OPENCHAIN

OPENCHAIN Specification

Version 2.0

Vertrauen in Open Source als Quelle für Softwarelösungen schaffen

Inhalte

This is an official translation from the OpenChain Project. It has been translated from the original English text. In the event there is confusion between this translation and the English version, The English text shall take precedence.

Dies ist eine offizielle Übersetzung des OpenChain-Projektes. Sie wurde aus dem englischsprachigen Originaltext übersetzt. Im Falle von Abweichungen zwischen der vorliegenden Übersetzung und der englischsprachigen Version hat der englischsprachige Text Vorrang.

1) Einleitung

Die vorliegende Spezifikation definiert die Schlüsselanforderungen an ein qualitätsgesichertes Open-Source-Lizenz-Compliance-Programm. Sie zielt darauf ab, eine Benchmark bereitzustellen, welche zwischen Organisationen Vertrauen beim Austausch von Open-Source-Software beinhaltenden Softwarelösungen schafft. Die Erfüllung der Spezifikation liefert den Nachweis dafür, dass ein Programm geschaffen wurde, um die erforderlichen Compliance-Artefakte (d.h. Rechtsinhalte, Quellcode, usw.) für jede Softwarelösung zu erzeugen. Die OpenChain-Spezifikation konzentriert sich auf die "Was" und "Warum" -Beschaffenheit eines Programms, anstatt "Wie" und "Wenn" -Überlegungen anzustellen. Dies sichert unterschiedlichen Organisationen mit unterschiedlicher Größe in unterschiedlichen Märkten die Flexibilität, diejenigen Richtlinien und Prozesse auszuwählen, die auf ihre Größe, ihre Ziele und ihren Anwendungsbereich zugeschnitten sind. So kann bspw. ein OpenChain-konformes Programm sich auf ein einzelnes Produkt oder aber die gesamte Organisation beziehen.

Die vorliegende Einführung liefert allen potentiellen Nutzern den Kontext. Abschnitt 2 definiert Schlüsselbegriffe, die in der Spezifikation genutzt werden. Abschnitt 3 bestimmt die Anforderungen, die ein Programm erfüllen muss, um Konformität zu erreichen. Jeder Anforderung ist eine Liste von Verifikationsmaterial (d.h. Nachweisen) zugeordnet, welches vorhanden sein muss, damit eine bestimmte Anforderung als erfüllt angesehen werden kann. Verifikationsmaterial muss nicht veröffentlicht werden, wenngleich eine Organisation sich dazu entschließen kann, dieses Dritten zugänglich zu machen – bspw. nach Abschluss einer Geheimhaltungsvereinbarung (Non-Disclosure Agreement bzw. NDA).

Die Spezifikation wurde in einer offenen Initiative entwickelt, in welche Beiträge von mehr als 150 Mitwirkenden eingeflossen sind. Einen Einblick in die Entwicklungsgeschichte erhalten Sie über die Spezifikations-Mailingliste und in den häufig gestellten Fragen (FAQs).

2) Definitionen

„Compliance-Artefakte“ - Eine Zusammenstellung von Artefakten, die das Ergebnis des Programms für eine Zugelieferte Software darstellt. Die Zusammenstellung kann eines oder mehrere der folgenden Elemente enthalten (ist aber nicht auf diese beschränkt): Quellcode, Benennung des Autors, Urheberrechtshinweise, Kopien der Lizenzbedingungen, Bearbeitungshinweise, schriftliche Angebote, eine Open-Source-Komponenten-Stückliste („Bill of Materials“ bzw. „BoM"), SPDX-Dokumente, etc.

„Identifizierte Lizenzen“ - eine Reihe von Open-Source-Softwarelizenzen, identifiziert als Ergebnis einer geeigneten Methode zur Identifizierung derjenigen Open-Source-Komponenten, aus denen sich eine Zugelieferte Software zusammensetzt.

„OpenChain-konform“ - ein Programm, das alle Anforderungen dieser Spezifikation erfüllt.

„Open Source“ - Software, die einer oder mehreren Lizenzen unterliegt, die den Definitionsanforderungen für Open Source der Open Source Initiative (OpenSource.org), denen für Freie Software (veröffentlicht durch die Free Software Foundation) oder einer ähnlichen Lizenz entsprechen.

„Programm“ - Richtlinien, Prozesse und Mitarbeiter, die die Compliance-Aktivitäten einer Organisation für Open Source-Lizenzen steuern.

