

Open Source Compliance

RA Dr. Christian Laux, LL.M.

OpenExpo 2010, Bern

25. März 2010

Software im Unternehmenseinsatz

- Vertragliche Erlaubnis des Rechtsinhabers: „Lizenz“
- Ziele:
 - Eigene Software mit eigenem Lizenzkonzept an den Markt
 - Interne Nutzung soll ungestört sein

Compliance

- Einhaltung sämtlicher für das Unternehmen relevanten gesetzlichen Pflichten, Vorschriften und Richtlinien
- Bezüglich Open Source: Lizenzbedingungen einhalten

Lizenzmanagement als Complianceaufgabe

- Selbstverständlich für proprietäre Software
- Open Source rutscht oft durch die Maschen der Compliance
 - freie Verfügbarkeit
 - keine Lizenzgebühren
- Genehmigungsfreiheit auch intern?

Pflichten aus Open Source Lizenzen

Notices

„Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.“ (BSD)

Pflichten aus Open Source Lizenzen

Kopie der Lizenz

„a copy of this Agreement must be included with each copy of the Program “ (Eclipse Public License, Version 1.0)

Pflichten aus Open Source Lizenzen

Änderungsvermerk

„You must cause any modified files to carry prominent notices stating that You changed the files.“ (Apache 2.0)

Pflichten aus Open Source Lizenzen

Corresponding Source

„You may convey a covered work in object code form ... provided that you also convey the machine-readable Corresponding Source under the terms of this License .“ (GNU General Public License, Version 3)

Pflichten aus Open Source Lizenzen

Copyleft

„You must cause any work

- that you distribute or publish,
- that in whole or in part contains or is derived from the Program or any part thereof,

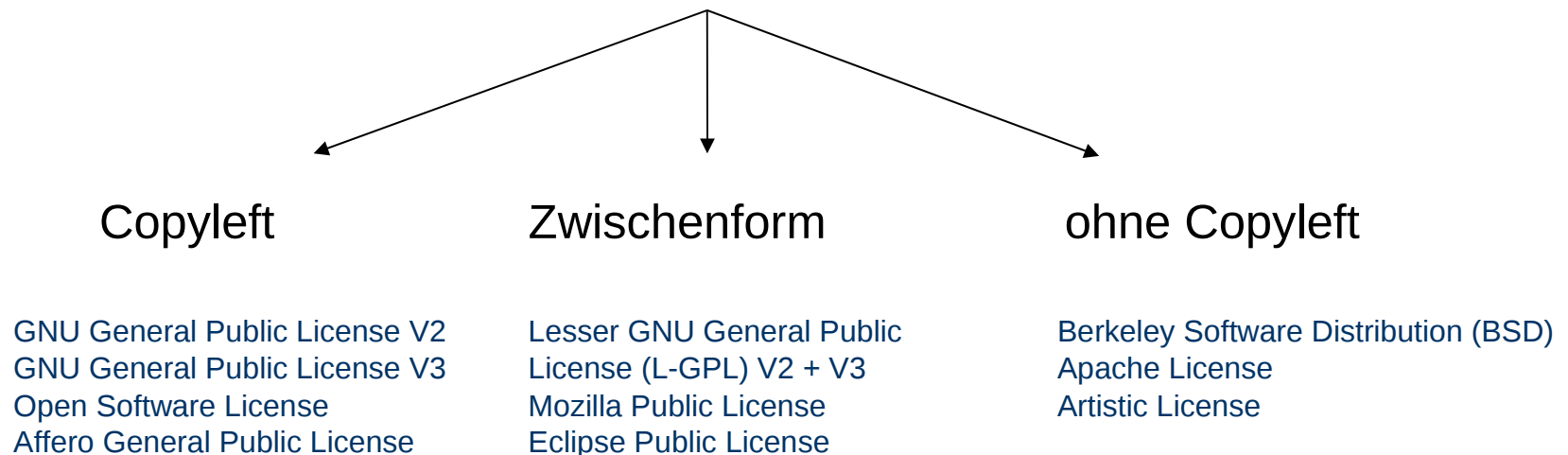
to be licensed

- as a whole
- at no charge
- to all third parties

under the terms of this License“ (GPL Version 2)

