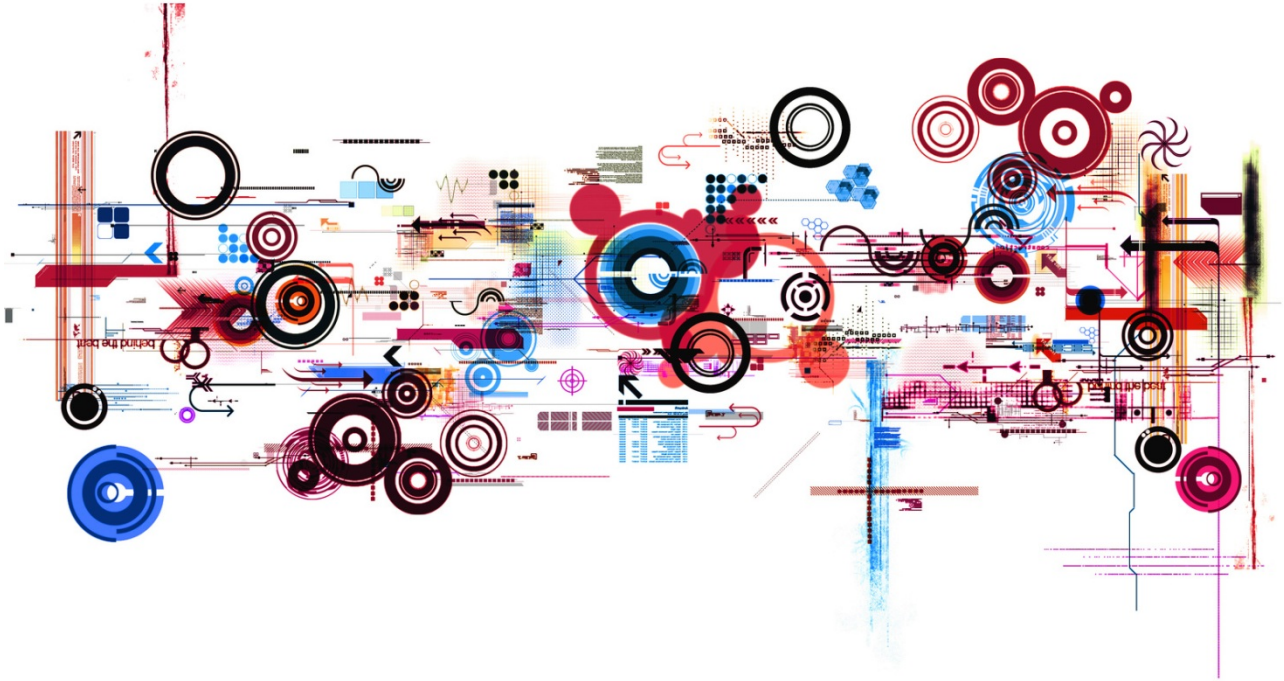
Open Source Management in Unternehmen

Praktische Hinweise für ein Open Source Management Programm



Referent: Udo Steger
Rechtsanwalt, München

Das Programm

Das Programm 1/2

- Bedeutung von OSS Management
  - Ein paar Begriffe zur Einführung *)
  - OSS ist überall
  - Fälle aus der Rechtsprechung *)
  - OSS und M&A *)
  - Typische Fehler beim Umgang mit OSS
- Strategische Überlegungen beim OSS Management
  - Produktpalette des Unternehmens
  - Wege von OSS in die Produkte des Unternehmens
  - Geschäftsmodell des Unternehmens *)
  - Patente

(*) = Im Vortrag gekürzt, Download-Version vollständig

Das Programm 2/2

- Werkzeuge und Prozesse beim OSS Management
  - Ziel - das ist zu tun
  - Rollenverteilung
  - Datenbank
  - Development - Einbindung in den Entwicklungsprozess
  - Supply Chain - Einbindung in den Beschaffungsprozess
  - Sales - Einbindung des Vertriebs, Umgang mit Kunden
  - Kontrolle der Weitergabe von OSS an Kunden *)
  - Dokumentation *)
  - Verträge
  - Mitwirkung bei OSS Projekten (Contributions) *)
  - Unternehmensrichtlinie zum Umgang mit OSS

- Schlussfolgerungen und Thesen

(*) = Im Vortrag gekürzt, Download-Version vollständig

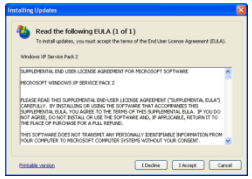
Bedeutung von OSS Management

Bedeutung von OSS Management: Ein paar Begriffe zur Einführung

- „OSS“: Open Source Software
  - Hier verwendet als Oberbegriff für Open Source Software, Freeware, Public Domain, „Donationware“, Content mit „freien“ Lizenzen
- „BOM“: Bill of Material
  - Liste der Komponenten eines Produkts, d.h. Hardware, Software
  - Erlaubt die Zuordnung von Komponenten (Version, Eigenschaften wie z.B. OSS, Inkompatibilitäten) zu Produkten
  - BOS: Bill Of Software für Software, Hardware mit Firmware

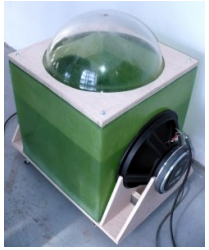
- „xGPLv2“, „xGPLv3“
  - verschiedene Versionen der GNU General Public License

- „copyleft“, „patentleft“
  - Lizenzbestimmungen, die Veröffentlichung von Quellcode oder eine Zwangspatentlizenz / Nichtdurchsetzbarkeit von Patenten vorsehen
- „EULA“: End User License Agreement
  - Lizenzbestimmungen für Endbenutzer



Bedeutung von OSS Management: OSS ist überall 1/2

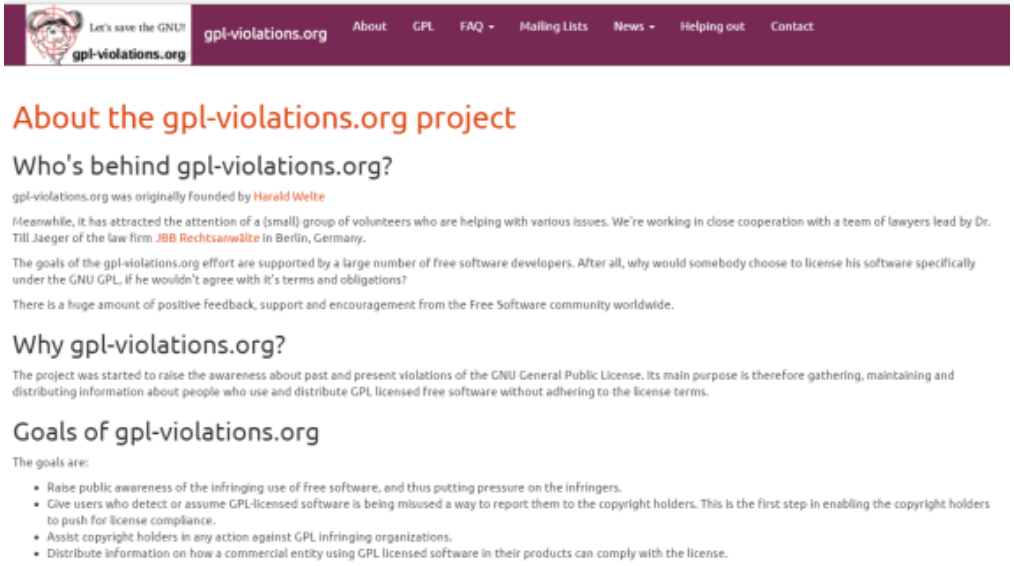
- Irrtum #1: „Wir benutzen keine OSS“
  - Faktisch in praktisch jeder Software und jedem Gerät mit Firmware
    - Smartphones (Android), Desktop-Telefone, Drucker, Routern (Linux), Fernseher, Kameras, Autos, Waschmaschinen, etc.
    - Extreme Modularität und Anpassbarkeit von Linux führt dazu, dass sich Linux-Betriebssystemkerne in hunderten von Gerätearten finden.