„Software-Mitarbeiter“ - jeder Mitarbeiter oder Auftragnehmer einer Organisation, der die Vorgaben für Zugelieferte Software festlegt, zu ihr beiträgt oder für ihre Vorbereitung verantwortlich ist. Abhängig von der jeweiligen Organisation können dies insbesondere (und nicht nur) Software-Entwickler, Release-Ingenieure, Qualitätsprüfer, sowie Mitarbeiter im Produkt-Marketing und im Produkt-Management sein.

„SPDX“ - der von der SPDX (Software Package Data Exchange)-Arbeitsgruppe der Linux Foundation erstellte Format-Standard für den Austausch von Lizenz- und Urheberrechtsinformationen für ein bestimmtes Softwarepaket. Eine Beschreibung der SPDX-Spezifikation finden Sie unter www.spdx.org.

„Zugelieferte Software“ - Software, welche eine Organisation an Dritte weitergibt (z. B. andere Organisationen oder Einzelpersonen).

„Verifikationsmaterial“ - Nachweise, die vorhanden sein müssen, damit eine bestimmte Anforderung als erfüllt angesehen werden kann.

3) Anforderungen

1.0 Programm-Grundlagen

1.1 Richtlinie

Es existiert eine schriftliche Open-Source-Richtlinie, in der die Anforderungen an die Open-Source-Lizenz-Compliance der Zugelieferten Software geregelt ist. Die Richtlinie muss innerhalb der Organisation kommuniziert werden.

Verifikationsmaterial:

- ☐ 1.1.1 Eine schriftlich dokumentierte Open-Source-Richtlinie.
- ☐ 1.1.2 Ein dokumentiertes Verfahren, welches die Software-Mitarbeiter auf die Existenz der Open-Source-Richtlinie aufmerksam macht (z. B. über Schulungen, ein internes Wiki oder eine andere gängige Kommunikationsmethode).

Begründung:
Es soll sichergestellt werden, dass die notwendigen Schritte unternommen wurden, um eine Open-Source-Richtlinie zu erstellen, festzulegen und Software-Mitarbeiter auf deren Existenz hinzuweisen. Obwohl an dieser Stelle keine inhaltlichen Vorgaben an die Open-Source-Richtlinie gestellt werden, können diese durch andere Abschnitte dieser Spezifikation auferlegt werden.

1.2 (Fach-)Kompetenz

Die Organisation muss:

- **Diejenigen Rollen und zugehörigen Verantwortlichkeiten dieser Rollen identifizieren, die die Performanz und Effektivität des Programms beeinflussen;**
- **Den notwendigen Grad an Fachkompetenz der Person(en) bestimmen, welche die jeweilige Rolle bekleiden;**
- **Sicherstellen, dass diese Personen auf Basis einschlägiger Ausbildung, Schulung und/oder Erfahrung die notwendige Fachkompetenz besitzen;**
- **Falls notwendig: Maßnahmen ergreifen, dass die hinreichende Fachkompetenz erworben wird; und**
- **Eine hinreichende Dokumentation als Beleg der Fachkompetenz aufrechterhalten.**

Verifikationsmaterial:

- ☐ 1.2.1 Eine dokumentierte Liste an Rollen inklusive zugehöriger Verantwortlichkeiten für die unterschiedlichen Programmteilnehmer.
- ☐ 1.2.2 Ein Dokument, welches die Kompetenzanforderungen an die jeweiligen Rollen festlegt.
- ☐ 1.2.3 Dokumentierte Nachweise der bei jedem Programm-Teilnehmer ermittelten Fachkompetenz.

Begründung:
Es soll sichergestellt werden, dass diejenigen Teilnehmer, welche Rollen im Programm ausführen, einen der jeweiligen Rolle und Verantwortlichkeit angemessenen Grad an Fachkompetenz erreicht haben.

1.3 Bekanntheit ("Awareness")

Die Organisation muss sicherstellen, dass Programm-Teilnehmern

a) die Open-Source-Richtlinie;
b) relevante Open-Source-Ziele;
c) ihr jeweiliger Beitrag zur Effektivität des Open-Source-Compliance-Programms; und
d) die Auswirkungen einer Nichterfüllung der Programm-Anforderungen

bekannt sind.

Verifikationsmaterial:

☐ 1.3.1 Dokumentierte Nachweise des bei jedem Programm-Teilnehmer ermittelten Bekanntheitsgrades in Bezug auf die Programmziele, ihren jeweiligen Beitrag zum Programm und der Auswirkungen einer Nichtkonformität gegenüber dem Programm.

Begründung:

Es soll sichergestellt werden, dass den Teilnehmern ihre jeweiligen Rollen und Verantwortlichkeiten innerhalb des Programms in hinreichendem Maße bekannt sind.

