Open Source License Compliance and Ory Open Source

Prof. Dr. Dirk Riehle

Univ. Erlangen, Bayave GmbH

2021-10-29 @ Ory Summit

Open Source Software

Open source software

- Software given to you under an open source license

Open source software license

- **Rights grant**
  - Free use, source code, right to modify, right to pass on
- **Obligations**
  - Attribution, license texts, source code provision, etc.
- **Prohibitions**
  - No endorsement, no trademark use, etc.

Benefits of Using Open Source Software

High quality software (almost) for free

No vendor lock-in, leads to

- Improved cost predictability
- Lower operational risk
- Ability to help yourself if needed

(Often) instant standards compatibility

Use-Cases of Open Source Software

In-house use

- All the rights, few to **none of the obligations**

Distribution (use in products) to third parties

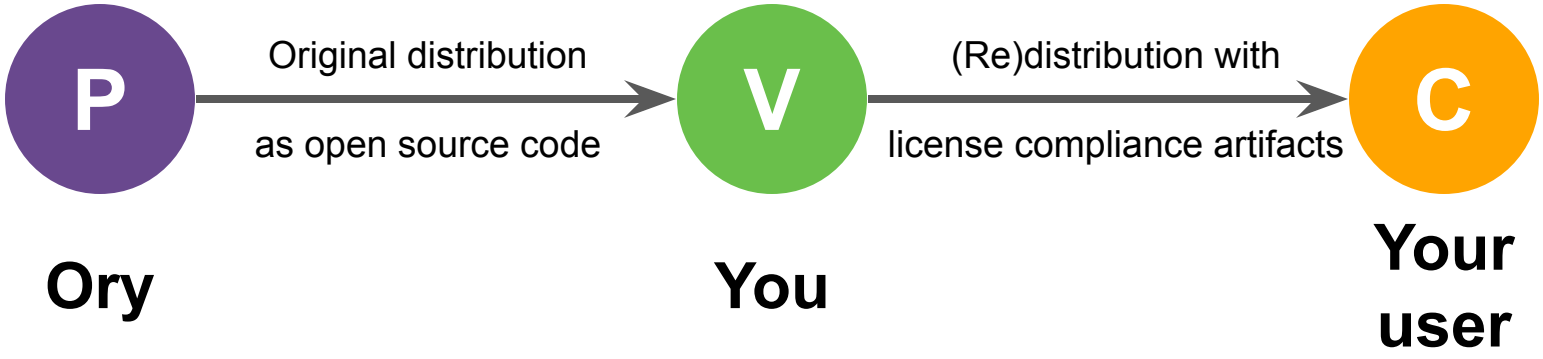
- All the rights, most or **all of the obligations**

Using Open Source in Products and Applications

Giving binary code to third parties (customers) constitutes distribution

P = Original open source programmer
V = Vendor (of any kind, IT or non-IT)
C = Vendor's customer

Using Ory Open Source in Products and Applications



P = Original open source programmer
V = Vendor (of any kind, IT or non-IT)
C = Vendor's customer

Vendor Concerns (Your Concerns)

Can I use Ory Open Source or do I infringe on somebody's rights?

How do I use Ory Open Source in a license-compliant way?

Open Source Audit of Ory Open Source [1] [2]

Using FOSSOLOGY, we identified the following licenses in Ory Open Source

	kratos	hydra	keto	oath-keeper
Apache-2.0	4	116	151	204
MIT	9	9	12	16
CC-BY-2.5	-	-	7	7
Dual license: Apache-2.0 or EPL-1.0	-	-	1	1
LGPL-2.1-or-later	-	-	20	20
MPL-2.0	-	-	4	4
Dual license: Apache 2.0 or LGPL-3.0-or-later	-	-	9	9
Dual license: CDDL or GPL-2.0-only with Classpath-exception-2.0			1	1

[1] Please see the legal notices at the end of this document
[2] All licenses in gray rows were found in swagger-codegen-cli-2.2.3.jar

Open Source License Categories

Permissive licenses

- Example licenses: **MIT, BSD-3-Clause, Apache-2.0, …**

Weak copyleft licenses

- Examples: **LGPL-2.1-or-later, MPL-1.1, …**

Strong copyleft licenses

- Examples: **GPL-2.0-only, AGPL-3.0-or-later**

What Constitutes Binary Distribution?

Distribution is defined by every license itself (read the license!)