- Irrtum #2: „Dann vermeiden wir halt OSS“
  - Faktisch kaum möglich, da OSS überall eingesetzt wird, auch als Teil kommerzieller Produkte
  - Verzicht auf OSS wäre, sofern möglich, ernster Wettbewerbsnachteil

Bedeutung von OSS Management: OSS ist überall 2/2

- Irrtum #3: „Ach was, wird schon keiner merken“
  - Zunehmende Bereitschaft der Autoren, OSS Lizenzen auch gerichtlich durchzusetzen
    - Rechtspranger www.gpl-violations.org
  - Teil der IT Due Diligence Prüfung bei Unternehmensübernahmen
  - Autoren sind neugierig, wo ihre OSS genutzt wird
    - es wurden schon Cartridges geknackt



Let's save the GNU! gpl-violations.org

gpl-violations.org | About | GPL | FAQ | Mailing Lists | News | Helping out | Contact

About the gpl-violations.org project

Who's behind gpl-violations.org?

gpl-violations.org was originally founded by Harald Welte

Meanwhile, it has attracted the attention of a (small) group of volunteers who are helping with various issues. We're working in close cooperation with a team of lawyers lead by Dr. Till Jaeger of the law firm JBB Rechtsanwälte in Berlin, Germany.

The goals of the gpl-violations.org effort are supported by a large number of free software developers. After all, why would somebody choose to license his software specifically under the GNU GPL, if he wouldn't agree with it's terms and obligations?

There is a huge amount of positive feedback, support and encouragement from the Free Software community worldwide.

Why gpl-violations.org?

The project was started to raise the awareness about past and present violations of the GNU General Public License. Its main purpose is therefore gathering, maintaining and distributing information about people who use and distribute GPL licensed free software without adhering to the license terms.

Goals of gpl-violations.org

The goals are:

- Raise public awareness of the infringing use of free software, and thus putting pressure on the infringers.
- Give users who detect or assume GPL-licensed software is being misused a way to report them to the copyright holders. This is the first step in enabling the copyright holders to push for license compliance.
- Assist copyright holders in any action against GPL infringing organizations.
- Distribute information on how a commercial entity using GPL licensed software in their products can comply with the license.

Bedeutung von OSS Management: Fälle aus der Rechtsprechung

- Schadensersatz bei Verletzung von OSS Lizenzen
  - Gestattung unentgeltlicher Nutzung mittels „*OSS Lizenz bedeutet nicht den Verzicht auf Ansprüche wegen etwaiger lizenz- und damit urheberrechtswidriger Handlungen*“ (LG Bochum, Urt. vom 03.03.2016, Az. I-8 O 294/15, nicht rechtskr.).

- OSS Lizenzen gelten auch für Firmware als Teil von Hardware
  - Router-Firmware mit OSS kann GPL unterfallen, kein Änderungs-verbot (LG Berlin, Urt. vom 08.11.2011, Az. 16 O 255/10 - AVM).

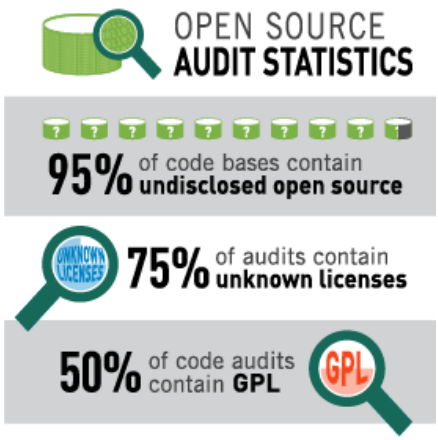
- Auch stillgelegter Code mit OSS Anteil kann Rechte verletzen
  - Es bestehen auch dann Ansprüche, wenn der unter der OSS Lizenz stehende Code lediglich zu Testzwecken verwendet wurde und innerhalb der verbreiteten Software keine Funktion erfüllt (LG Bochum, Urt. vom 03.03.2016, Az. I-8 O 294/15).

Bedeutung von OSS Management: Fälle aus der Rechtsprechung

- Genau der Code muss veröffentlicht werden, der benutzt wurde:
  - Zum Download angebotener GPL-lizensierter Quellcode muss der sein, aus dem der Object-Code (hier Firmare) erzeugt wurde (LG Hamburg, Urt. vom 14.06.2013, Az: 308 O 10/13 - Fantec)
- Darlegung der Urheberschaft kann schwer sein
  - (Mit-)Urheberschaft des OSS Autors muss hinreichend konkret belegt sein (LG Hamburg, Urt. vom 08.07.2016, Az. 310 O 89/15 – vmware)
- I.d.R. klagen die Urheber, aber: Versata vs. Ameriprise
  - Versata SW enthält GPLv2-lizensierte Komponente von XimpleWare.
  - Ameriprise ließ Versata SW bearbeiten. Versata klagte.
  - Ameriprise: SW sei „infiziert“ und nach GPLv2 zu lizensieren.
  - Verfahren 2015 durch Vergleich beigelegt

Ca. ½ der Urteile aus Deutschland: http://www.ifross.org/v-urteile

Bedeutung von OSS Management: Fälle aus der Rechtsprechung



(Grafik: Black Duck Software, Inc.)

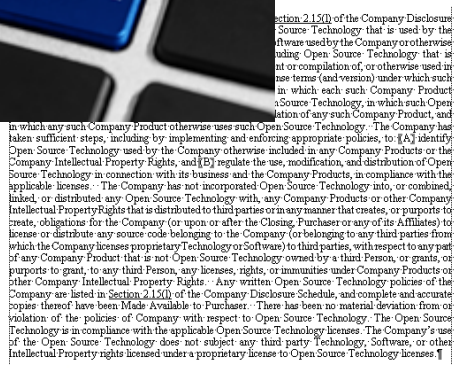
Schlussfolgerungen:

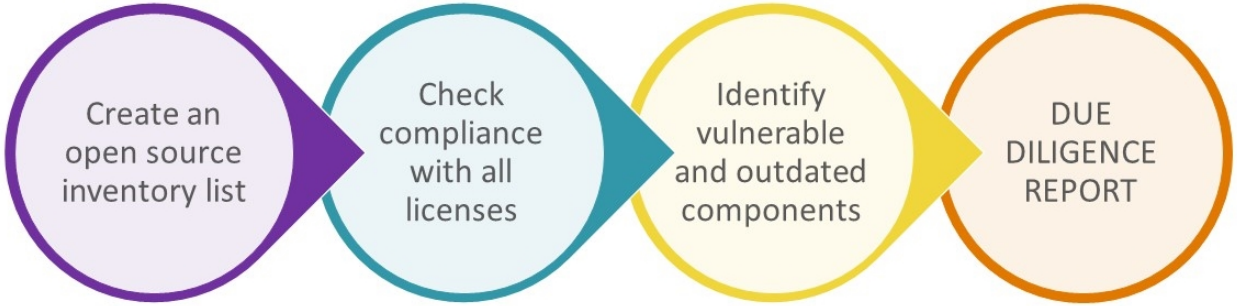
1. Nur weil OSS kostenfrei ist, sind Ansprüche von OSS Autoren nicht ausgeschlossen.
2. OSS Lizenzen gelten auch für Firmware.
3. OSS Lizenzen gelten auch dann, wenn der Code im Produkt stillgelegt ist, aber mitgeliefert wird.
4. Es muss versionsgenau der Quellcode veröffentlich werden, der zur Erstellung des Object Codes genutzt wurde hat
5. Die Darlegung der Urheberschaft kann v.a. bei Projekten mit vielen Miturhebern schwierig sein, ist aber nicht unmöglich.
6. Kunden könnten im Fall einer Verletzung von OSS Lizenzen Handlungen vornehmen, die die Lizenzbestimmungen sonst verbieten, und ggfs. Mängelrechte haben.

