Open Source Compliance bei Embedded Systems

Dr. Hendrik Schöttle

20. September 2023

Warum Compliance?

- Die unerlaubte Verwertung urheberrechtlich geschützter Werke ist nach §§ 106, 108a UrhG strafbar!
- Verbreitung von OSS bei Verletzung der OSS-Lizenzpflichten kann zu Unterlassungsansprüchen und zu Schadensersatz führen
- Einzelne Mitentwickler von systemnahen Linux-Komponenten bzw. Komponenten des Linux-Kernels greifen immer wieder Verletzungen bei diesen Softwareprodukten aus kommerziellen Gründen an
- Auch Organisationen überwachen die Einhaltung von OSS-Lizenzbedingungen, wie etwa die Software Freedom Conservancy
- Unternehmen verwenden OSS-Lizenzen, um kommerzielle, kostenpflichtige Lizenzen im Wege des Dual Licensing durchzusetzen

Warum Compliance?

- **Ziff. 4. S. 2 GPL-2.0**

  You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License.

- **§ 106 UrhG – Unerlaubte Verwertung urheberrechtlich geschützter Werke**

  (1) Wer in anderen als den gesetzlich zugelassenen Fällen ohne Einwilligung des Berechtigten ein Werk oder eine Bearbeitung oder Umgestaltung eines Werkes vervielfältigt, verbreitet oder öffentlich wiedergibt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

  (2) Der Versuch ist strafbar.

- **§ 108a UrhG – Gewerbsmäßige unerlaubte Verwertung**

  (1) Handelt der Täter in den Fällen der §§ 106 bis 108 gewerbsmäßig, so ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

Warum Compliance?

- Beim Verstoß gegen Lizenzpflichten der GPL-2.0 erlöschen sämtliche Rechte unter der Lizenz
- Folge: kein Verbreitungsrecht mehr
- Strafbarkeit wegen Verwertung urheberrechtlich geschützter Werke möglich
- Bei Gewerbsmäßigkeit Freiheitsstrafe von bis zu fünf Jahren möglich, §§ 106 Abs. 1 i.V.m. 108a Abs. 1 UrhG

GEGEN COMMUNITY-RICHTLINIEN

Entwickler soll sich an GPL-Durchsetzung bereichert haben

Möglicherweise hat sich ein Linux-Entwickler mit Hilfe der GPL und Schadenersatzansprüchen finanziell bereichert. Dieses Vorgehen entspreche aber nicht den Community-Richtlinien der FSF und der SFC und wirft grundsätzliche Fragen auf.

22. Juli 2016, 13:41 Uhr, Sebastian Grüner

{* OSES *}

Linux kernel community tries to castrate GPL copyright troll

Greg Kroah-Hartman issues 'enforcement statement' after chap wins 'a few million Euros' with questionable claims

Simon Sharwood

Wed 18 Oct 2017 // 01:16 UTC

Linux kernel maintainer Greg Kroah-Hartman and several other senior Linux figures have published a “Linux Kernel Community Enforcement Statement” to be included in future Linux documentation, in order to ensure contributions to the kernel don't fall foul of copyright claims that have already seen a single developer win "at least a few million Euros.”

In a post released on Monday, October 16th, Kroah-Hartman explained the Statement's needed because not everyone who contributes to the kernel understands the obligations the GNU Public Licence 2.0 (GPL 2.0), and the licence has “ambiguities … that no one in our community has ever considered part of compliance.”

Those ambiguities, he writes, have been used by a developer named Patrick McHardy to run multiple copyright enforcement lawsuits.

Verletzung von OSS-Lizenzbedingungen | Risiken

- Klassische Fehler beim Einsatz von OSS:
  - Keine Mitlieferung des Lizenztextes
  - Fehlende Source Codes
  - Fehlerhafte Einbindung von GPL-/LGPL-Komponenten
- Risiken bei Verletzung von OSS-Lizenzbedingungen:
  - Strafbarkeit, bis zu fünf Jahren Freiheitsstrafe
  - Wegfall von Nutzungsrechten wegen Lizenzverletzung
  - Unterlassungsansprüche
  - Schadensersatz
  - GPL-Infektion → Keine wirtschaftliche Verwertungsmöglichkeit entwickelter proprietärer Produkte

