Open
Source
Automation
Development
Lab eG

OSADL eG · Im Neuenheimer Feld 583 · 69120 Heidelberg

Inhalt und Umfang des OSADL Compliance Checks

für Free und Open Source-Software (FOSS)

1. Ziele

Zum Risikomanagement eines jeden Unternehmens gehört die Einhaltung von gesetzlichen und vertraglichen Pflichten. Dazu gehören die Pflichten, die sich aus dem Urheberrecht und basierend darauf aus FOSS-Lizenzen ergeben. Die Berücksichtigung dieser Pflichten und möglicherweise zusätzlich bestehender interner Richtlinien wird mit dem Begriff „FOSS-Compliance" bezeichnet. Für Linux-basierte Systeme bietet OSADL das License Compliance Audit (LCA) an, in dessen Rahmen die Einhaltung der Lizenzpflichten der GPL-2.0 für den Linuxkernel und der Lizenz der damit verbundenen C-Bibliothek, zum Beispiel der LGPL-2.1 für die glibc, für ein spezifisches Produkt im Detail überprüft werden. Obwohl bei diesem Produktaudit auch die internen Unternehmensprozesse bewertet werden, möchte OSADL seinen Mitgliedern mit dem OSADL Compliance Check eine weitere Möglichkeit zur Überprüfung von Open Source-Lizenzpflichten und verbundenen Unternehmensprozessen anbieten.

Der Compliance Check bezieht sich wie das LCA auf ein spezifisches Produkt, betrachtet aber alle darin enthaltene Open Source-Software und ist nicht auf Linux-basierte Systeme beschränkt. Die Prüfung wird jedoch nicht im Detail für die Lizenzpflichten jeder einzelnen Komponente vorgenommen. Vielmehr soll überprüft werden, ob die mit dem Produkt verfügbar gemachten FOSS-Compliance-Materialien insgesamt konsistent sind. Stichprobenartig werden zusätzlich einzelne Komponenten und Lizenzpflichten im Detail überprüft. Ebenfalls werden die Unternehmensprozesse, die zur Erstellung der FOSS-Compliance-Materialien beitragen, betrachtet.

Mit dem Compliance Check können Unternehmen also überprüfen lassen, ob ihre Prozesse grundsätzlich dazu geeignet sind, FOSS-Compliance für ihre Produkte zu erreichen, und ob das geprüfte Produkt im Wesentlichen lizenzkonform vertrieben werden kann.

2. Prüfungsumfang

Der OSADL Compliance Check bezieht sich stets auf ein konkretes Produkt, auch wenn zusätzlich eine Bewertung der internen Unternehmensprozesse zur Einhaltung der FOSS-Lizenzbedingungen vorgenommen wird. Grund dafür ist der Ansatz, nicht nur Prozesse zu bewerten, sondern anhand der Ergebnisse zu kontrollieren, ob damit Lizenzvorgaben grundsätzlich eingehalten werden können.

Zu beachten ist, dass ein tiefgehendes Verständnis von Lizenzbedingungen von der Rechtsauslegung abhängt. Jedoch werden nicht alle Auslegungsfragen vor Gericht entschieden. Im Falle einer nicht eindeutigen Situation werden die Anforderungen des Compliance Checks auf eine vernünftige aber strenge Sichtweise gegründet. Weitere Ausführungen zu solchen Standpunkten sind in den Juristischen FAQ auf der OSADL-Webseite (nur für Mitglieder) und/oder im entsprechenden Prüfbericht nach Abschluss des Compliance Checks zu finden.

Der OSADL Compliance Check ist primär auf die Einhaltung der auf das Urheberrecht bezogenen FOSS-Lizenzbedingungen ausgerichtet. Eine Prüfung der Verletzung von Patenten Dritter wird nicht vorgenommen. Solche Patente dürfen grundsätzlich nicht ohne Zustimmung des Patentinhabers benutzt werden. Hier obliegt es jedem Nutzer der jeweiligen Open Source-Software selbst, die erforderliche Patentrecherche durchzuführen und zu prüfen, dass eigene Patente in dem erforderlichen Umfang lizenziert werden.