Daher: ein OSS Compliance Prozess ist zwingend nötig.

Bedeutung von OSS Management: OSS & M&A

- Auch die Kollegen aus dem M&A Bereich haben das Thema für sich entdeckt…
- Bei M&A Transaktionen kann der Kaufpreis durch mangelnde OSS Compliance entscheidend beeinträchtigt werden.





Grafiken: WhiteSource Software

Bedeutung von OSS Management: Typische Fehler beim Umgang mit OSS

Die Realität sieht oft so aus:

- Es werden keine oder unvollständige Lizenztexte beigefügt
- Keine Bereitstellung des (richtigen) Quellcodes
- Keine Nennung von Autorennamen (Attribution)
- Mangelhafte Integration von GPL/LGPL-lizensierter OSS in den eigenen Code löst „Infektion“ aus, d.h. den Copyleft-Effekt
- Keine Prüfung auf Lizenzkonflikte
- Kein Abgleich auf mögliche Gefährdung von Patenten
- Keine Dokumentation der Nutzung von OSS
  - Kaum Abwehr von Ansprüchen möglich, die im Zusammenhang mit OSS (auch: Gewährleistung, Produkthaftung) erhoben werden
- Keine Überwachung von (Auftrags-)entwicklern & Lieferanten
- Fehlende Prozesse zum Umgang mit OSS
  - Ständig Ad-Hoc Lösungen finden zu müssen, bindet Ressourcen

Strategische Überlegungen beim OSS Management

Strategische Überlegungen beim OSS Management: Produktpalette des Unternehmens 1/2

Eigene Produktpalette beeinflusst Umfang des OSS Managements:

- Herstellung eigener Produkte (SW / HW mit SW), Vertrieb
  - Wie stark ist Kontrolle über die Produktentwicklung / Supply Chain?
  - Wie stark ist Kontrolle über Produktvertrieb und Weitergabe von OSS?
- Vertrieb von Drittherstellerprodukten mit eigener Leistung (VAR)
  - wie vor, P: Lieferanten geben aber oft nur limitierte Gewährleistung
- Anpassung eigener/fremder Produkte (Professional Services)
  - wie vor, falls Kontrolle über die für den Kunden eingesetzte OSS
  - P: eigene Gewährleistungsverpflichtungen, Offenlegung von Code
- Auftragsentwicklung für Dritte (Individual-SW)
  - wie vor, zudem oft Integration mit den OSS Managementprozessen des / der Kunden nötig. P: Mangelhaftung, Agile Verfahren

Strategische Überlegungen beim OSS Management: Produktpalette des Unternehmens 2/2

Strategische/Taktische Fragen:

- Soll der Quell-Code im Unternehmen bleiben, oder kann (oder soll er sogar) offengelegt werden (copyleft)?
- Bestehen rechtliche Schranken, den Quell-Code offenzulegen?
  - Vertraulichkeitsverpflichtungen, Geheimschutz, Know-How
  - proprietärer Code von Dritten
- Pflegeaufwand:
  - Wie oft muss der Code angepasst werden?
  - Art der Produkte: komplexes System, Embedded System
  - Update Zyklen? IT Sicherheit?
- Einsatzzwecke der eigenen Softwareprodukte
  - Produkt ist eigenständig, z.B. ein Router oder eine Telefonanlage
  - Produkt ist Komponente von Drittprodukten, z.B. Baugruppe, Chip
  - Lebens- und Einsatzdauer des Produkts
  - Verwendung im KRITIS Umfeld?

Strategische Überlegungen beim OSS Management: Wege von OSS in die Produkte des Unternehmens

OSS gelangt auf vielen Wegen ins Unternehmen und die Produkte:

- Eigene Produktentwicklung nutzt OSS
- Auftragsentwickler nutzen OSS
- Standardsoftware enthält OSS, und/oder Anpassungen
- zugekaufte OEM Versionen mit OSS
- Weiterverkauf von Hardware mit Firmware, die OSS enthält
- Zukauf von Hardware-Komponenten, Treiber, Referenz-Implementation mit OSS
- Vorgaben des Kunden bei der Entwicklung
- Hersteller lizensieren neuere Versionen einer Software als OSS
- OSS Projekt ändert die bislang verwendete (akzeptable) OSS Lizenz auf andere (nicht mehr akzeptable) OSS Lizenz
  - z.B. „Update“ von GPLv2 => GPLv3

Folge: auf der BOM kann eine ganze Menge OSS stehen.

Strategische Überlegungen beim OSS Management: Geschäftsmodell

Welches Geschäftsmodell verfolgt das Unternehmen mit OSS?

- Produkte herstellen und vertreiben
  - Eigene Produkte mit OSS Anteil
  - Werden überwiegend Produkte bereitgestellt (SaaS) oder vermietet?
- Dienstleistungen/Services erbringen
  - Schwerpunkt auf Beratungs- und Supportleistungen, nicht auf Produkt
  - Prof. Services/ individuelle Entwicklungen
- Produkte Dritter vertreiben und Partizipation an Umsätzen
  - Appshop- oder Plattform-Gedanke, Partizipation am Erfolg Dritter
  - z.B. Google mit App Store
- Ergänzung Produkte Dritter um eigene Leistungen (VAR)
  - Drittprodukte mit OSS integrieren mit eigenen proprietären Produkten

Strategische Überlegungen beim OSS Management: Patente

- Patentleft Effekt mancher OSS Lizenzen
  - Zwangs-Patentlizenz, falls eigene Patente berührt
  - gilt jedenfalls bei Bearbeitung der OSS
    - z.B. Re-Packaging / „Härten“ einer Linux Distribution. Gelingt dies, ohne OSS Komponenten zu bearbeiten (GPL)?
  - wird u.U. schon bei bloßer Weitergabe (!!) einer unter Patentleft stehenden OSS ausgelöst
    - vgl. CR 2013, 1 – Schöttle – *Der Patentleft-Effekt der GPLv3* oder hier.

- Risikoabwägung
  - Umfang und Bedeutung des eigenen Patentportfolios
  - Hardwarenähe / Technizität der eigenen Produkte
  - Geschäftsmodell: werden Produkte ausgeliefert oder Produkte nur zur Nutzung bereitgestellt (SaaS)?

