License-Compliant Delivery Handbook Demonstration

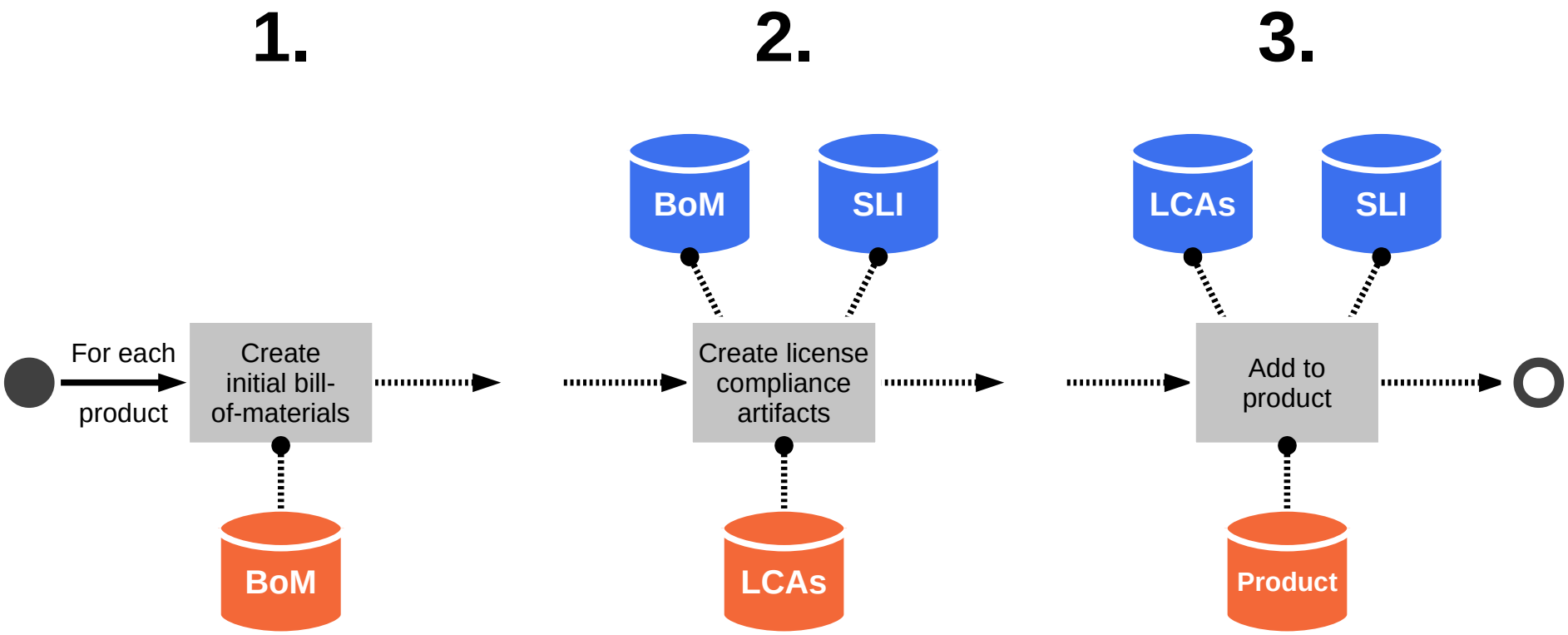
Prof. Dr. Dirk Riehle

Bayave GmbH / Universität Erlangen

Problem (How to Fulfill License Obligations)

- (Nearly) all software products contain open source code
  - Open source code comes with license obligations that need to be fulfilled
  - Not satisfying license obligations may lead to an immediate sales stop
- Fulfilling license obligations is hard!
  - There are many different licenses, hard to understand, often outdated
  - Possibly a lot of open source in your products that needs compliance
- **Open source program offices need a standardized license interpretation**
  - Explains licenses and guides developers in fulfilling license obligations
  - Helps company ensure license-compliant delivery

License-Compliant Delivery Process



BoM = bill of materials
SLI = standardized license interpretation
LCA = license compliance artifacts

Step 1: Create Initial Bill-of-Materials (“Stückliste”)

- See our service offering for license and / or code scanning of existing code bases

Step 2: Create Artifacts and Establish Processes

- For each distinct piece of open source code
  - Determine the open source license
  - From software use-case, determine distribution-case
    - Unchanged binary
    - Modified binary
    - Source code
  - From license and and distribution-case, determine obligations
  - Fulfill obligations
    - Create license compliance artifacts
    - Establish processes
  - Bundle artifacts

Step 3: Add to Product (in a License-Compliant Way)

- Artifact organization and presentation
  - Files
  - User interface
- Distribution mode
  - Server application
  - Web application
  - Embedded device

Bayave’s

license-compliant delivery handbook

provides a

---

standardized license interpretation

for step 2 (creation of LCAs) and

for step 3 (license-compliant delivery)

Handbook: License Overview Example (Unchanged Binary Distribution)