Verletzung von OSS-Lizenzbedingungen | Risiken

- Einhaltung von OSS-Lizenzen wird inzwischen von mehreren Organisationen überwacht und verfolgt
- Beispiele:
  - Software Freedom Law Center (SFLC)
  - gpl-violations.org
- Vermehrte Verfolgung derartiger Ansprüche in der jüngeren Vergangenheit auch von Privatpersonen

software freedom conservancy

DONATE JOIN VIZIO

HOME WHAT WE DO WHO WE ARE LEARN NEWS

Conservancy's Copyleft Compliance Projects

As existing donors and sustainers know, the Software Freedom Conservancy is a 501(c)(3) non-profit charity registered in New York, and Conservancy helps people take control of their computing by growing the software freedom movement, supporting community-driven alternatives to proprietary software, and defending free software with practical initiatives. Conservancy accomplishes these goals with various initiatives, including defending and upholding the rights of software users and consumers under copyleft licenses, such as the GPL.

Free and open source software (FOSS) is everywhere and in everything; yet our software freedom is constantly eroded. With the help of its volunteers, **member projects**, and **staff**, Conservancy stands up for users' software freedom via its copyleft compliance work.

Conservancy's primary work in copyleft compliance currently focuses on our **Strategic GPL Enforcement**

What We Do

Copyleft Compliance
Vizio Lawsuit
Member Projects
Outreachy

Vizio Lawsuit

About the Lawsuit
Press Release

▶ **Support Now!**

Verletzung von OSS-Lizenzbedingungen | Rechtsprechung

- **OLG Karlsruhe, Urteil vom 23.04.2008, 6 U 180/06, CR 2009, 217: Persönliche Geschäftsführerhaftung bei Lizenzverletzung**

  – Unternehmen setzte Software ohne erforderliche Lizenzen ein. Ehemaliger Mitarbeiter erstattete Strafanzeige

  – Persönliche Haftung des GmbH-Geschäftsführers wegen Sorgfaltspflichtverletzung auf Schadensersatz:
  Der Beklagte zu 2 war mithin verpflichtet, dafür Sorge zu tragen, dass auf den Computern des Unternehmens nur lizenzierte Software genutzt wird. Den sich daraus ergebenden Anforderungen ist der Beklagte zu 2 nicht einmal ansatzweise nachgekommen.

Haftung des Managements bei Lizenzverletzungen möglich

Best Practice

- Nach dem Compliance-Handbuch der Linux Foundation ist ein Open-Source-Compliance-Team mit **mindestens 4 Vollzeitstellen** erforderlich:
  - *„The core team, often called the Open Source Review Board (OSRB), consists of representatives from engineering and product teams, one or more legal counsel, and the Compliance Officer. The extended team consists of various individuals […] Unlike the core team, members of the extended team are only working on compliance on a part-time basis […].“*

Ibrahim Haddad, Open Source Compliance in the Enterprise, 2nd Edition 2018, p. 33

www.linuxfoundation.org/compliance-and-security/2018/12/open-source-compliance-in-the-enterprise/

Best Practice | Lizenzmatrix

- Warum eine Lizenzmatrix bei der Umsetzung von Open Source Compliance?
  - Übliches Vorgehen: Raussuchen von Lizenztext und Urhebervermerken, Mitliefern dieser Texte, fertig.
  - Das reicht nicht!
  - In vielen Fällen kann OSS nur unter Verstoß gegen die zugrunde liegenden Lizenzbedingungen eingesetzt werden!
  - Warum? Entwickler nehmen einfach „die neueste Lizenz“, ohne deren Pflichten zu prüfen und ohne sich über die Folgen im Klaren zu sein.
  - Beispiel: Lizenzierung von iOS-Apps unter der GPL-3.0
  - DRM-Verbot der GPL-3.0 in Ziffer 3: Derjenige, der ein GPL-Programm vertreibt, muss auf ein Verbot zur Umgehung technischer Schutzmaßnahmen für dieses Programm verzichten