- Anforderungen des Kunden: Patentportfolio, OSS Richtlinie

Werkzeuge und Prozesse beim OSS Management

Werkzeuge und Prozesse beim OSS Management: Ziel – das ist zu tun

Ein OSS Management Prozess sollte folgende Ziele erreichen:

- **Jegliche OSS gelangt nur nach Durchlaufen eines gesteuerten Prozesses in Produkte des Unternehmens**
  - OSS Management ist integraler Teil des Entwicklungsprozesses
  - Verwendung von OSS in Produkten ist umfassend dokumentiert
  - Komponenten-genau, über Versionen hinweg
- Die Einhaltung der OSS Lizenzbestimmungen ist gewährleistet
  - Es wird nicht zu viel, und nicht zu wenig veröffentlicht
- Es gibt einen OSS Management<u>prozess</u> (nicht nur ein Projekt)
  - Prozess ist mit anderen relevanten Prozessen im Unternehmen abgestimmt, z.B. Vulnerability Management, Patente
  - Verbildliche Dokumentation des OSS Managementprozesses
- OSS wird in einem geordneten Verfahren veröffentlicht
- Unternehmensleitung versteht und unterstützt OSS Management

Werkzeuge und Prozesse beim OSS Management: Rollenverteilung 1/2

- OSS Team mit Beteiligten aus allen relevanten Bereichen des Unternehmens
  - Rechtsabteilung: Lizenzprüfung, jur. Risikobewertung
  - Programmierer: Technische Zusammenhänge, Art der Integration
  - Qualitätsmanagement: scannen, Dokumentation
  - Produktion/Supply Chain: EULAs, Veröffentlichung der OSS
  - (opt.) IP/Patente wg Risiken für Patent-Portfolio, IT Security
- Aufgaben
  - Sichert die Einhaltung der OSS Richtlinien, auch mit internen Audits
  - Prüft scan reports, git Hinweise zur Behebung von Beanstandungen
  - Bewertet technisch oder rechtlich unklare Fälle/Lizenzen
  - Entscheidet im Alltag, bereitet Management Entscheidungen vor
  - Weiterentwicklung des OSS Management Prozesses und der verwendeten Werkzeuge
    - Führt OSS Richtlinien ein und entwickelt sie weiter
    - Definiert neue Prozesse, z.B. zu OSS Contribution

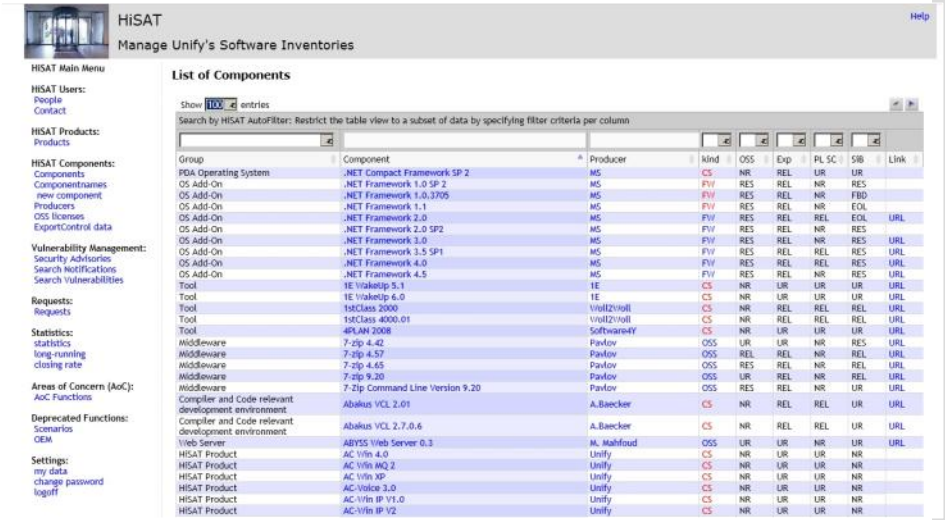
Werkzeuge und Prozesse beim OSS Management: Rollenverteilung 2/2

- OSS Agent
  - Rolle in jedem Programmierteam, Ansprechpartner des OSS Teams
  - Achtet auf Einhaltung der OSS Richtlinien im Team
  - Sorgt im Tagesgeschäft für
    - Dokumentation des OSS Einsatzes, Pflege der Datenbanken
    - Stößt Prüfungsprozesse an, z.B. neue Lizenz
    - Scannen, scannen, scannen
  - „Auge und Ohr“ des OSS Teams

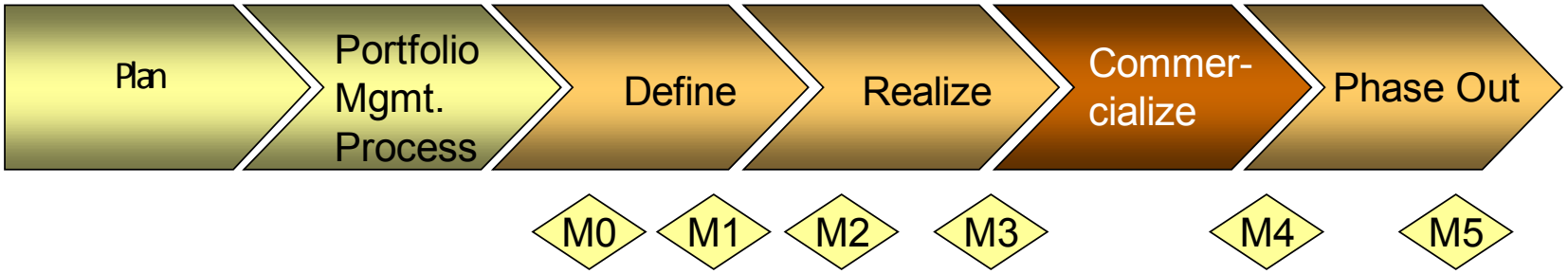
- Management Sponsor
  - trifft Entscheidungen und hilft, diese durchzusetzen
    - Änderungen der OSS Strategie können weitreichende Folgen haben
  - Beschafft/verantwortet Ressourcen oder Budgets
    - Kosten des OSS Scan Tools und der Verschiebung von Terminen
  - möglichst der Vorstand/GF, der für die Produkte zuständig ist

Werkzeuge und Prozesse beim OSS Management: Datenbank

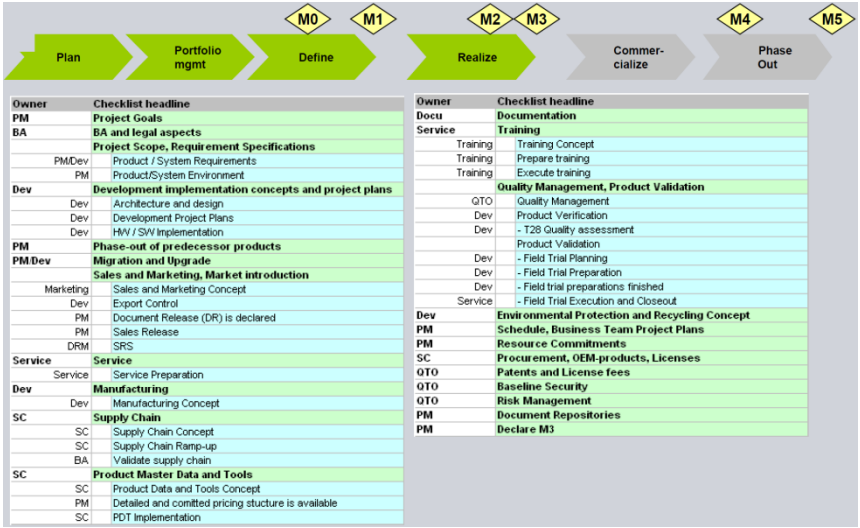
- Produkt- und Komponenten-Datenbank, speichert
  - alle eigenen Produkte samt Quellcode (Code Repository)
  - die OSS Komponenten
  - Umstände der Beschaffung (z.B. Archive, Screenshots)
  - Nutzung für OSS, freeware, public domain, ggfs. “open” content (creative commons etc.)
  - ggfs. Abgleich mit IT-Security/ Vulnerability Management
- Wichtig: zentrale Sammelstelle für das OSS Team, um die Arbeit zu organisieren und zu dokumentieren („OSS Helpdesk“)



