Rechtsfragen der Open-Source-Compliance

Herangereift

Tobias Haar

Wer Open-Source-Komponenten nutzt und weitergibt, muss die rechtlichen Rahmenbedingungen einhalten – sonst drohen empfindliche Konsequenzen. Ein Blick auf die Complianceansätze.

Der Einsatz von unter Open-Source-Lizenzen stehender Software ist weit verbreitet. Rechtlich handelt es sich dabei um ein spannendes, aber auch komplexes Thema mit zahlreichen Verästelungen. Auch für Open-Source-Komponenten (OSK) sind geltende Gesetze anzuwenden – in erster Linie das Urheberrecht. Ob Geld für die Nutzung urheberrechtlich geschützter Werke zu zahlen ist, spielt aus juristischer Sicht kaum eine Rolle.

Vor etwa zwanzig Jahren rückten OSK in den Blickpunkt von Juristen, für die zahlreiche Aspekte zunächst schlecht greifbar waren. In Deutschland klärte sich eine zentrale Rechtsfrage mit dem Urteil des Landgerichts München I vom Mai 2004. Seine Kernaussage lautet: Ein Verstoß gegen eine Open-Source-Lizenz verletzt das Urheberrecht. Daher können OSK-Nutzer in ähnlicher Weise in die juristische Verantwortung genommen werden wie bei proprietärer Software. Gegenstand des Gerichtsverfahrens in München war die Software netfilter/iptables. Geklagt hatte ein Hauptverantwortlicher für das Softwareprojekt.

Besonders spannend und juristisch relevant war damals, dass diese Software unter der GNU GPLv2 stand, also einer Copyleft-Lizenz. Jede Weiterentwicklung war somit ebenfalls unter dieser Lizenz zu verbreiten. Außerdem verlangt die GPL die Mitlieferung des GPL-Lizenztextes, einen Copyrightvermerk mit Hinweis auf die Urheber der OSK, einen vorgegebenen Haftungsausschluss sowie Zugang zum vollständigen Quelltext bei Auslieferung von kompiliertem Code.

Die Erkenntnis aus dem Urteil von 2004: Da die GPL nach deutschem Recht wirksame Grundlage der Nutzung entsprechend lizenzierter OSK sein kann, haben GPL-Verletzungen urheberrechtliche Konsequenzen – insbesondere erlischt das Nutzungsrecht, und zwar automatisch und ohne dass es einer Handlung der OSK-Entwickler bedarf. Dieser juristische Grundsatz dürfte auch für OS-Lizenzen gelten, die noch nicht Gegenstand von Gerichtsentscheidungen waren.

Verstöße kosten Zeit und Geld

Bei Verstößen drohen Unterlassungsansprüche der Urheber, etwa in Gestalt von Abmahnungen oder einstweiligen Verfügungen. Das alles kostet Geld und Zeit. Oftmals müssen Sachverständige hinzugezogen werden. Dazu muss der Quellcode zugänglich sein, was wiederum mit gerichtlicher Hilfe mittels des Softwarebesichtigungsanspruchs durchgesetzt werden kann (siehe iX 2/2009, S. 114).

Steht eine Urheberrechtsverletzung fest, kann der Urheber eine Vernichtung von Produkten verlangen, die die nicht lizenzierte OSK enthalten. In ähnlicher Weise sieht § 98 des Urheberrechtsgesetzes einen Rückruf und „deren endgültiges Entfernen aus den Vertriebswegen“ vor. Unter Umständen kann der Rechteinhaber die Herausgabe der Produkte gegen eine angemessene Vergütung verlangen. Auch wenn die Verhältnismäßigkeit gewahrt bleiben muss, können solche Maßnahmen erhebliche Konsequenzen haben. Theoretisch reicht es bereits aus, wenn in einem Nutzerhandbuch für ein elektronisches Gerät mit GPL-Code die GPL nicht abgedruckt ist.

In der Praxis wird meist ein Auskunftsanspruch geltend gemacht. Dieses Recht ist gerichtet „auf unverzügliche Auskunft über die Herkunft und den Vertriebsweg der rechtsverletzenden Vervielfältigungsstücke oder sonstigen Erzeugnisse“. Das Urheberrechtsgesetz beschreibt weitere Details der Auskunftspflicht. Dies ist für den Rechtsverletzer zumindest lästig, kann aber die Grundlage bilden für weiter gehende Ansprüche des Rechteinhabers und damit eine juristische Eskalation.