1.4 Programmumfang

Für unterschiedliche Programme gelten möglicherweise unterschiedliche Definitionen zu deren Umfang. Beispielsweise könnte ein Programm sich auf eine einzelne Produktlinie, einen Organisationsbereich oder eine gesamte Organisation beziehen. Für jedes Programm muss der Umfang festgelegt werden.

Verifikationsmaterial:

☐ 1.4.1 Eine schriftliche Erklärung, welche Umfang und Grenzen des Programms klar definiert.

Begründung:

Es soll sichergestellt werden, dass die Flexibilität besteht, ein Programm aufzusetzen, welches den Anforderungen einer Organisation am besten entspricht. Einige Organisationen könnten ein Programm für eine bestimmte Produktlinie unterhalten, während andere ein Programm zur Steuerung der Zugelieferten Software der gesamten Organisation einrichten könnten.

1.5 Lizenzverpflichtungen

Es besteht ein Verfahren zur Überprüfung der Identifizierten Lizenzen um jeweils gewährte Rechte bzw. auferlegte Einschränkungen und Verpflichtungen zu bestimmen.

Verifikationsmaterial:

☐ 1.5.1 Ein dokumentiertes Verfahren zur Überprüfung und Dokumentation der durch die jeweiligen Identifizierten Lizenzen gewährten Rechte bzw. auferlegten Beschränkungen und Verpflichtungen.

Begründung:

Es soll sichergestellt werden, dass ein Prozess besteht, in dem die Lizenzpflichten für die verschiedenen, im Kontext der Organisation möglichen, Anwendungsfälle geprüft und identifiziert werden (wie in Anforderung 3.2 definiert).

2.0 Definition und Unterstützung relevanter Aufgaben

2.1 Zugang

Erstellung und Aufrechterhaltung eines Prozesses, um auf Open-Source-Anfragen von außerhalb der Organisation wirkungsvoll zu reagieren. Veröffentlichung einer Schnittstelle, über die Dritte Open-Source-Compliance-Anfragen absetzen können.

Verifikationsmaterial:

- ☐ 2.1.1 Eine öffentlich sichtbare Bekanntgabe einer Schnittstelle, über welche Dritte eine Open-Source-Compliance-Anfrage stellen können (*z. B.* durch Veröffentlichen einer Kontakt-E-Mail-Adresse oder Aufnahme in das Open Compliance-Verzeichnis der Linux Foundation).
- ☐ 2.1.2 Ein intern dokumentiertes Verfahren für die Bearbeitung von Open-Source-Lizenz-Compliance-Anfragen von Dritten.

Begründung:
Es soll sichergestellt werden, dass Dritte eine angemessene Möglichkeit besitzen, sich mit der Organisation in Bezug auf Open-Source-Compliance-Anfragen in Verbindung zu setzen – sowie dass die Organisation in der Lage ist, wirkungsvoll auf dieselben zu reagieren.

2.2 Effektive Ausstattung

Identifikation der Programm-Aufgabe(n) und Ausstattung derselben mit den notwendigen Ressourcen:

- **Zuweisen der Verantwortlichkeiten für die erfolgreiche Bearbeitung von Programm-Aufgaben.**
- **Programm-Aufgaben verfügen über ausreichende Ressourcen:**
  - **für die Ausführung der Aufgaben wurde ausreichend Zeit zur Verfügung gestellt; und**
  - **es wurde ein angemessenes finanzielles Budget zugewiesen.**
- **Es existiert ein Prozess für die Überprüfung und Aktualisierung der Richtlinie sowie für hierbei unterstützende Aufgaben;**
- **Juristische Expertise in Bezug auf Open-Source-Compliance ist vorhanden und für diejenigen Personen verfügbar, welche hierzu eventuell Unterstützung benötigen; und**
- **es existiert ein Prozess für die Lösung von Open-Source-Lizenz-Compliance-Problemen.**

Verifikationsmaterial:

- ☐ 2.2.1 Ein Dokument mit den Personennamen, Gruppenzugehörigkeiten oder Funktionen, denen Programm-Rolle(n) zugeordnet sind.
- ☐ 2.2.2 Die identifizierten Rollen im Programm sind mit ausreichenden personellen und finanziellen Ressourcen ausgestattet.
- ☐ 2.2.3 Benennung der juristischen Expertise, die sowohl intern als auch extern zur Adressierung von Open-Source-Compliance-Themen zur Verfügung steht.
- ☐ 2.2.4 Ein dokumentiertes Verfahren, das interne Verantwortlichkeiten für die Open-Source-Compliance zuweist.
- ☐ 2.2.5 Ein dokumentiertes Verfahren zur Prüfung und Behebung von Fällen der Nichterfüllung von Open-Source-Compliance-Anforderungen.