Werkzeuge und Prozesse beim OSS Management: Development – Einbindung in den Entwicklungsprozess 1/3



- Phase M0 – M5: Lebenszyklus eines Produktes
  - Meist wird erst in den Phasen M3 – M4 Geld verdient
  - Bei „continuous delivery“ eher eine Schleife
- OSS Management muss den gesamten Lebenszyklus umfassen
  - je früher die OSS kontrolliert wird, desto besser

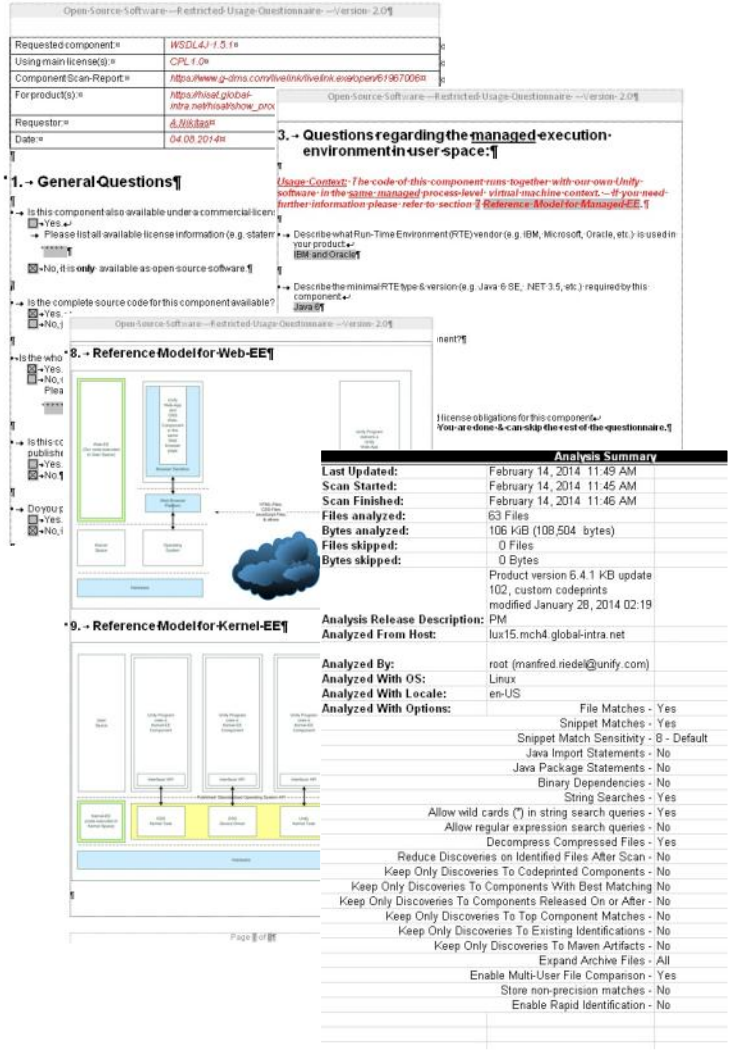


Owner	Checklist headline
PM	**Project Goals**
BA	**BA and legal aspects**
	Project Scope, Requirement Specifications
PM/Dev	Product / System Requirements
PM	Product/System Environment
Dev	**Development implementation concepts and project plans**
Dev	Architecture and design
Dev	Development Project Plans
Dev	HW / SW Implementation
PM	**Phase-out of predecessor products**
PM/Dev	**Migration and Upgrade**
	Sales and Marketing, Market introduction
Marketing	Sales and Marketing Concept
Dev	Export Control
PM	Document Release (DR) is declared
PM	Sales Release
DRM	SRS
Service	**Service**
Service	Service Preparation
Dev	**Manufacturing**
Dev	Manufacturing Concept
SC	**Supply Chain**
SC	Supply Chain Concept
SC	Supply Chain Ramp-up
BA	Validate supply chain
SC	**Product Master Data and Tools**
SC	Product Data and Tools Concept
PM	Detailed and comitted pricing stucture is available
SC	PDT Implementation

Owner	Checklist headline
Docu	**Documentation**
Service	**Training**
Training	Training Concept
Training	Prepare training
Training	Execute training
	Quality Management, Product Validation
QTO	Quality Management
Dev	Product Verification
Dev	- T28 Quality assessment
	Product Validation
Dev	- Field Trial Planning
Dev	- Field Trial Preparation
Dev	- Field trial preparations finished
Service	- Field Trial Execution and Closeout
Dev	**Environmental Protection and Recycling Concept**
PM	**Schedule, Business Team Project Plans**
PM	**Resource Commitments**
SC	**Procurement, OEM-products, Licenses**
QTO	**Patents and License fees**
QTO	**Baseline Security**
QTO	**Risk Management**
PM	**Document Repositories**
PM	**Declare M3**

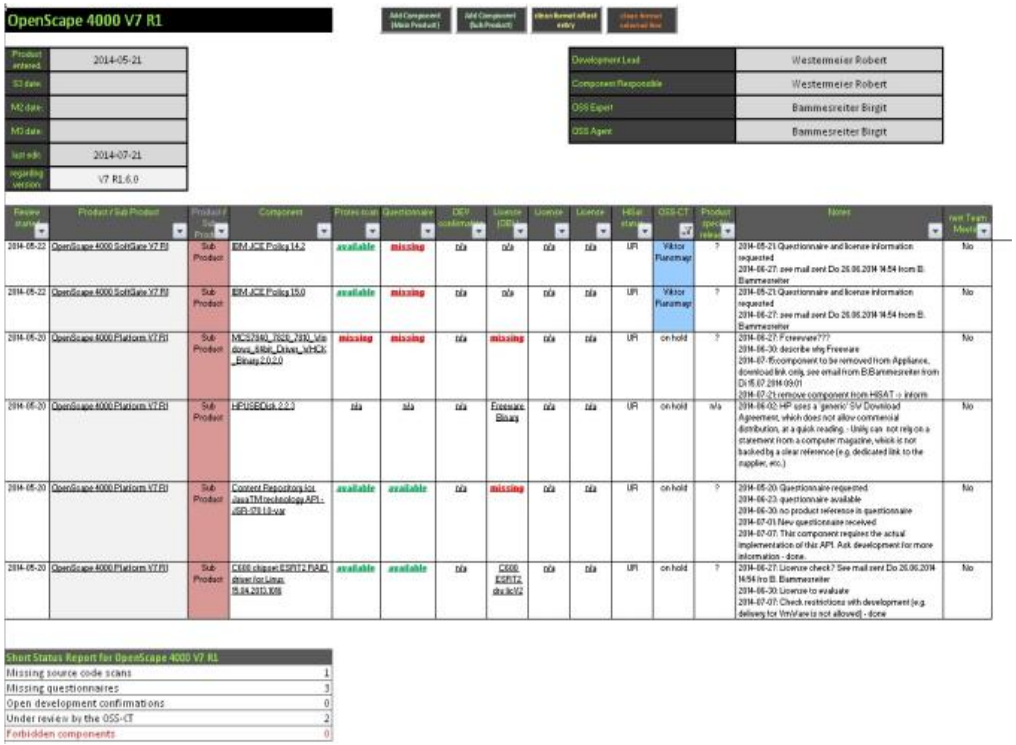
Werkzeuge und Prozesse beim OSS Management: Development – Einbindung in den Entwicklungsprozess 2/3

- Integration des OSS Managementprozesses in die Entwicklung
  - Gilt auch für Bugfixing und Vulnerability Management
- Neue OSS Komponenten in Datenbank eintragen
  - Job-Triggering: Freigabe, Lizenzprüfung
- Erstellung eines Scan reports
  - z.B. Black Duck Protex Scan
  - Alle Scan Reports werden archiviert.