Zusammenfassende Übersicht

Open Source Lizenzen



Konfliktmöglichkeiten

Probleme als Nutzer

- Nutzungsverbot, Produktionsausfall
- finanzielle Ersatzforderungen
 - Haftung
 - entgangener Gewinn
- Strafrecht
- negative Publicity

Probleme als Lieferant und Redistributor

- wie ein Nutzer
- evtl. Pflicht, Code zu veröffentlichen
 - Broadcom/Linksys: Driver Software für Router
- Verlust möglicher Umsätze
 - Broadcom/Linksys: Source-Codes verfügbar, in der Folge: Vielzahl von alternativen Firmwares auf dem Markt, oft mit einem erweiterten Funktionsumfang

Probleme bei Transaktionen

- Unternehmensverkauf, Outsourcing, Zusammenarbeitsverträge
- Due Diligence
- Gewährleistungen im Kaufvertrag
- wird das Problem erst während des Verkaufs erkannt, ist viel verloren

Probleme unternehmensintern

- Versteckte Verbindlichkeiten / Rückstellungen
- Haftung als Verwaltungsrat (Art. 754 Abs. 2 OR):
 - "Wer die Erfüllung einer Aufgabe befugterweise einem anderen Organ überträgt, haftet für den von diesem verursachten Schaden, sofern er nicht nachweist, dass er bei der Auswahl, Unterrichtung und Überwachung die nach den Umständen gebotene Sorgfalt angewendet hat."

Schutzvorkehren

Vertraglicher Schutz

- Vertragliche Klauseln
 - Gewährleistung
 - Haftung
- Auswahl des Dienstleisters entscheidend

Interne Organisation

- Gesetzliche Regelung?
- Standards?
 - ISO 17799 (Orientierung an Sicherheitszielen)
 - ITIL (Prozessorientiert)
 - COBIT (Kontrollorientiert)
- Best Practices?
 - Einhaltung Best Practices = IT-Governance?
 - Branchenspezifische Best Practice

Best Practice

- Identifizieren
 - Anwendbare Lizenzen
 - Herkunft (Rechtsinhaberschaft, Fundstelle, etc.)
- Analysieren
 - Rechte und Pflichten
 - Beabsichtigte Nutzung
- Abläufe festlegen
 - erlaubte Open Source Software
 - Eskalation für andere Open Source Software
- Dokumentieren

Resultate der OSS Compliance

- Risikominimierung im internen Verhältnis
 - Haftungsreduktion im internen Verhältnis
 - Sorgfalt, sofern Best Practices angemessen sind mit Blick auf Tätigkeit des Unternehmens
- Relevanz für D&O Versicherungen?

Resultate der OSS Compliance

- Abwehr finanzielle Ansprüche
 - Haftungsreduktion extern
 - keine Grobfahrlässigkeit
 - Abwehr des Vorwurfs „Wissenmüssen“
- Management der Reputationsrisiken
(„you need to have a good story ...“)

Zusammenfassung

- Vertragliche Massnahmen
- Organisatorische Massnahmen
 - beim Einsatz von OSS in eigenen Produkten
 - bei Beschaffung von Software von Dritten
 - Einsatz von Policies
 - Einsatz von technischen Hilfsmitteln empfehlenswert

Kontakt

Dr. Christian Laux, LL.M. (Stanford)

Rechtsanwalt

Bratschi Wiederkehr & Buob

Bahnhofstrasse 106

8001 Zürich

058 258 1100

058 258 1199

christian.laux@bratschi-law.ch

NEU: <http://blawg.ch-open.ch>