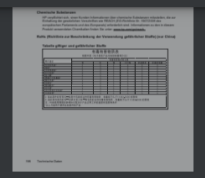
				Linux.
ProtonMail	E-Mail client ProtonMail	GPLv3	git	Also available for Android.
Signal	Encrypted instant messaging, voice and video calling	GPLv3	git	Also available for Android, Windows, MacOS and Linux.
Surespot	Encrypted instant messaging	GPLv3	git	Also available for Android.
Tutanota	Email client	GPLv3	git	Also available for Android, Windows, MacOS and Linux.
Wire	Encrypted instant messaging, voice and video calling	GPLv3	git	Also available for Android, Windows, MacOS and Linux.
Joplin	Note taking and to-do application with synchronization capabilities	MIT	git	Also available for Android, Windows, macOS and Linux.
NetNewsWire	RSS reader	MIT	git	Also available for macOS.
OsmAnd	Offline maps and navigation using OpenStreetMap data	MIT	git	Also available for Android.
The White House	The official White House app	MIT	git	
Wikipedia	The official Wikipedia app	MIT	git	Also available for Android, webOS and Kindle.
Firefox Focus	Mobile web browser	MPL 2.0	git	Also available for Android.
Firefox for iOS	Mobile web browser	MPL 2.0	git	
VLC for iOS	A port of the free VLC media player	MPL 2.0 GPLv2+	git	
Collabora Online	Office suite compatible with Microsoft Office, enterprise ready LibreOffice	MPLv2.0	git	Also available for Android, Chrome OS, iPadOS, Windows, macOS and Linux.
Onion Browser	An open-source, privacy-enhancing web browser for iOS, utilizing the Tor anonymity network	own	git	

Best Practice | Kompatibilitäts-Check

Bei einigen Lizenzen fehlen zudem Regelungen zur Rechtseinräumung. Bei anderen wird sogar klar darauf hingewiesen, dass Nutzungsrechte fehlen.

Beispiel: LibTomCrypt:

> *LibTomCrypt is public domain. As should all quality software be.*
>
> *All of the software was either written by or donated to Tom St Denis for the purposes of this project. The only exception is the SAFER.C source which has no known license status (assumed copyrighted) which is why SAFER,C is shipped as disabled.*


202


203


204


205

SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LICENSE.md4-pubdom--jm_share_folder

LibTomCrypt is public domain. As should all quality software be.

All of the software was either written by or donated to Tom St Denis for the purposes of this project. The only exception is the SAFER.C source which has no known license status (assumed copyrighted) which is why SAFER,C is shipped as disabled.

Tom St Denis

LICENSE.md5-pubdom--jm_share_folder

LibTomCrypt is public domain. As should all quality software be.

All of the software was either written by or donated to Tom St Denis for the purposes of this project. The only exception is the SAFER.C source which has no known license status (assumed copyrighted) which is why SAFER,C is shipped as disabled.

Tom St Denis

Best Practice | Lizenzmatrix

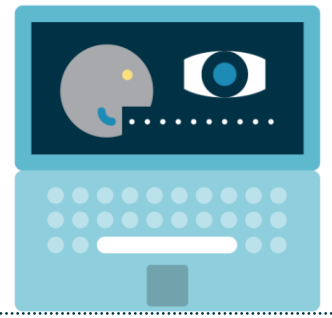
- Warum eine Lizenzmatrix bei der Umsetzung von Open Source Compliance?
  - Übliche Scanning Tools stellen oftmals lediglich Lizenztexte und Copyright-Klauseln zusammen, bieten aber keinen detaillierten und nachvollziehbaren Überblick über übrige Lizenzpflichten
  - Sämtliche Pflichten einer Lizenz müssen
    - erfasst, bewertet und dann
    - gegen eigene Verwendung abgeglichen werden.
  - Die Interpretation einzelner Lizenzen und deren Pflichten ist häufig umstritten
  - Allein die binäre Darstellung eines Ergebnisses hilft bei umstrittenen Interpretationen nicht weiter

Best Practice | Lizenzmatrix

- Beispiel: Use Case „ASP-Nutzung“: Ist ein Zugänglichmachen von Software in Form von Application Service Provision (ASP/SaaS) zulässig?
  - Viele Lizenzen enthalten hierzu keine klaren Regelungen
  - Übliche Lösung: Viele Memos zu einzelnen Lizenzen. Unübersichtlich und keine Hilfe bei schnellem Überblick über Einhaltung der Pflichten abhängig von konkretem Use Case
- Unsere Lösung:
  - Aufspalten der Frage in Teilaspekte und -argumente, die dafür oder dagegen sprechen
  - Gewichtung der Aspekte mit unterschiedlichen Score-Werten und Bewertungslogiken
  - Berechnung der Score-Werte
  - Übersichtliche Darstellung
  - Vergleich mit Anwendungsszenarien des jeweiligen Unternehmens

FOSSmatrix – Schritt für Schritt zur Compliance

Lizenz-dokumentation	Welche Rechte und Pflichten ergeben sich aus Lizenzen?
Entwicklung von Use Cases	Wie wird die Software konkret verwendet?
Mapping von Use Cases	Bei welchen Lizenzen gibt es Konflikte mit dem Use Case?