3. Prüfungsinhalt

Gegenstand des OSADL Compliance Checks ist die Überprüfung der zu einem Produkt gehörenden FOSS-Compliance-Materialien daraufhin, ob sie geeignet sind, Lizenzpflichten für die enthaltenen FOSS-Komponenten zu erfüllen. Die Details der Überprüfung werden immer dem gegeben Produkt und den anwendbaren Lizenzen (siehe 4.) angepasst, orientieren sich aber an folgenden Eckpunkten:

a) SBOM

Die Mitlieferung einer Liste (optional in einem SBOM-Standardformat wie z.B. SPDX oder CycloneDX) der enthaltenen FOSS-Komponenten mit folgenden Informationen wird überprüft.

- Name der Komponente
- Version der Komponente
- anwendbare Lizenzen
- *optional:* Ursprung der Komponente (z.B. URL, Paketmanagementsystem)

b) Abhängigkeiten

Die Vollständigkeit der SBOM wird überprüft, indem kontrolliert wird, ob alle zur Laufzeit einer Komponente benötigten abhängigen Komponenten ebenfalls in der SBOM enthalten sind. In diesem Rahmen wird das eingesetzte Tooling oder die bestehenden Prozesse zur Software Compliance Analyse bewertet.

c) Informationspflichten

Die Erfüllung der Informationspflichten der FOSS-Lizenzen für die in der SBOM genannten Komponenten wird überprüft.

- Lizenztext aller anwendbaren FOSS-Lizenzen, die dessen Mitlieferung fordern
- Copyright-Vermerke aller Komponenten, deren Lizenzen die Mitlieferung fordern
- ggf. weitere rechtliche Hinweise wie z.B. separater Haftungsausschluss, Acknowledgments, NOTICE-Datei, falls entsprechende FOSS-Lizenzen, die deren Mitlieferung fordern, anwendbar sind

Hier wird zwischen Vertrieb des Produkts mit FOSS-Quellcode und ohne FOSS-Quellcode unterschieden.

In diesem Rahmen wird das eingesetzte Tooling zum Lizenz-Scanning bewertet.

d) Offenlegungspflichten

Falls anwendbare Lizenzen Offenlegungspflichten enthalten, wird folgendes überprüft:

- Verfügbarmachung des Quellcodes entsprechend der Lizenzbedingungen (z.B. direkte Mitlieferung, schriftliches Angebot, Referenzierung)
- Falls es sich um GNU-Lizenzen (AGPL, LGPL, GPL) handelt:
  - Überprüfung, ob ein Rebuild möglich ist.
  - Überprüfung, ob ein Mechanismus zur Installation modifizierter Versionen vorhanden ist.

e) Modifizierte Software

Falls Änderungen an FOSS-Komponenten unter einer Copyleft-Lizenz vorgenommen wurden, wird die korrekte Lizenzierung dieser Änderungen überprüft. Außerdem wird überprüft, ob für die vorgenommene Lizenzierung eine Freigabe durch eine vertretungsberechtigte Person des Unternehmens vorliegt.

Falls eine auf eine modifizierte Software anwendbare Lizenz die Mitlieferung von Modifikationshinweisen fordert, wird deren Verfügbarkeit überprüft.

f) Begleitdokumente

Die zum Produkt gehörenden Begleitdokumente (AGB, EULA, sonstige Vertragsbedingungen) werden daraufhin geprüft, ob FOSS-Lizenzen berücksichtigt werden. Dabei wird die juristische Gültigkeit verwendeter Formulierungen nicht im Detail bewertet.

g) Verlinkte proprietäre Komponenten

Das Produkt wird daraufhin untersucht, ob proprietäre Komponenten mit FOSS-Komponenten verlinkt sind. Dazu werden Callgraphs der jeweiligen proprietären Komponente erstellt. Falls die auf die verlinkten FOSS-Komponenten anwendbaren Lizenzen Auswirkungen auf die proprietären Komponenten haben, so wird überprüft, ob die gestellten Bedingungen erfüllt werden:

- LGPL: Bearbeitungserlaubnis, Erlaubnis zum Reengineering, Neuverlinkbarkeit
- Lizenzen mit uneingeschränktem Copyleft: Lizenzierung der proprietären Komponente unter der anwendbaren FOSS-Lizenz oder Entfernen der Copyleft-Komponente

4. Typische FOSS-Lizenzen

Folgende typische FOSS-Lizenzen sind in vielen FOSS-Komponenten enthalten. Die hier angegebenen Steckbriefe geben lediglich einen Überblick über die Lizenzpflichten. Im Detail werden die Lizenzpflichten nach den OSADL License Obligations Checklisten für die tatsächlich im Produkt anwendbaren Lizenzen ermittelt.