	Apache-2.0	Artistic-1.0	0BSD	BSD-1-Clause	BSD-2-Clause	BSD-3-Clause	EPL-1.0	AGPL-3.0-or-later	GPL-2.0-or-later	GPL-3.0-or-later	LGPL-2.1-or-later	LGPL-3.0-or-later	Libpng	MIT	MPL-1.1	MPL-2.0	MS-PL	Python-2.0	Zlib
Legal notices																			
Provide license text	1			1	1	1		1	1	1	1	1		1		1	1	1	
Provide additional terms (GPLv3+)								1		1		1							
Provide disclaimer		1		1	1	1	1		1		1								
Provide copyright notices	1	1		1	1	1		1	1	1	1	1		1			1	1	
Provide existing notices	1							1	1	1	1	1			1		1		
Document third-party dependencie															1				
Source code																			
Provide link to original source code		1																	
Apply source code notice (MPL-1.1																			
Provide corresponding source cod		1					1	1	1	1	1	1				1			
Provide installation information (GI								1		1		1							
Provide change notices							1												
Provide change report																			
Engineering																			
Conditionally display notices (GPL																			
Enable modification (LGPL-2.1)																			
Liabilities																			
Provide indemnification	1						1									1			

Handbook: License Interpretation Example

- License interpretation
  - Broken down by distribution-case
- Currently 19 licenses
  - Can be extended for new licenses

SPDX identifier	Apache-2.0
License information	https://spdx.org/licenses/Apache-2.0.html
Unchanged binary distribution obligations	1. Provide license text 2. Provide copyright notices 3. Provide existing notices (file name is "NOTICE") 4. Provide indemnification
Derivative binary distribution obligations	1. Provide license text 2. Provide copyright notices 3. Provide existing notices (file name is "NOTICE") 4. Provide change notices, if any 5. Provide indemnification
Source code distribution obligations	1. Provide license text 2. Provide copyright notices 3. Provide existing notices (file name is "NOTICE") 4. Provide corresponding source code 5. Provide change notices, if any 6. Provide indemnification

Handbook: Obligations Step-by-step Example

- Obligation definition
  - Explains the obligation
- Obligation fulfillment
  - Step-by-step instructions
- Currently 15 obligations
  - Standardized! One set of step-by-step instructions capturing several licenses

5.1 Provide license text

To fulfill this obligation, you must provide the license text of the open source code to the recipient of the distribution.

5.1.1 Steps to take

Take the following steps to provide license text:

1. Retrieve the license text from the original open source code and copy it to the proper place in the distribution
   a. Do not use or link to an official version on the web; use the version that comes with the open source code

You can typically find the license text in the root directory of the open source code you are using in a file called “LICENSE” or “COPYING”.

5.1.2 Example license text

The following text is a copy of the MIT license template. It becomes a full-fledged license if its user, the copyright holder, adjusts the copyright statement with his or her name and the year.

```
Copyright <YEAR> <COPYRIGHT HOLDER>

Permission is hereby granted, free of charge, to any person obtaining a copy of this
software and associated documentation files (the "Software"), to deal in the Software
without restriction, including without limitation the rights to use, copy, modify, merge,
publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons
to whom the Software is furnished to do so, subject to the following conditions:
```

Handbook: Process Obligation Example

- Some obligations require processes
  - Also effects delivery

5.15 Provide indemnification[8]

To fulfill this obligation, you need to

- indemnify any contributors to code you distributed and to
- put the associated processes of legal and organizational support in place.

Some licenses require that you indemnify contributors to the code you are distributing. This obligation is not complied with by providing notices to recipients; rather it requires that you have a process in place for providing indemnification and handling any corresponding requests.

To fulfill this obligation, you need to appropriately react to requests for indemnification by contributors against which claims have been brought forward by a third party you provided with a distribution.

Appropriate reaction is a process that may include, but is not limited to:

- Receiving and speedily reacting to notifications about claims
- Collaborating with the contributor to react to third-party claims
- Participating in the defense and settlement of any such claims

There are no hard and fast rules on how to do this; this is a question of setting-up a process that does not fail. One best practice is to clearly name a competent point of contact at the company at the beginning of the legal notices (license compliance artifacts). This point of contact should

- understand the significance of any incoming legal help request and
- be stable in case people change positions or leave.

Regular product support might not know how to handle incoming indemnification requests and might choose to ignore them; an open source program office, if it exists, is typically a better choice.

Please consult your legal counsel on how to establish such a process.

Underlying Methodology

- Years of research into license interpretation using
  - Original license texts
  - Original license owner explanations
  - Legal commentary and court findings
  - Community discussions and consensus
- Combined with engineering expertise
- Refined by practical use through customers

The License-Compliant Delivery Handbook

- The purchase of the handbook includes
  - Perpetual usage license
  - One year of updates
  - 8h of support
- Handbook options and add-ons
  - Scope and number of users
  - Added years of updates
  - Additional support

Thank you! Questions?

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

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

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