Begründung:
Es soll sichergestellt sein, dass i) Programm-Verantwortlichkeiten tatsächlich unterstützt und mit ausreichenden Ressourcen ausgestattet sind und ii) Richtlinien und unterstützende Prozesse regelmäßig aktualisiert werden, um Änderungen in den Best Practices für Open Source-Compliance zu berücksichtigen.

3.0 Überprüfung und Genehmigung von Open-Source-Inhalten

3.1 Komponentenstückliste / Bill of Materials

Es existiert ein Prozess zum Erstellen und Verwalten einer Bill of Materials, die jede Open-Source-Komponente (und ihre Identifizierten Lizenzen) enthält, aus der sich die Zugelieferte Software zusammensetzt.

Verifikationsmaterial:

- ☐ 3.1.1 Ein dokumentiertes Verfahren zur Identifizierung, Nachverfolgung, Prüfung, Freigabe und Archivierung von Informationen über die Gesamtheit der Open-Source-Komponenten, aus denen eine Version Zugelieferter Software besteht.
- ☐ 3.1.2 Eine Aufzeichnung der Open-Source-Komponenten von Zugelieferter Software, welche nachweist, dass das dokumentierte Verfahren ordnungsgemäß befolgt wurde.

Begründung:
Es soll sichergestellt werden, dass ein Prozess zum Erstellen und Verwalten einer Bill of Materials der Open-Source-Komponenten existiert, aus welchen die Zugelieferte Software besteht. Die Bill of Materials ist erforderlich, um systematisch die Lizenzbedingungen jeder Komponente zu überprüfen und freizugeben, um die Lizenzpflichten und -bedingungen im Hinblick auf die Verbreitung der Zugelieferten Software zu ermitteln.

3.2 Lizenz-Compliance

Das Programm muss es ermöglichen, die üblichen Anwendungsfälle von Open-Source-Lizenzen abzudecken, mit denen Software-Mitarbeiter im Kontext Zugelieferter Software konfrontiert sind. Zu den üblichen Fällen zählen dabei insbesondere (beachten Sie allerdings, dass die Liste weder abschließend ist, noch alle Anwendungsfälle Anwendung finden müssen):

- **Verbreitung in Binärform;**
- **Verbreitung in Sourcecode-Form;**
- **Integration mit anderer Open-Source-Software, so dass die Voraussetzungen des Copyleft vorliegen können;**
- **Enthält bearbeitete Open-Source-Software;**
- **Enthält Open-Source-Software oder andere Software unter einer inkompatiblen Lizenz, die mit anderen Komponenten innerhalb der Zugelieferten Software interagiert; und / oder**
- **Enthält Open-Source-Software mit Verpflichtungen hinsichtlich einer Nennung der Urheberschaft.**

Verifikationsmaterial:

- ☐ 3.2.1 Ein dokumentiertes Verfahren, welches es ermöglicht, die üblichen Anwendungsfälle von Open-Source-Lizenzen für die Open-Source-Komponenten von Zugelieferter Software abzudecken.

Begründung:
Es soll sichergestellt werden, dass das Programm ausreichend robust ist, um die üblichen Anwendungsfälle von Open-Source-Lizenzen einer Organisation zu bedienen. Es muss gewährleistet sein, dass ein Verfahren zur Unterstützung dieser Tätigkeit besteht und dass das Verfahren befolgt wird.

4.0 Erzeugung und Bereitstellung von Compliance-Artefakten

4.1 Compliance-Artefakte

Es existiert ein Prozess, um für die Zugelieferte Software die Compliance-Artefakte zusammenzustellen.

Verifikationsmaterial:

- ☐ 4.1.1 Ein dokumentiertes Verfahren, welches sicherstellt, dass die Compliance-Artefakte entsprechend der Anforderungen der Identifizierten Lizenzen zusammengestellt und zusammen mit der Zugelieferten Software weitergegeben werden.

- ☐ 4.1.2 Ein dokumentiertes Verfahren, um Kopien der Compliance-Artefakte der Zugelieferten Software zu archivieren – wobei geplant sein muss, dass das Archiv einen ausreichenden Zeitraum[1] über das letzte Angebotsdatum einer Zugelieferten Software hinaus aufrechterhalten wird bzw. mindestens so lange, wie es die Identifizierten Lizenzen verlangen (je nachdem, welcher Zeitraum länger ist). Es existieren Aufzeichnungen als Beleg, dass das Verfahren ordnungsgemäß befolgt wird.

