case of identical handling of two software components, both licensed under GPL-2.0, the copyleft may be triggered in one case, whereas it is not triggered in the other case only because one licensor has expressed an understanding that the copyleft effect is given, whereas the other licensor interprets the same license differently. As a consequence, it is strongly recommended, if in doubt, to consider a project's website, frequently asked questions list, and other available documentation together with the software.
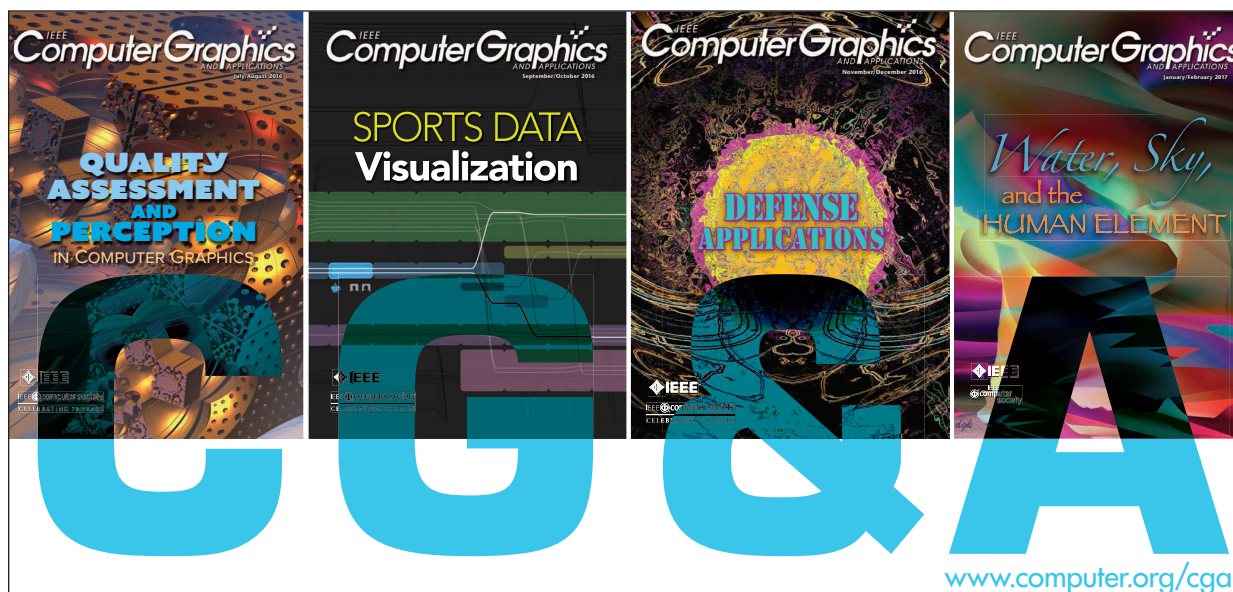
OSS compliance may be difficult. In particular, the information and documentation requirements are harder to fulfill than

they seem. However, as cases of OSS license enforcement have increased in the recent past, OSS license requirements can no longer be neglected. It is essential to set up the necessary processes to ensure license compliance when dealing with OSS. One essential element of such compliance is setting up a tailor-made OSS policy. Once it is drafted, compliance with it has to be ensured. Unless the number of OSS components and software updates is limited, tools for scanning and administering the necessary information are unavoidable. However, as the task of OSS compliance cannot be fully automated, an open source board staffed with representatives with sufficient technical and legal skills will need to review and assess the tools' results. ▣

REFERENCES

1. The gpl-violations.org project. Accessed on: June 14, 2019. [Online]. Available: http://gpl-violations .org
2. S. J. Vaughan-Nichols, "Linux beats legal threat from one of its own developers," ZDNet, Mar. 8, 2018. [Online]. Available: https://www.zdnet.com/article /linux-beats-internal-legal-threat/
3. S. Sharwood, "Linux kernel community tries to castrate GPL copyright troll," The Register, Oct. 18, 2017. [Online]. Available: https://www .theregister.co.uk/2017/10/18/linux_ kernel_community_enforcement_ statement/
4. Free Software Foundation, "GNU General Public License, version 2," June 1991. [Online]. Available: https://www.gnu.org/licenses /old-licenses/gpl-2.0.en.html
5. Free Software Foundation, "GNU General Public License," June 2007. [Online]. Available: https://www .gnu.org/licenses/gpl-3.0.en.html
6. "LG Munich I, judgment v. 12.07.2007, Az. 7 O 5245/07," Institute for Legal Issues of Free and Open Source Software, July 12, 2007. [Online]. Available: http:// www.ifross.org/Fremdartikel /LGMuenchenUrteil.pdf
7. T. Jaeger and A. Metzger, *Open Source Software*, 4th ed. (in German), Munich: C. H. Beck, 2017, marginal 37.
8. A. Hemel and S. Coughlan, *Practical GPL Compliance*. San Francisco: Linux Foundation, 2017, p. 39.

HENDRIK SCHÖTTLE is a partner and IT law specialist at Osborne Clarke in Munich, Germany. Contact him at Hendrik.Schoettle@osborneclarke .com.