Werkzeuge und Prozesse beim OSS Management: Development – Einbindung in den Entwicklungsprozess 3/3

- Einschaltung des OSS Teams
  - Bei Erreichen eines Meilensteins im Softwareentwicklungsprozess muss ein standardisierter Fragebogen ausgefüllt werden.
- Ergebnisse werden vom OSS Team analysiert
- Alle dazu beschlossenen Maßnahmen werden dokumentiert und archiviert
  - Freigabe
  - Weitere Informationen
  - Ggfs. Nachbesserung durch Entwickler
  - Prüfung anhand OSS Lizenz
  - Genehmigung Autor



Werkzeuge und Prozesse beim OSS Management: Supply Chain – Einbindung in den Beschaffungsprozess

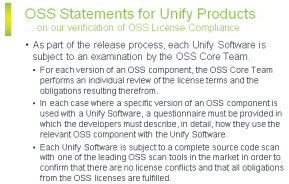
- Einbindung der Lieferanten
  - Eigene Entwickler, Konzerngesellschaften, Auftragsentwickler liefern meist Quellcode
  - Lieferanten von fertigen Produkten oder Komponenten (SW, HW), OEM Hersteller liefern meist eine „black box“

- Prüfung der gelieferten OSS Informationen
  - Wo Quellcode vorliegt, Scan und Einbindung in Prozess meist unproblematisch.
  - Scan Report ohne negativen Befund kann Abnahmekriterium sein
  - Problem: „black box“ Produkte. Oft nur Schlüssigkeitsprüfung möglich

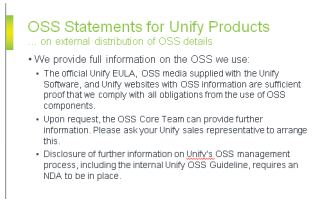
  - Mittelfristig: Verpflichtung zur Lieferung von Informationen im Software Package Data Exchange (SPDX) Format
    - Möglichkeit zur weiteren Automatisierung
    - CR-Online Blog, Beitrag vom 23.10.2016

Werkzeuge und Prozesse beim OSS Management: Sales – Einbindung des Vertriebs, Umgang mit Kunden

- „Kunden“
  - Direkte Kunden
  - Indirekte Kunden, Vertriebspartner
  - VAR Kunden



- An Kunden gerichtete Informationen
  - Öffentliche Unterlagen, die den OSS Prozess erläutern
  - Festlegen, wer wem welche Informationen geben darf
  - Keine Zusagen des Vertriebs oder Herausgabe anderer Unterlagen ohne das OSS Team!



- Auftragsentwicklung, OEM Kunden
  - Einbindung in den OSS Management Prozess des Kunden
  - Zugang zu Ressourcen, z.B. Scanning Software, Code Repository
  - Was muss wie beschrieben werden (Formate, SPDX)

Werkzeuge und Prozesse beim OSS Management: Kontrolle der Weitergabe von OSS an Kunden 1/2

- Herstellung der Produkte
  - (Noch Halb-) Automatisierte Erstellung der BOS / OSS EULA
  - Dokumentation der genauen Produktkonfiguration, ggfs. per Kunde
  - Produktion von Datenträgern
- OSS Bereitstellung gegenüber Kunden (Kundengruppen s.o.):
  - Download-Angebot nicht immer ausreichend (Risikofrage)
  - Prozess zum Zusenden eines Datenträgers
  - z.T. auch physischer OSS Datenträger in Box
  - nicht zu viel, nicht zu wenig
- Datenbank:
  - Was wurde wann mit welchen Komponenten veröffentlicht?
  - Updates, Upgrades, Bugfixes jeweils neue „Veröffentlichung“
  - Veröffentlichung der zum Object Code passenden Quellcodes

UNIFY

Release Notes [1]

Release Notes Version: *V1.0* **Document Owner:** Zoltan Miskei

Product Name: OpenScape 4000 CSTA

Product Version: *V7*

Software Release is identified by **Version: V7 R1.206.0**
(only V7 integration release of OpenScape 4000 V7 R1.8.0)
Major Release ☐ **Minor Release** ☒ **Fix Release** ☐ **Hotfix Release** ☐

Production Version:

System: File type	Product Item Number / File name	Size
rpm	*hp4k-CAP_Inside-7.1.0-1.noarch.rpm*	24 kByte
rpm	*hp4k-CAP_Inside-image-7.1.6-0@APE.noarch.rpm*	309828 kByte
rpm	*hp4k-common-1-13.noarch.rpm*	16 kByte

Export Control Classification Data **AL:** N **ECCN:** 5D002TSU

Field Trial: ☐ **eeQS:** ☐ **Limited Availability:** ☐ **General Availability:** ☒

Notice:
This document contains confidential information that is proprietary to Unify GmbH & Co. KG. No part of i ts contents may be used, copied, disclosed, or conveyed to any party in any manner whatsoever without prior consent.

DECLARATION DATE: Date : 2014-05-28

DECLARED BY: Corresponding PL-Development : Andrea Nagy
Corresponding Test TPL : Zoltan Miskei

DELIVERABLES: **Full Release:** ☒ **Delta Release:** ☐

Copyright © Unify GmbH & Co. KG, 2013
Hofmannstr. 51, 81379 Munich, Germany
All rights reserved.
The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.
Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify GmbH & Co. KG. All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.

Werkzeuge und Prozesse beim OSS Management: Kontrolle der Weitergabe von OSS an Kunden 2/2

- Exportkontrolle
  - Hardware & Software fallen unter das Außenwirtschaftsrecht
  - Embargolisten für bestimmte Länder und bestimmte Güter
  - Sperrlisten bzgl. Personen und Organisationen
  - Auch die kostenfreie Bereitstellung von SW über das Internet kann für Exportkontrolle relevant sein
- „Dual-Use Güter“: können zivil oder militärisch eingesetzt werden
  - Anhang I der EG-Dual-Use-Verordnung (EG) Nr. 428/2009 definiert Kategorien von Dual-Use Gütern
  - Alle Lieferungen und Leistungen,
    - auch Softwareüberlassung, Support
    - ggfs. auch bereits bloße Bereitstellung zum Download aus dem Ausland
  - Wissenstransfer (z.B. Supportforen, die vom Ausland erreichbar sind).
  - Prüfung auf Konflikte mit OSS Lizenzen, die eine allgemeine Bereitstellung fordern
    - Insbesondere bei Verschlüsselungstechnologien

Werkzeuge und Prozesse beim OSS Management: Dokumentation

- Datenbank/Code Repository
  - Enthält alle Produkte und Versionen, sowie Komponenten
  - Enthält definierte Versionen
  - Enthält die BOMs
  - Dokumentiert die Umstände, unter denen Code erworben wurde
  - wird nur nach Durchlaufen eines formalen Prozesses um neue OSS Komponenten (oder neue Versionen) ergänzt.

