Open
Source
Automation
Development
Lab eG

OSADL eG · Im Neuenheimer Feld 583 · D-69120 Heidelberg

Content and scope of the OSADL Compliance Check

for Free and Open Source software (FOSS)

1. Objectives

Compliance with legal and contractual obligations is part of every company's risk management. This includes obligations arising from copyright law and, based on this, from FOSS licenses. The term "FOSS compliance" refers to the consideration of these obligations and any additional internal guidelines that may exist. For Linux-based systems, OSADL offers the License Compliance Audit (LCA), which checks in detail the compliance of a specific product with the license obligations of GPL-2.0 for the Linux kernel and the license of the associated C library, for example LGPL-2.1 for glibc. Although this product audit also evaluates internal company processes, OSADL would like to offer its members another option for reviewing Open Source license obligations and related company processes with the OSADL Compliance Check.

Like the LCA, the compliance check refers to a specific product, but considers all Open Source software contained therein and is not limited to Linux-based systems. However, the check is not carried out in detail for the licensing obligations of each individual component. Rather, the aim is to check whether the FOSS compliance materials made available with the product are consistent overall. In addition, individual components and license obligations are checked in detail on a random basis. In addition, the company processes that contribute to the creation of the FOSS compliance materials are considered.

The compliance check allows companies to verify whether their processes are fundamentally suitable for achieving FOSS compliance for their products and whether the tested product can essentially be distributed in compliance with the applicable licenses.

2. Scope

The OSADL Compliance Check always refers to a specific product, even if an additional assessment of internal company processes for compliance with FOSS license conditions is carried out. The reason for this is the approach of not only evaluating processes, but also using the results to check whether license requirements can be fundamentally complied with.

It should be noted that a thorough understanding of license terms depends on legal interpretation. However, not all questions of interpretation are decided in court. In the event of an ambiguous situation, the requirements of the compliance check are based on a reasonable but strict interpretation. Further details on such positions can be found in the Legal FAQ on the OSADL website (for members only) and/or in the corresponding audit report after completion of the compliance check.

The OSADL Compliance Check is primarily focused on compliance with FOSS license terms relating to copyright. It does not check for infringements of third-party patents. Such patents may not be used without the consent of the patent holder. It is the responsibility of each user of the respective Open Source software to carry out the necessary patent research and to check that their own patents are licensed to the required extent.

3. Content

The purpose of the OSADL Compliance Check is to review the FOSS compliance materials associated with a product to determine whether they are suitable for fulfilling the license obligations for the FOSS components contained therein. The details of the review are always adapted to the given product and the applicable licenses (see 4.), but are based on the following key points:

a) SBOM

The inclusion of a list (optionally in an SBOM standard format such as SPDX or CycloneDX) of the FOSS components contained in the product with the following information is checked.

- Name of the component
- Version of the component
- Applicable licenses
- *optional:* Origin of the component (e.g. URL, package management system)

b) Dependencies

The completeness of the SBOM is verified by checking whether all dependencies required at runtime of a component are also included in the SBOM. In this context, the existing processes for software compliance analysis and the associated tooling are evaluated.

c) Information obligations

Compliance with the information requirements of the FOSS licenses for the components listed in the SBOM is verified.

- License text of all applicable FOSS licenses that require its delivery
- Copyright notices for all components whose licenses require their delivery
- Any additional legal notices, such as separate disclaimers, acknowledgments, NOTICE files, if applicable

A distinction is made here between distribution of the product with FOSS source code and without FOSS source code.

In this context, the tooling used for license scanning is evaluated.

d) Disclosure obligations

If applicable licenses contain disclosure requirements, the following is checked:

- Making the source code available in accordance with the license terms (e.g., immediate delivery, written offer, reference)
- In the case of GNU licenses (AGPL, LGPL, GPL):
  - Verification that a rebuild is possible.
  - Check whether a mechanism for installing modified versions is available.

e) Modified software

If changes have been made to FOSS components under a copyleft license, the correct licensing of these changes is checked. In addition, it is checked whether the licensing has been approved by an authorized representative of the company.

If a license applicable to modified software requires the inclusion of modification notices, their availability is checked.

f) Accompanying documents

The accompanying documents for the product (terms and conditions, EULA, other contractual terms) are checked to ensure that FOSS licenses are taken into account. The legal validity of the wording is not assessed in detail.

g) Linked proprietary components

The product is examined to determine whether proprietary components are linked to FOSS components. For this purpose, callgraphs of the respective proprietary components are created. If the licenses applicable to the linked FOSS components have an impact on the proprietary components, a check is made to ensure that the conditions are met:

- LGPL: permission to modify, permission to re-engineer, re-linkability
- Licenses with unrestricted copyleft: Licensing of the proprietary component under the applicable FOSS license or removal of the copyleft component

4. Typical FOSS licenses

The following typical FOSS licenses are included in many FOSS components. The profiles provided here merely give an overview of the license obligations. The license obligations are determined in detail according to the OSADL License Obligations Checklists for the licenses actually applicable to the product.

- Apache-2.0
  - Permissive
  - Provide license text
  - Provide modification notices
  - Provide adapted NOTICE file with derivative works

- BSD-2-Clause
  - Permissive
  - Provide license text
  - Provide copyright notices

- BSD-3-Clause
  - Permissive
  - Provide license text (often customized)
  - Provide copyright notices

- GPL-2.0
  - Unrestricted copyleft
  - Provide license text
  - Provide copyright notices
  - Provide separate disclaimer
  - Provide modification notices
  - Source code disclosure requirements (immediate delivery or written offer)
  - Rebuild and installation information

- GPL-3.0
  - Unrestricted copyleft
  - Provide license text
  - Provide copyright notices
  - Provide modification notices
  - Source code disclosure requirements (immediate delivery or written offer or reference)
  - Rebuild and installation information

- LGPL-2.1
  - Restricted copyleft
  - Provide license text
  - Provide copyright notices
  - Provide separate disclaimer
  - Provide modification notices
  - Source code disclosure requirements (immediate delivery or written offer)
  - Rebuild and installation information
  - Relinkability
  - Permission to modify, permission to re-engineer linked components

- LGPL-3.0
  - Restricted copyleft
  - Provide license text
  - Provide copyright notices
  - Provide modification notices
  - Source code disclosure requirements (immediate delivery or written offer)
  - Rebuild and installation information
  - Relinkability
  - Permission to modify, permission to re-engineer linked components

- MIT
  - Permissive
  - Provide license text
  - Provide copyright notices

- MPL-2.0
  - Restricted, file-based copyleft
  - Provide license text with source code
  - Provide copyright notices with source code
  - Disclosure requirements (reference)

5. Report

Following the compliance check, the client receives a report summarizing the results of the evaluation, listing any deficiencies, and containing an assessment of the extent to which the license obligations for the assessed product have been taken into account. The report also contains information on the extent to which existing company processes have contributed to FOSS compliance and where there may be gaps.

The report does not confirm license compliance, but rather provides an assessment of whether and to what extent the materials provided are fundamentally suitable for complying with individual license terms of the applicable FOSS licenses

6. Assessors

The OSADL Compliance Check is carried out by appropriately qualified OSADL employees. The assessors have an in-depth understanding of copyright law and practical experience with FOSS licensing. For parts of the compliance check, it is possible to commission external employees who are also appropriately qualified. The final result is always reviewed by an OSADL employee. However, none of the assessors are licensed attorneys; therefore, the result of the compliance check does not constitute individual legal advice.