Was unterscheidet die FOSSmatrix von anderen Tools?

Die FOSSmatrix fängt da an, wo die üblichen Scanning Tools aufhören:

Input:

- Use Cases
  (einmal vorab via Webinterface definiert)
- Lizenzliste
  (für jedes Projekt unterschiedlich, Auswahl via Webinterface, via CSV-Import oder via API)
- Wahl des Use Case (manuell via Webinterface oder via API)

Output:

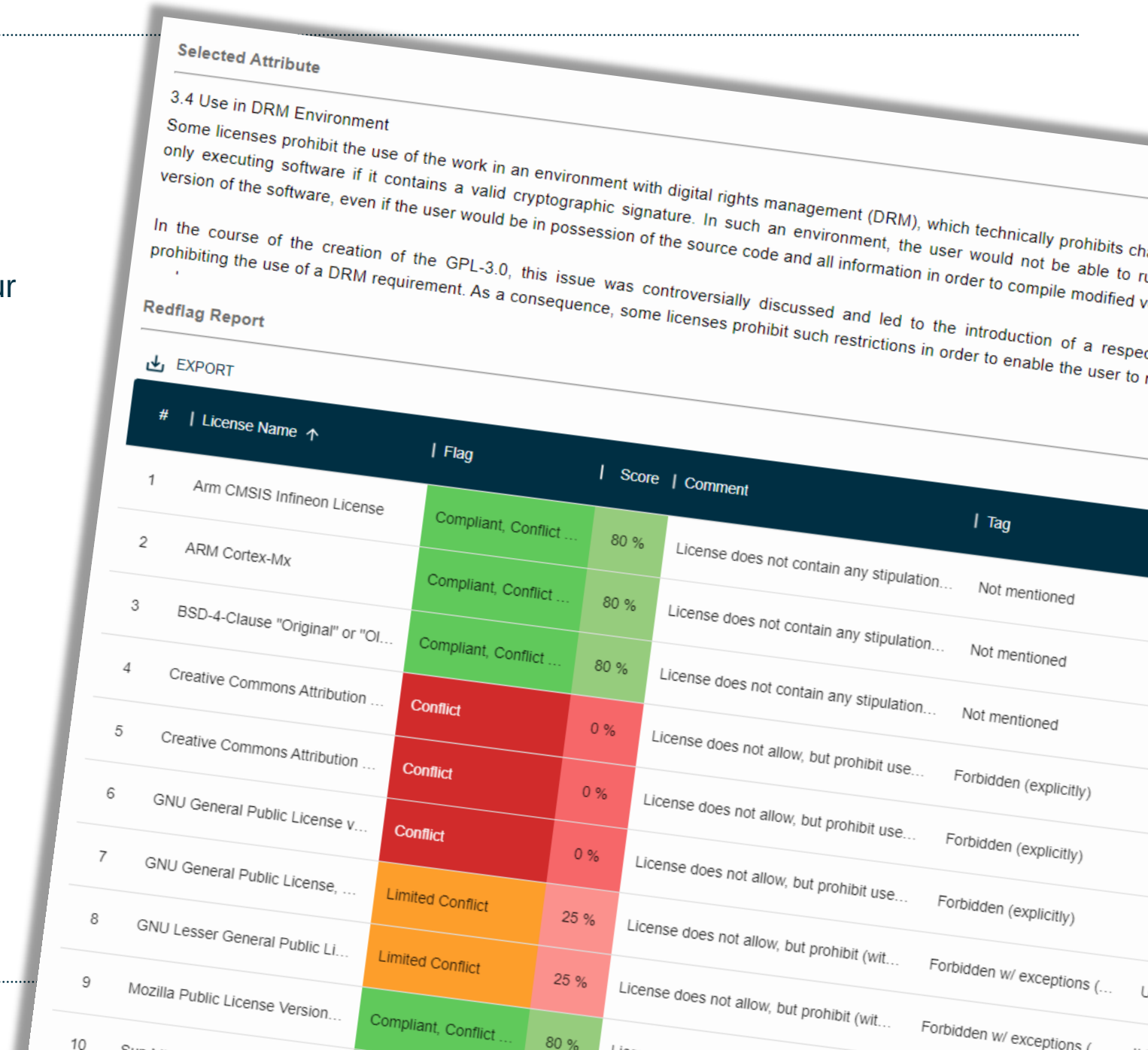
- Überblick über Konflikte bei einzelnen Attributen der Lizenzen (Webinterface, CSV-Export oder API)
- Weitere Angaben zu den Attributen, Verweise auf Literatur, Rechtsprechung, etc.