- Automatisierung:
  - Mittels BOM automatisierte Erstellung der OSS EULA
  - Hilft bei Bereitstellung veröffentlichter Quellcode vs. kompilierter Quellcode
  - Kommend: SPDX als Hilfe zur Automatisierung
  - Zukunftsmusik: automatisierte Publikation des Quellcodes auf Webseite und/oder auf Datenträger, Datenträger-erstellung.

Werkzeuge und Prozesse beim OSS Management: Verträge 1/2

- Einkaufsverträge mit Auftragsentwicklern
  - gelieferter Code muss ohne bedenklichen Befund gescannt werden
  - erst dann Abnahme/Freigabe oder Meilenstein / Sprintziel erreicht
- Einkaufsverträge mit Lieferanten von Standardsoftware
  - Gewährleistung, Freistellung bei Verletzung der Rechte Dritter
  - Selten: ausführliche Pflichtenbeschreibung, Scanreports
- Problem: Einkaufsverträge mit OEMs
  - OEM: Hersteller liefert Produkt zur Integration ins eigene Produkt, ggfs. in speziell angepasster Form
  - i.d.R. keine Lieferung von Quellcode = kein Scan möglich
  - Externe Scanangebote oft sehr teuer, OEM will auch nicht scannen.
- Problem: kostenfreier Referenzcode von Hardware-Herstellern
  - kostenfrei = Haftungsausschluss, OSS Informationen oft lückenhaft

Werkzeuge und Prozesse beim OSS Management: Verträge 2/2

- Verträge mit Kunden
  - OSS vs. Gewährleistung
  - OSS vs. Verpflichtung zur Fehlerbeseitigung
  - Verträge mit OEM
- Standardverträge/-dokumente
  - EULA, Verkaufs-AGB
  - Entwicklungs-AGB, z.B. Prof. Services
  - Reseller-Verträge, OEM Verträge
- Individuelle Lösungen
  - Professional Services auf Grundlageindividueller Verträge
  - Öffentliche Hand / EVB-IT
    - EVB-IT sind nicht wirklich OSS-kompatibel

Article 8 - Open-Source-Software

8.1 → Licensor represents, warrants and guarantees that, unless specified in **Attachment 6**, the Licensed Software does not contain any Open Source Software, as defined in this Article below, or any shareware or freeware components.

→ As used herein, the term "Open Source Software" means any software that is licensed royalty-free (i.e., fees for exercising the licensed rights are prohibited, whereas fees for reimbursement of costs incurred by licensor are generally permitted) under any license terms or other contract terms ("Open License Terms") which require, as a condition of use, modification and/or distribution of such software and/or any other software incorporated into, derived from or distributed with such software ("Derivative Software"), either of the following:

8.1.1 → that the source code of such software and/or any Derivative Software be made available to third parties;

8.1.2 → that permission for creating derivative works of such software and/or any Derivative Software be granted to third parties.

By means of example and without limitation, Open License Terms include the following licenses or distribution models: the Apache License, a BSD-like License, the GNU General Public License (GPL), the GNU Lesser or Library GPL (LGPL).

8.2 → The Licensed Software contains only the following Open Source Software as specified in **Attachment 6**.

8.3 → Licensor represents, warrants and guarantees that:

8.3.1 → Without prior written permission by SEN the Licensed Software does not contain Open Source Software, which is licensed under the GPL;

8.3.2 → the Open Source Software listed in **Attachment 6** is the only software contained in the Licensed Software which falls under the above definition of Open Source Software;

8.3.3 → all of the license obligations applicable to the listed (completely fulfilled by Licensor;

8.3.4 → Licensor has provided SEN with all required license ter and build scripts, in order to enable SEN, its Affiliated customers to create an executable version of such Open

Licensor shall inform SEN promptly in writing if new or other Ope

24.6.2 → use the Software for the purpose of developing, or having developed any Derivative Work of the Software. In the event the Customer creates any Derivative Work of the Software (other than modifications or alterations to FOSS), all rights, title and interest in and to such Derivative Work shall vest solely in the Supplier.

24.7 → The Software may contain third party software, including FOSS. No additional license fee is charged to the Customer for the use of such third party software. The Customer acknowledges that third party software may be subject to specific license terms of the respective author or licensor and accepts the license conditions for such third party software which can be provided upon Customer's request. Licence conditions for third party software and for end user devices can be downloaded at [___]. Where a third party software License provides for the provision of the respective source code, Supplier shall make this source code available at the Customer's request.

Bei Verwendung der EVB-IT bzw. BVB[9] ist im Einzelnen zu prüfen, ob die Vertragsbestimmungen im Einklang mit den jeweils maßgeblichen OSS-Lizenzen stehen. Eine unveränderte Heranziehung der Standardverträge kann mitunter problematisch sein. Dies soll an zwei Beispielen näher dargestellt werden:

Die EVB-IT Überlassung Typ A und Typ B können bei der Beschaffung von Standard-Open-Source-Software von einem Zwischenhändler nicht ohne Weiteres benutzt werden. Die genannten Vertragswerke sehen eine Rechtseinräumung durch den Auftragnehmer (das heißt den Zwischenhändler) vor; dies kommt beim Erwerb von OSS in aller Regel aber nicht in Frage, da der Zwischenhändler keine entsprechenden Rechte innehat und deswegen auch keine Nutzungsrechte einräumen kann. Die Klauseln über die Nutzungsrechtseinräumung müssten hier also gestrichen werden, um das Formular benutzen zu können.