Begründung:
Es soll sichergestellt werden, dass angemessene Anstrengungen unternommen werden, um die der Zugelieferten Software beizufügenden Compliance-Artefakte derart zu erstellen, wie durch die Identifizierten Lizenzen gefordert.

[1] Abhängig von Domäne, Rechtsordnung und/oder Kundenverträgen

5.0 Verstehen des Engagements gegenüber der Open Source Community

5.1 Beiträge

Wenn eine Organisation Beiträge zu Open-Source-Projekten erlaubt,

- **muss eine schriftliche Richtlinie zur Regelung der Beiträge zu Open-Source-Projekten existieren;**
- **muss diese Richtlinie intern kommuniziert werden; und es**
- **muss ein Prozess existieren, der diese Richtlinie umsetzt.**

Verifikationsmaterial:

Wenn eine Organisation Beiträge zu Open-Source-Projekten erlaubt, muss Folgendes existieren:

- ☐ 5.1.1 Eine dokumentierte Richtlinie für Beiträge zu Open Source;
- ☐ 5.1.2 ein dokumentiertes Verfahren, welches Beiträge zu Open Source regelt; und
- ☐ 5.1.3 ein dokumentiertes Verfahren, welches alle Software-Mitarbeiter auf die Existenz der Richtlinie für Beiträge zu Open Source aufmerksam macht (z. B. über Schulung, internes Wiki oder eine andere gängige Kommunikationsmethode).

Begründung:

Wenn eine Organisation Beiträge zu Open-Source-Projekten erlaubt, soll sichergestellt werden, dass die Organisation der Entwicklung und Umsetzung einer Richtlinie für Beiträge ausreichende Beachtung geschenkt hat. Die Richtlinie für Beiträge zu Open Source kann Teil einer übergreifenden Open-Source-Richtlinie oder eine eigene separate Richtlinie sein.

6.0 Erfüllung der OpenChain-Anforderungen

6.1 Konformität

Damit einer Organisation ein OpenChain-konformes Programm bescheinigt werden kann, muss diese bestätigen, dass ihr Programm die in der vorliegenden OpenChain-Spezifikation beschriebenen Kriterien erfüllt.

Verifikationsmaterial:

- ☐ 6.1.1 Ein Dokument, welches bestätigt, dass das gemäß Anforderung 1.4 definierte Programm alle Anforderungen der vorliegenden Spezifikation erfüllt.

Begründung:
Es soll sichergestellt werden, dass ein Programm alle Anforderungen dieser Spezifikation erfüllt, wenn eine Organisation angibt, dass ihr Programm OpenChain-konform sei. Ein Erfüllen nur einzelner Anforderungen würde hierzu als nicht ausreichend erachtet.

6.2 Gültigkeitsdauer

Die Bescheinigung eines gemäß der vorliegenden Spezifikation OpenChain-konformen Programms ist ab dem Datum, zu welchem die Konformitätsprüfung bestätigt wurde, für 18 Monate gültig. Das Verfahren zur Registrierung einer Konformitätsprüfung finden Sie auf der Website des OpenChain-Projekts.

Verifikationsmaterial:

- ☐ 6.2.1 Ein Dokument, welches bestätigt, dass das Programm alle Anforderungen der vorliegenden Spezifikation (Version 2.0) während der vergangenen 18 Monate seit Bestätigung der Konformitätsprüfung erfüllt hat.

Begründung:
Es ist für eine Organisation wichtig, auf einem aktuellen Stand bezüglich der Spezifikation zu bleiben, wenn sie ihre Programmkonformität auf Dauer behaupten will. Diese Anforderung stellt sicher, dass die die Konformität unterstützenden Prozesse und Kontrollen des Programms nicht abgeschwächt werden, wenn eine Organisation die Programmkonformität über den angegebenen Zeitraum hinaus geltend machen will.

Anhang I: Sprachübersetzungen

Um die weltweite Akzeptanz zu fördern, begrüßen wir Bemühungen, die Spezifikation in mehrere Sprachen zu übersetzen. Da auch die OpenChain Initiative als Open-Source-Projekt aufgesetzt ist, werden Übersetzungen durch diejenigen gesteuert, die bereit sind, ihre Zeit und ihr Fachwissen zu Übersetzungen unter den Bedingungen der CC-BY 4.0-Lizenz und den Übersetzungs-Richtlinien des Projekts beizutragen. Die Details der Richtlinien sowie verfügbare Übersetzungen finden Sie auf der Spezifikations-Webseite des OpenChain-Projekts.