Die beschriebenen Grundsätze sind wesentlich für die OS-Compliance, auch OS License Management oder OS Governance genannt. In Unternehmen handelt es sich um eine Schnittstellenaufgabe: Zum einen stehen rechtliche Fragen im Raum, was die Zuständigkeit der Juristen und – soweit vorhanden – von Complianceabeauftragten begründet. Zum anderen sind die Fachbereiche in Forschung, Entwicklung, Produktion, Marketing et cetera einzubinden, da sie die OS-Lizenzen kennen und im Produkt- oder Dienstleistungszyklus berücksichtigen müssen.

Eine OS-Compliance steht und fällt mit dem Wissen um den Einsatz von OSK in einem Unternehmen. Dabei spielt es zunächst keine Rolle, ob solche Kompo-

nenten in intern genutzten Systemen, in Produkten oder bei Dienstleistungen eingesetzt werden. Aus juristischer Sicht ist es unerheblich, ob eine Bestandsaufnahme internen Abteilungen obliegt – etwa einem OS-Compliance-Manager – oder externen Dienstleistern. Wichtig ist das Verständnis, dass es sich hierbei meist nicht um einen einmaligen Vorgang handelt.

Eine solche Review ist stets nur eine Momentaufnahme und ersetzt keinen dauerhaften Complianceprozess. Dazu zählt die interne Aufklärung über rechtliche Herausforderungen der Nutzung von OSK. Je nach dem konkreten Einsatz von OSK in einem Unternehmen müssen Entwickler, Produktdesigner et cetera einen Prozess befolgen, der Dokumentation und Umgang mit Risiken der OSK-Nutzung angemessen beschreibt. Eigene Lieferanten sind hier einzubinden, weil ein Unternehmen auch für Lizenzverletzungen einstehen muss, die auf zugelieferte Komponenten zurückgehen.

Ob Regressansprüche gegen den Lieferanten oder externen Entwickler bestehen, ist eine nachgelagerte Frage. Hilfreich ist es oft, externen Entwicklern die Nutzung von OSK grundsätzlich vertraglich zu verbieten und sie nur nach einem genauen Prozess im Einzelfall zu erlauben. Dies ermöglicht zumindest dem Auftraggeber, OSK zu dokumentieren. Bei einer Insolvenz des externen Dienstleisters liegen dann wenigstens Informationen über den OSK-Einsatz vor, die für juristische Diskussionen entscheidend sein können.

Zum Einhalten der Compliance werden mitunter ein OS Review Board und Playbooks für den idealerweise standardisierten Umgang mit üblicherweise verwendeten OS-Lizenzmodellen empfohlen. Hierzu zählen neben der GPL (Version 2 und 3 sowie den verwandten Lesser GPL für Bibliotheken) die MIT-, die Apache-2.0- und die BSD-Lizenz. Zumindest teilweise lassen sich die Aufgaben der OS-Compliance automatisieren.

Eine OS-Review findet mitunter auch im Rahmen von Fusionen oder Übernahmen oder für Zertifizierungen auf Wunsch der Kunden statt. Es gilt dabei, rechtliche Risiken bereits im Voraus zu erkennen und möglichst auszuschließen. Hier können auch Compliancezertifizierungen helfen, wie zahlreiche Dienstleister sie anbieten. Eine Selbstzertifizierung etwa gemäß OpenChain Self Certification genügt meist jedoch nicht.

Der Vergleichbarkeit von OS-Audits dient ein ISO-Standard mit der Bezeichnung ISO/IEC 5230:2020 – Information Technology – OpenChain Specification. Laut der International Organization for Standardization beschreibt der Standard die wichtigsten Anforderungen zur Einhaltung von Open-Source-Lizenzen. Er soll das Vertrauen zwischen Organisationen stärken, die Open-Source-Software austauschen.

Standardformat erleichtert die Compliance

Eine Zertifizierung nach diesem Standard durch externe Dritte dürfte bei Unternehmenskäufen oder höherwertigen Produkten und Dienstleistungen einen Vermarktungsvorteil bieten. 2021 wurde Software Package Data Exchange (SPDX) als ISO/IEC-Standard 5962:2021 zertifiziert. Das Format dient der standardisierten Einführung von Prozessen, die Informationen zu Herkunft, Lizenzbedingungen, IT-Sicherheit et cetera von Software erfassen sollen.