OSB Open Source Business ALLIANCE INFORMATION

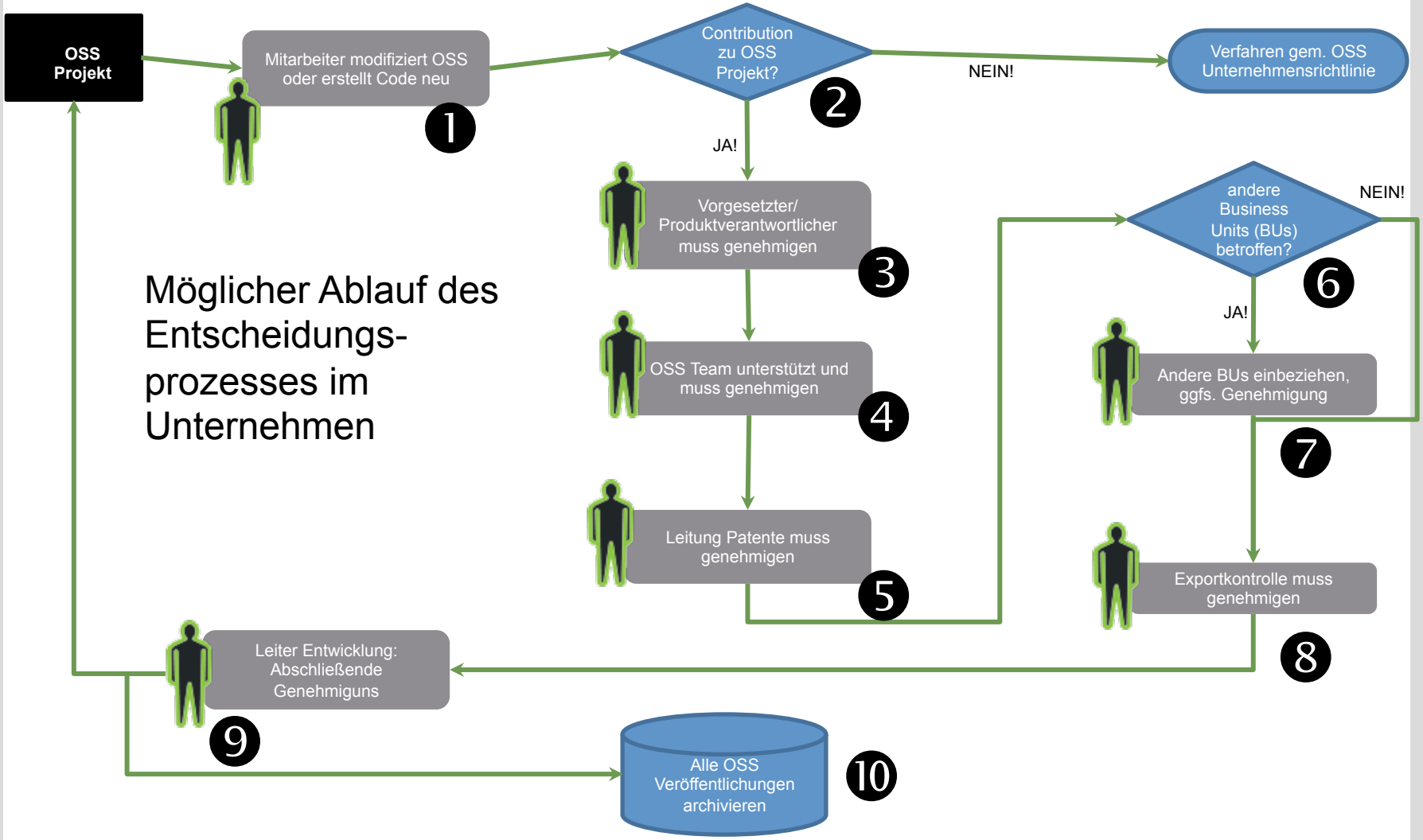
EVB-IT

HANDREICHUNGEN ZUR NUTZUNG DER EVB-IT BEIM EINSATZ VON OPEN SOURCE SOFTWARE
Beschaffung von Open Source Software für Behörden und öffentliche Einrichtungen

Werkzeuge und Prozesse beim OSS Management: Mitwirkung bei OSS Projekten (Contribution) 1/2

- „Contribution“ = aktive/passive Mitwirkung an OSS Projekt
  - OSS wird modifiziert oder Code soll als OSS veröffentlicht werden
- Was genau wird veröffentlicht?
  - Datenerhebung mittels OSS Contribution Form
- Rechtliche Vorgaben des Projekts beachten
  - „Contribution Agreements“, Standard-OSS Lizenz
- Bei Eigenveröffentlichung/Lizenzwahl: welche OSS Lizenz?
- Stakeholder im Unternehmen
  - Produktmanager, andere (Produkt-)Teams bzw. Business Units
  - Patentabteilung, Leitung der Produktentwicklung
- Exportkontrollprüfung vor Veröffentlichung!
- Dokumentation/Archivierung
  - was wurde wann unter welcher Lizenz veröffentlicht
- Ggfs. Unternehmensrichtlinie

Werkzeuge und Prozesse beim OSS Management: Mitwirkung bei OSS Projekten (Contribution) 2/2



Möglicher Ablauf des Entscheidungs-prozesses im Unternehmen

Werkzeuge und Prozesse beim OSS Management: Unternehmensrichtlinie zum Umgang mit OSS

Unternehmensrichtlinie zu OSS:

- Dokumentiert, welche strategischen Entscheidungen das Unternehmen in Bezug auf OSS getroffen hat
- Institutionen festlegen: OSS Team, OSS Agent, Mailbox,
- (Pflicht) Werkzeuge definieren: Scanning Tool, Fragebogen, Datenbank
- Beschreibt:
  - das Verfahren zum Umgang mit OSS
  - welche Lizenzen im Unternehmen OK sind und welche nicht
  - wie etwas als OSS veröffentlicht wird
  - wie Lieferanten einzubinden sind

- Zeigt Möglichkeiten auf, drohende Lizenzkonflikte zu vermeiden
  - z.B. wie sollten Lizenzen wie die LGPL in Produkte integriert werden?

Schlussfolgerungen und Thesen

Schlussfolgerungen und Thesen 1/3

- OSS ist und bleibt ein fester, dauerhafter Teil der Softwarewelt
- OSS kostet vielleicht nichts, ist aber nicht kostenlos
- OSS Management ist ein Prozess, kein Projekt

- Rechtsprechung erkennt OSS Lizenzen grds. an
  - OSS Gerichtsverfahren (noch) selten, Zeit nutzen!
  - Kläger sind meist „Überzeugungstäter“, noch keine Abmahnindustrie
- OSS ist fester Teil der Due Diligence Prüfung bei M&A
- Fehlende OSS Compliance ist ein ernstes Risiko für alle Unternehmen, deren Produkte Software enthalten

- Beobachtung: bei Unternehmen werden extrem restriktive Lizenzen (z.B. xGPLv3) zunehmend unbeliebt
  - Unternehmen, die kommerziell getrieben OSS veröffentlichen, tendieren immer öfter zu liberalen Lizenzen (z.B. Apache, BSD)

Schlussfolgerungen und Thesen 2/3

- OSS Management erfordert die Zusammenarbeit von Experten aus vielen Unternehmensbereichen
- Unternehmen sollten sich entscheiden,
  - welche OSS Lizenzen akzeptabel sind,
  - welche OSS Lizenzen für sie unvermeidlich sind
  - wie die eigene IP trotz Nutzung von OSS geschützt werden kann, z.B. um Infektionen durch Copyleft Effekt vermeiden
- Entscheidungen über den Einsatz von OSS können langfristige Folgen haben, die später nur schwer rückgängig zu machen sind
  - z.B. Entscheidung, OSS mit xGPL Lizenzen zu benutzen

- OSS Management benötigt die richtigen Werkzeuge:
  - OSS Scanning Tool, Code Repository, Lizenzdatenbank
  - Verträge: Lieferanten und Auftragsentwickler müssen in den eigenen OSS Managementprozess eingebunden werden

Schlussfolgerungen und Thesen 3/3

- Es muss klar sein, welcher Code in welchem Produkt steckt
- Scannen, und nochmal scannen. So früh wie möglich.
- Mitarbeiter schulen, insbes. Entwickler

- Unternehmen sollten klare Regeln haben, wer Aussagen zu OSS gegenüber Kunden, Vertriebspartnern, Verbänden trifft

- Entscheiden und überprüfen, wie die in den Produkten enthaltene OSS ausgeliefert oder veröffentlicht wird
- Einhaltung der OSS Management Prozesse auditieren
- Alle Entscheidungen zum OSS Management dokumentieren
- Unternehmensrichtlinie zum OSS Management verabschieden

Vielen Dank!

Udo Steger
Rechtsanwalt / Partner

Aderhold Rechtsanwaltsgesellschaft mbH
Wagmüllerstraße 23
80538 München
Tel.: +49 (89) 306683-207
E-Mail: u.steger@aderhold-legal.de

Follow me:

@LinkedIn: https://de.linkedin.com/in/usteger
@XING: https://www.xing.com/profile/Udo_Steger
@Twitter: @usteger
@Blog: www.paytechlaw.com