- Apache-2.0
  Steckbrief:
  - permissiv
  - Lizenztext mitliefern
  - Modifikationshinweise mitliefern
  - angepasste NOTICE-Datei mit abgeleiteten Werken mitliefern

- BSD-2-Clause
  Steckbrief:
  - permissiv
  - Lizenztext mitliefern
  - Copyright-Vermerke mitliefern

- BSD-3-Clause
  Steckbrief:
  - permissiv
  - Lizenztext mitliefern (oft individualisiert)
  - Copyright-Vermerke mitliefern

- GPL-2.0
  Steckbrief:
  - uneingeschränktes Copyleft
  - Lizenztext mitliefern
  - Copyright-Vermerke mitliefern
  - separaten Haftungsausschluss mitliefern
  - Modifikationshinweise mitliefern
  - Offenlegungspflichten (direkte Mitlieferung oder schriftliches Angebot)
  - Rebuild- und Installationsinformationen

- GPL-3.0
  Steckbrief:
  - uneingeschränktes Copyleft
  - Lizenztext mitliefern
  - Copyright-Vermerke mitliefern
  - Modifikationshinweise mitliefern
  - Offenlegungspflichten (direkte Mitlieferung oder schriftliches Angebot oder Referenzierung)
  - Rebuild- und Installationsinformationen

- LGPL-2.1
  Steckbrief:
  - eingeschränktes Copyleft
  - Lizenztext mitliefern
  - Copyright-Vermerke mitliefern
  - separaten Haftungsausschluss mitliefern
  - Modifikationshinweise mitliefern
  - Offenlegungspflichten (direkte Mitlieferung oder schriftliches Angebot)
  - Rebuild- und Installationsinformationen
  - Neuverlinkbarkeit
  - Bearbeitungserlaubnis, Erlaubnis zum Reengineering verlinkter Komponenten

- LGPL-3.0
  Steckbrief:
  - eingeschränktes Copyleft
  - Lizenztext mitliefern
  - Copyright-Vermerke mitliefern
  - Modifikationshinweise mitliefern
  - Offenlegungspflichten (direkte Mitlieferung oder schriftliches Angebot oder Referenzierung)
  - Rebuild- und Installationsinformationen
  - Neuverlinkbarkeit
  - Bearbeitungserlaubnis, Erlaubnis zum Reengineering verlinkter Komponenten

- MIT
  Steckbrief:
  - permissiv
  - Lizenztext mitliefern
  - Copyright-Vermerke mitliefern

- MPL-2.0
  Steckbrief:
  - eingeschränktes, Datei-basiertes Copyleft
  - Lizenztext mit Quellcode liefern
  - Copyright-Vermerke mit Quellcode liefern
  - Offenlegungspflichten (Referenzierung)

5. Prüfbericht

Im Anschluss an den Compliance Check wird dem Auftraggeber ein Bericht übergeben, der die Ergebnisse der Prüfung zusammenfasst, Mängel auflistet und eine Bewertung dazu enthält, inwieweit die Lizenzpflichten für das geprüfte Produkt berücksichtigt wurden. Weiterhin enthält der Report Hinweise, inwieweit bestehende Unternehmensprozesse zur FOSS-Compliance beigetragen haben und wo möglicherweise Lücken bestehen.

Mit dem Bericht ist keine Bestätigung der Lizenzkonformität verbunden, sondern ein Prüfergebnis, ob und inwieweit die zur Verfügung gestellten Materialien grundsätzlich dazu geeignet sind, einzelne Lizenzbedingungen der anwendbaren FOSS-Lizenzen zu berücksichtigen.

6. Prüfer

Der OSADL Compliance Check wird von entsprechend qualifizierten Mitarbeitern des OSADL durchgeführt. Die Prüfer besitzen ein tiefgehendes Verständnis von Urheberrecht und praktische Erfahrung mit FOSS-Lizenzierung. Für einzelne Teilprüfungen ist die Beauftragung externer Mitarbeiter, die entsprechend qualifiziert sind, möglich. Das Endergebnis wird immer von einem OSADL-Mitarbeiter überprüft. Kein Prüfer verfügt allerdings über eine Zulassung als Rechtsanwalt; insofern handelt es sich beim Ergebnis der Prüfung nicht um eine individuelle Rechtsberatung.