- Scanning Tools: Identifizierung von verwendeten OSS-Komponenten. Management von Compliance-Artefakten (also SBOM, Lizenztexte, Source Code)
- FOSSmatrix: Rechtliche Prüfung und Abgleich von Lizenzen mit konkretem Einsatzszenario (Use Case)
- Umgesetzt als Webservice, bedienbar per Browser, kann via RESTful API in eigene Toolchain integriert werden

FOSSmatrix im Überblick

Standardisierte Bewertung einzelner Lizenzpflichten als Webservice mit Schnittstelle zur Integration in bestehende Toolchain

- **Auswertung von Lizenzen**, standardisiert, vollständig dokumentiert und parametrisierbar mit Prozentangaben zur automatischen Weiterverarbeitung
- Derzeit knapp 200 Lizenzen, klassifiziert nach insgesamt 75 Attributen (inkl. Stammdaten). Sowohl „Klassiker“, als auch Exoten und kommerzielle Lizenzen
- **Use Case Mapping** gegen die jeweiligen Lizenzen mit automatischer Konfliktprüfung
- Keine mehrseitigen Memos – sondern Rechtsberatung als strukturierte Daten
- Mehr als 10 Jahre Erfahrung zu OSS



Kontakt

Dr. Hendrik Schöttle
Partner, Fachanwalt für IT-Recht
Germany

+49 89 5434 8046
hendrik.schoettle@osborneclarke.com

„Im Bereich Open Source ein Spitzenname“

Wettbewerber, JUVE-Handbuch 2021/2022

Dr. Hendrik Schöttle berät im IT- und Datenschutzrecht.

Hendrik Schöttle wurde in den letzten Jahren wiederholt sowohl vom Handelsblatt und von Best Lawyers als auch von der Wirtschaftswoche und vom Kanzleimonitor als einer der besten Anwälte bzw. als mehrfach empfohlener Anwalt im IT-Recht genannt. Laut JUVE-Handbuch 2021/2022 ist er „im Bereich Open Source ein Spitzenname“. Das Kanzleihandbuch Legal 500 Deutschland empfiehlt ihn, weil er durch „sehr gute IT-Kenntnisse besticht, auch wenn es sich um exotische Fragen handelt“ und durch ein „sehr schnelles Verständnis technischer Details“.

Er hat langjährige Erfahrung bei der Beratung, Vertragsgestaltung und Verhandlung von komplexen IT-Projekten. Seine Schwerpunkte sind IoT, Digitalisierung und Cloud Computing. Er berät zu Software-Lizenzmodellen, insbesondere zu Open-Source-Software, und im Datenschutzrecht. Zu seinen Mandanten gehören international tätige Technologiekonzerne sowie namhafte IT- und E-Business-Unternehmen.

Hendrik Schöttle arbeitet seit 2005 als Rechtsanwalt, seit 2007 im Münchner Büro von Osborne Clarke. Er war mehrfach im Rahmen von Secondments in Rechtsabteilungen von IT-Unternehmen tätig. Zudem hat er mehrere Jahre als Software-Entwickler am Institut für Rechtsinformatik der Universität des Saarlandes gearbeitet. Seine praktische Erfahrung und sein technisches Know-how kommen seinen Mandanten bei der technologienahen Beratung zugute.

Er ist Autor zahlreicher Veröffentlichungen, Mitautor mehrerer Handbücher und Kommentare, unter anderem des Beck’schen Handbuchs IT- und Datenschutzrecht und des juris Praxiskommentars zum BGB.

Hendrik Schöttle ist Dozent der Deutschen Anwaltakademie für den Fachanwaltslehrgang IT-Recht und hält regelmäßig Vorträge zu Themen des IT-Rechts.

Er ist Mitglied im Vorstand des Arbeitskreises Open Source des BITKOM, Mitglied des Ausschusses Datenschutzrecht der Bundesrechtsanwaltskammer (BRAK), der Arbeitsgemeinschaft Informationstechnologie im Deutschen Anwaltverein (DAV) und der Deutschen Gesellschaft für Recht und Informatik (DGRI).