

Open Source Licensing

Rechtssicherheit in der Softwareentwicklung gewährleisten

Betriebliche Informationssysteme verbauen zahlreiche Open Source-Komponenten. Für Anbieter und Anwender verlässliche Open Source-Lizenzen regeln die Nutzung. Die Wahl der passenden Lizenz ist dennoch kompliziert.

Definition

Open Source Licensing bedeutet, kreative Inhalte unter einer gültigen Open Source-Lizenz zu veröffentlichen. Diese erlaubt mit einem nicht exklusiven und nicht diskriminierenden Vertrag die freie Nutzung, Modifikation und Verbreitung.

Anbieter stellen Komponenten unter einer Open Source-Lizenz zur Verfügung. Hierfür wählen sie eine passende Open Source-Lizenz aus. Die Auswahl hängt davon ab, welche Verpflichtungen Anbieter den Anwendern auferlegen möchten.

Anwender prüfen die Verpflichtungen. Sie sind bereit und in der Lage alle Ver-

pflichtungen einer Lizenz zu erfüllen, dürfen sie die Komponente unter der Lizenz verwenden. Dies geschieht unabhängig von der Anzahl an Verpflichtungen. Kann die Anwender nur einen Teil der Verpflichtungen erfüllen, schließt dies die Nutzung aus.

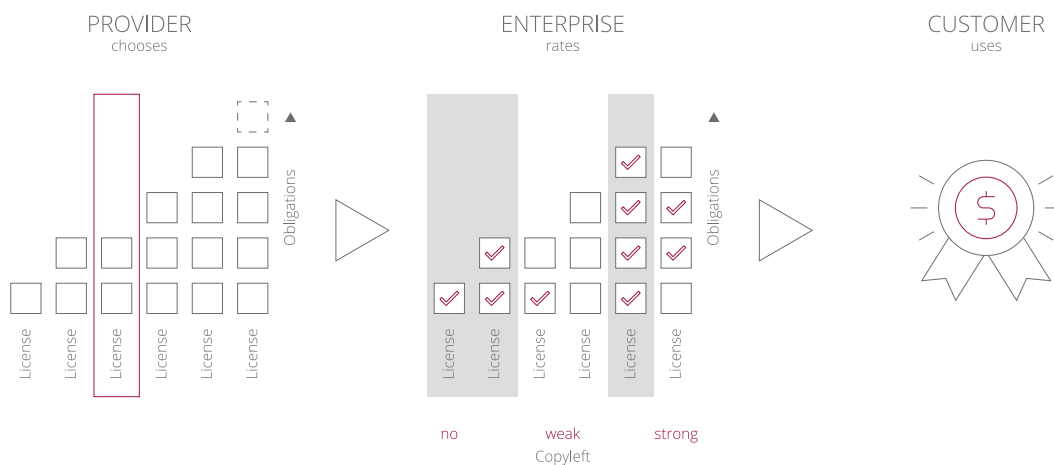
Referenzszenario

Ein Unternehmen implementiert ein betriebliches Informationssystem. Der IT-Architekt sammelt und vergleicht mehrere Komponenten, welche die fachlichen und technischen Anforderungen erfüllen. Zudem prüft er die Lizenz, weil jede unterschiedliche Verpflichtungen bedeutet. Einige können entfallen, wenn

sie nur für eine bestimmte Art der Nutzung gelten. Kann oder will der Architekt eine Verpflichtung nicht erfüllen, so ist das ein Ausschlusskriterium. Abschließend achtet er darauf, die Verpflichtungen einzuhalten, etwa den Lizenztext mit dem Softwareprodukt auszuliefern.

Potenzial

Open Source Licensing reduziert den Aufwand, Softwarelizenzen zu prüfen und ermöglicht tausende Komponenten in einem kleinen Projekt zu verbauen. Entwickler können die Lizenzen eigenständig - oft ohne Anwalt - prüfen. Zudem vereinfacht Open Source Licensing die Bereitstellung von Komponenten



Recht

- Standardlizenzen
- Gerichtsurteile
- Anwälte
- Einhaltung / Compliance
- inter-/nationales Recht

Stiftungen

- Apache Software Foundation
- Eclipse Foundation
- Linux Foundation
- Mozilla Foundation
- CNCF

OSL

Organisationen

- Open Source Initiative (OSI)
- Software Package Exchange (SPDX)
- Creative Commons

Plattformen

- GitHub
- npm, Docker Hub, PyPI
- Kaggle
- Wikipedia

ten, weil vielfältige Lizenzen aus einem breiten Katalog wählbar sind. Die individuelle Lizenzarbeit kann entfallen.