Interpreting the Apache-2.0 license, the following constitutes distribution

- Giving users / customers a compiled binary of the open source code
- Providing Javascript to users / customers that runs in their browser
- Making container images available with the binary inside

The Apache-2.0 license does not consider cloud service provision distribution

In case of distribution, you have to fulfill the complete set of license obligations

Permissive License Obligations

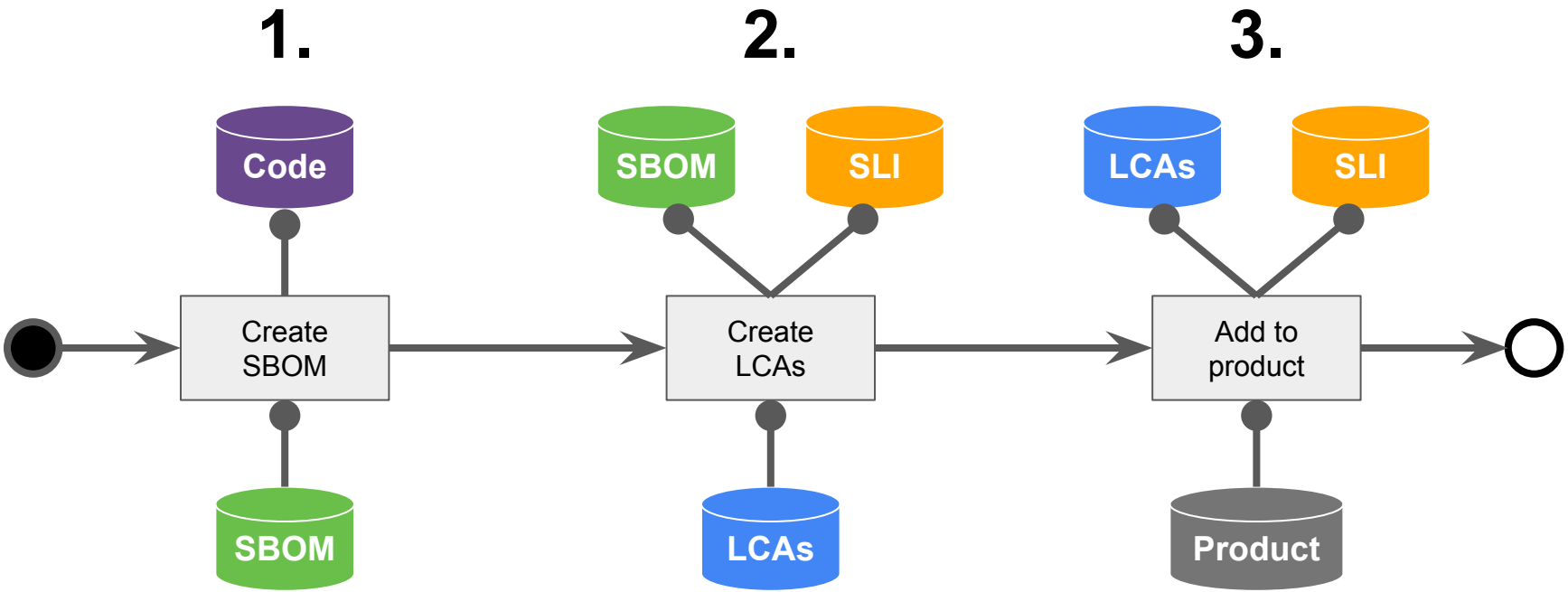
Provision of **legal notices**, assembled from

- Copyright notices
- License texts
- Change notices
- ...

Index

Contents

License Compliant Delivery Workflow



SBOM = Software bill of materials
SLI = Standard(ized) license interpretation
LCAs = License compliance artifacts (legal notices)

Open Source Program Office

Good open source governance is state of the art

- Makes the CEO responsible (liability, “Geschäftsführerhaftung”)

Open source program office

- People / org. unit with mandate to define open source policies

Open source program office responsibilities

- Inbound and outbound governance
- Education and marketing, inside and outside company
- Provision and operation of key workflows and artifacts

What Do You Need to Get Started?

1. License compliant delivery capability
2. Open source program office capability
3. Standardized license interpretation
4. Your first open source inventory

All available through Bayave GmbH

Thank You! Any Questions?

Prof. Dr. Dirk Riehle, M.B.A.

dirk.riehle@fau.de, https://oss.cs.fau.de

dirk.riehle@bayave.com, https://bayave.com

dirk@riehle.org, https://dirkriehle.com

Twitter: @dirkriehle

Legal Notices 1 / 2

Notice to readers

This document has been created with appropriate diligence. The user is solely responsible for the use of this document. Bayave GmbH is not a law firm and the author(s) are not lawyers. This document does not provide legal advice. The recipient of this document should consult their own legal counsel when applying this information. Best practices change over time and the reader should check whether the described practices are still considered valid.