Laut den Initiatoren soll SPDX „redundante Arbeit reduzieren, indem es gemeinsame Formate für Organisationen und Gemeinschaften zum Austausch wichtiger Daten bereitstellt“. Zuständig ist die Linux Foundation. Die Webseiten auf spdx.org bieten Informationen, die im Rahmen der OS-Compliance relevant sind und diese unterstützen können.

Die SPDX License List führt eine Vielzahl weitverbreiteter OS-Lizenzmodelle auf und verlinkt auf die jeweiligen Lizenzbedingungen. Mittels der SPDX IDs kann Software entsprechend der ihr zugrunde liegenden Lizenz markiert werden. Die IDs sind menschen- und maschinenlesbar.

Mithilfe der SPDX Documents können Lizenzinformationen für einzelne oder gebündelte OS-Dateien beschrieben werden. Das Sicherstellen der OS-Compliance soll sich durch die strukturierte Form der relevanten Informationen vereinfachen. Als Formate kommen Tag/Value (.spdx), JSON (.spdx.json), YAML (.spdx.yml), RDF/xml (spdx.rdf) und Excel-Spreadsheets (.xls) in Betracht. Auf den SPDX-Webseiten finden sich umfangreiche Erläuterungen über Einführung und Nutzung von SPDX Documents.

Lizenzauswahl für Eigenentwicklungen

Auch bei eigenen Softwareentwicklungen spielt die OS-Compliance zumindest indirekt eine Rolle: Jeder Entwickler muss sich die Frage stellen, ob er seine Entwicklung nur selbst oder auch durch Dritte nutzen lassen möchte. Hier helfen Tools wie choosealicense.com, die für einen Einzelfall passende Lizenz zu finden. Im Zweifel kann dies die Beratung durch die Rechtsabteilung oder einen auf IT-Recht spezialisierten Rechtsanwalt aber nicht ersetzen. Es ist nicht zwingend notwendig, bestehende OS-Lizenzmodelle für eigene Entwicklungen zu verwenden. Ein Urheber kann grundsätzlich bestimmen, wer seine urheberrechtlich geschützten Werke nutzen kann. Dann kann er aber auch bestimmen, welche Lizenz gelten soll – eine bereits bestehende oder eine eigene. Die Formulierung maßgeschneiderter Lizenzbedingungen bedarf aber der Zusammenarbeit zwischen Entwicklern und spezialisierten Juristen.

Außer für Softwarekomponenten gibt es OS-Lizenzmodelle für Daten und kreative Inhalte, etwa die Creative-Commons-Lizenzfamilie. Ein Exot ist die SIL Open Font License 1.1 für Schriften. Ähnlich dem Copyleft-Ansatz gibt es im Bereich der Erfindungen das Patentleft-Konzept – und so weiter. Die beschriebenen Rechtsgrundsätze sind für alle gleich. Die Anforderungen an OS-Compliance sind im Detail an die besonderen Umstände des Einzelfalls anzupassen.

Fazit

Die Einhaltung von Open-Source-Lizenzbedingungen ist für die meisten Unternehmen, Behörden und öffentlichen Stellen von hoher Relevanz. Nur so können juristische Konsequenzen vermieden werden, die mindestens Zeit und Geld kosten – von etwaigen Rufschädigungen etwa bei Produktrückrufen ganz zu schweigen.

Die Empfehlungen und Standards für Compliance haben sich in den letzten Jahren weiterentwickelt. Ein Beispiel ist das jüngst zum ISO-Standard erhobene Projekt Software Package Data Exchange (SPDX) der Linux Foundation. Geschäfts- und Behördenleitungen sowie die Verantwortlichen für die Einhaltung von Lizenzbedingungen müssen auch bei OS-Compliance den Stand der Technik berücksichtigen. Andernfalls drohen ihnen juristische Konsequenzen bis hin zu Schadenersatzforderungen oder Verlust des Arbeitsplatzes. (un@ix.de)

Tobias Haar, Rechtsanwalt, LL.M. (Rechtsinformatik), MBA,

ist Rechtsanwalt mit Schwerpunkt IT-Recht bei Vogel & Partner in Karlsruhe.