Reifegrad

Bewährte Open Source-Lizenzen sind über 40 Jahre alt. Einige Initiativen versuchen, Lizenzen für die Anwender weiter zu vereinfachen und verständlicher zu formulieren, etwa die Creative Commons Organisation. Die Open Source Initiative zertifiziert seit 25 Jahren Lizenzen anhand der eigenen Open Source-Definition. Die AGPL war ein erster Versuch, um einen starken Copyleft-Effekt bei Application Service Providern durchzusetzen. Viele Projekte versuchen diese Lücke durch eigene Lizenzen zu schließen unter zertifizieren sie bei der Open Source Initiative, etwa die Elastic License 2.0.

Die Linux Foundation hat das Software Package Data Exchange (SPDX) etabliert.

Es ermöglicht eine effiziente und zuverlässige Identifizierung von Lizenzen.

Marktübersicht

Die Open Source Initiative erkennt über 125 Lizenzen an. Die bekanntesten sind: MIT-Lizenz (MIT), ursprüngliche BSD-Lizenz (BSD-4-Clause), Apache License 2.0 (Apache-2.0), Mozilla Public License 2.0 (MPL-2.0), GNU General Public License v3.0 (GPL-3.0) und GNU Affero General Public License v3.0 (AGPL-3.0-only). Seltenere ist die von der Europäischen Union in 22 Sprachen erarbeitete European Union Public License 1.2 (EUPL-1.2).

Die Sicherstellung der Verpflichtungen unterstützen zahlreiche Tools. FOSSA durchsucht etwa Textdateien aller verbauten Abhängigkeiten nach Lizenztexten und listet diese auf. Andere versuchen über den Package Manager der jeweiligen Programmiersprache an die

Lizenzinformationen zu gelangen.

tl;drLegal stellt eine Zusammenfassung aller Lizenzen zur Verfügung.

Alternativen

Eine Alternative sind bewährte Lizenzen, welche die Open Source Initiative nicht anerkennt, etwa die Server Side Public License (SSPL), die Application Service Provider benachteiligt. Einige Projekte verzichten auf eine Open Source-Lizenz und stellen alles gemeinfrei (Public Domain) zur Verfügung. Andere definieren einen individuellen Vertrag.

Auch Kombinationen sind möglich. Während die Basisfunktionalität unter einer Open Source-Lizenz steht, ist die Nutzung weiterer Features kostenpflichtig. So kommt es zur doppelten Lizenzierung (Dual Licensing), die Anwendern zwei oder mehrere Softwarelizenzen zur Auswahl stellt.

Fazit

- + rechtssichere Standardlizenzen
- + verlässliche Gerichtsurteile
- + niedrige Einstiegshürde
- + vertrauenswürdige Lizenzen
- + Englisch
- Begriffe auf US-Recht ausgelegt
- komplex bei vielen Abhängigkeiten und Lizenzen
- ausgenutzte Lizenzlücken



Buzzword Factor (Ent./Customer)

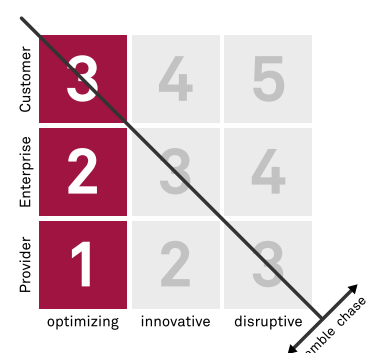
| | | |
|----------|-------------|-----------|
| 1 low | 2 medium | 3 high |
|----------|-------------|-----------|

Entry Barrier (Provider)

| | | |
|----------|-------------|-----------|
| 1 low | 2 medium | 3 high |
|----------|-------------|-----------|

Benefit Level (Provider)

| | | |
|----------|-------------|-----------|
| 1 low | 2 medium | 3 high |
|----------|-------------|-----------|



<https://msg.direct/techrefresh>

Stand: Oktober 2022

msg systems ag

Robert-Bürkle-Straße 1 | 85737 Ismaning/München | Telefon: +49 89 96101-0 | Fax: +49 89 96101-1113 | www.msg.group | info@msg.group