Disclaimer of warranty

Unless required by applicable law or agreed to in writing, Bayave GmbH provides this document without warranties or conditions of any kind, either express or implied, including, without limitation, any warranties or conditions of fitness for a particular purpose. The recipient is solely responsible for determining the appropriateness of using this document and assumes any risks associated with it.

Limitation of warranty

In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall Bayave GmbH be liable to the recipient of this document for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of using this document or out of the inability to use this document (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if Bayave GmbH has been advised of the possibility of such damages.

Legal Notices 2 / 2

License

- Licensed under the CC BY 4.0 International license

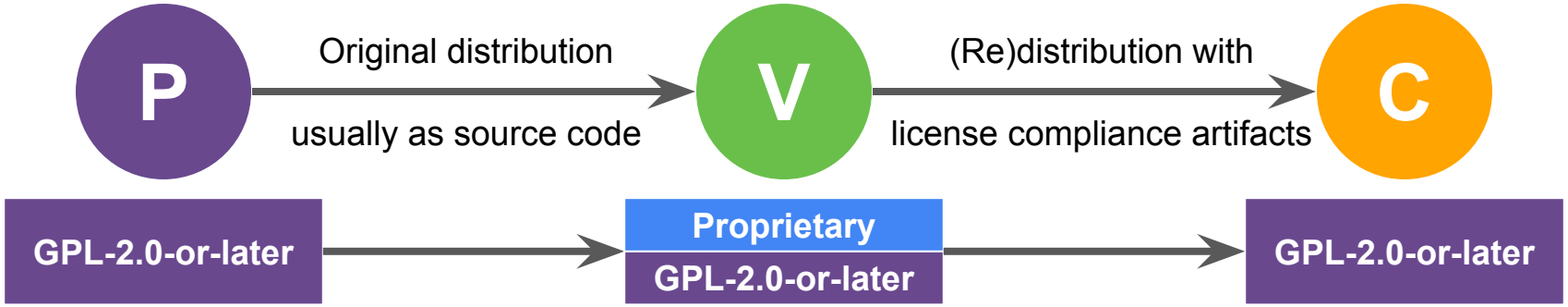
Copyright

- © Copyright 2021 Bayave GmbH, some rights reserved

Copyleft (License) Obligation

Copyleft

1. Obligation that requires provision of complete and corresponding source code
2. Namesake for a whole open source license category



Copyright Trolls (“Monetizer”)

Review products for license violation

Require fix of violation through support

- If ignored, send cease and desist letter (“Strafbewehrte Unterlassungserklärung”)
- Ask for compensation for enforcement work

If cease and desist letter was signed

- Come back with other violations, ask for penalty
- Threaten lawsuit, follow through

Typically settle out-of-court

Copyright Enforcers (“Philosophers”)

Become a Supporter! | Donate | News | Blog | Projects | Copyleft Compliance | NPOAcct | Sponsors | About

VMware Suit Concludes in Germany

VMware Announces Plans to Remove Non-complying Code, Hellwig Decides Not to Appeal

April 2, 2019

Today, Christoph Hellwig announced the conclusion of his case against VMware in Germany. The Hamburg Higher Regional Court affirmed the lower court's decision, which dismissed the case on purely procedural grounds; they did not address the main question of the case. (The February 28th decision can be found here.) Hellwig has decided with his legal counsel, Till Jaeger, and after conferring with Conservancy, to not appeal the case further in German courts.

“The subject of the complaint I filed was the question of whether the distribution of the software Hypervisor vSphere VMware ESXi 5.5.0 software is copyright infringement because VMware has no permission to create a derivative work from Linux under the GNU General Public License (GPL)” says Hellwig. Both courts declined to consider that essential question.

VMware, in their news item about the decision by the Court, announced that they will finally remove vmklinux from vSphere. Both Hellwig and Conservancy had asked VMware to remove the Linux code from VMware's proprietary kernel many times. While the preferred form of GPL compliance is release of the entire work under the terms of the GPL, a common alternative is to merely remove the GPL'd code from the product. VMware chose the latter method to comply.

“VMware knew what they were doing was wrong, but continued to generate revenue by infringing copyrights in Linux, while only slowly working toward non-infringement.” explained Karen Sandler, Conservancy's Executive Director. She added: “As we have always said, we simply want companies to follow the rules and do the right thing when they incorporate GPL'd code into their products.” Hellwig added: “When VMware takes this action, they will finally comply with the GPL. Reaching this goal has cost me a lot of time and energy in recent years.”