Curation of ORT output –

useful features from the perspective of FOSS license compliance

Dr. Till Jaeger | JBB Rechtsanwälte

ORT Community Days 2024, Berlin



FOSS License Compliance

- Common obligations
- Particularities of binary distribution
- Dealing with scan results

SBOM

- Legal Provisions (Cyber Resilience Act)
- Content of an SBOM

License Scanning and Curation

- Main licenses and internal licenses.
- Dual licensing
- (The issue of) Template Texts
- Different types of copyrightable works
- License compatibility
- OSSelot integration

FOSS License Compliance

FOSS LICENSE COMPLIANCE: Common Obligations



Include / Retain copyright notices



Include / Retain license text



Provide source code / offer to provide (access to) source code



Mark modifications, including date of modification



Provide NOTICE file



Acknowledge origin

FOSS LICENSE COMPLIANCE Particularities of Binary Distribution

- Source Code distribution vs Binary Distribution
 - Not human readable
 - License texts & copyright notices get lost / cannot be perceived
- Many licenses have special provisions for binary distribution
- Solution: prepare "Compulsory Statement Document"/"Disclaimer"/"FOSS Documentation"/"Disclosure Document" etc.
 - include all license texts
 - include all copyright notices and acknowledgments
 - include license election choices
 - include written offer for source code
 - include disclaimer

FOSS LICENSE COMPLIANCE: Common Obligations

E.g. Apache-2.0

- 4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:
 - (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
 - (b) You must cause any modified files to carry prominent notices stating that You changed the files; and
 - (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
 - (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one

FOSS LICENSE COMPLIANCE: Common Obligations

E.g. Apache-2.0

```
USE CASE Source code delivery
      YOU MUST Provide License text

☑ IF Software modification

           YOU MUST Provide Modification notice
           YOU MUST Forward Copyright notices
           YOU MUST Forward Patent notices Ref.
           YOU MUST Forward Trademark notices
                                                 Ref.
           YOU MUST Forward Attribution notices
                                                  Ref.

☑ IF Work Includes File "NOTICE"

                YOU MUST Delete Irrelevant parts
                                                 Ref.
                         Ref.
              EITHER
                     YOU MUST Provide File "NOTICE"
              ✓ OR
                     YOU MUST Provide File "NOTICE" In Source code
              OR
                     YOU MUST Provide File "NOTICE" In Documentation
                                                                      Ref.
              OR
                     YOU MUST Display File "NOTICE"
                                                     Ref.

☑ IF Service offerings

                           Ref.
           YOU MUST Indemnify Other contributors
                                                  Ref.
```

- 4. Redistribution. You may reproduce and distribution work or Derivative Works thereof in any medium modifications, and in Source or Object form, meet the following conditions:
 - (a) You must give any other recipients of the Derivative Works a copy of this License;
 - (b) You must cause any modified files to carry stating that You changed the files; and
 - (c) You must retain, in the Source form of any that You distribute, all copyright, patent attribution notices from the Source form excluding those notices that do not pertain the Derivative Works; and
 - (d) If the Work includes a "NOTICE" text file distribution, then any Derivative Works the include a readable copy of the attribution within such NOTICE file, excluding those in pertain to any part of the Derivative World

FOSS LICENSE COMPLIANCE Dealing with scan results

- All license texts to be extracted
 - Correct detection of licenses
 - Correction of false positives
- Extraction of NOTICE files on Apache-2.0 projects

- All Copyright notices to be extracted
 - Authors ≠ Copyright owners
 - Mapping copyright notices and licenses

FOSS LICENSE COMPLIANCE Dealing with scan results

- Obligations in FOSS licenses are triggered by "distribution"
- Which code is distributed?

Filtering files helps to reduce workload and applicable licenses



Legal Provisions for SBOM: Cyber Resilience Act (CRA)

- EU regulation addresses cyber security / vulnerabilities of software
- Measures include requirement of Software Bill of Materials (SBOM)
 - transparency
 - accountability
- CRA does not define contents of SBOM
 - Name and version of the software component
 - Link to download ressource
 - License in SPDX format
 - What else?

Legal Provisions for SBOM: Cyber Resilience Act (CRA)

Federal Office for Information Security (BSI) – technical directive published

- Technische Richtlinie TR-03183
 - Dependencies
 - Hash
 - Information about producer of the SBOM (URI, i.e. email, time stamp)
 - Name of producer -> name and URI of FOSS project?



Main license and "internal" licenses

- The main license is usually in a "COPYING" or "LICENSE" file at the top level of a source tree
- Individual folders or even single files may have code from other projects under the others project's license
- Such internal licenses are not void but apply next to the main license
- SPDX: Apache-2.0 AND MIT AND BSD-3-Clause
- Curation: deleting false positives and licenses which do not apply
- Curation: helpful to have easy access to the relevant source code for control

Dual Licensing

- Some files or even components provide for two or more licenses among which licensee can elect one
- SPDX: Apache-2.0 OR UPL-1.0
- Choice may be important for license compatibility
- Curation needed to elect one license.
- Control of concrete text

```
Code Blame 85 lines (64 loc) · 12.9 KB

1 Copyright (c) 2016, 2020, Oracle and/or its affiliates. All rights reserved.
2 This software is dual-licensed to you under the Universal Permissive License (UPL) 1.0 as shown at https://oss.oracle.com/licenses/upl or Apache License 2.0 as shown at http://www.apache.org/licenses/LICENSE-2.0. You may choose either license.
```

- Template licenses and individual licenses
 - The Apache-2.0 looks always the same (but be aware of "Frankenstein licenses")
 - BSD-3-Clause licenses look mostly different
 - Curation: individual text to be added

Copyright (c) <year> <owner>.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- 3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. e.g. "Google, Inc.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

- Source code packages may contain different copyrightable works
 - Computer programs ("functional code")
 - Fonts (may be protected by design law and/or as computer programs)
 - Icons (e.g. .png, .jpg files)
 - Logos (may be protected as trademarks)
 - Documentation (e.g. text files)
 - Specifications (may have specific licenses which are related to the implementation of the standard and/or sample code)
 - Curation: what is really distributed? Knowing file type and corresponding license
 - Curation: filter out works that are not distributed

- Sourcecode files may refer to URLs
 - URL still available?
 - Does the URL contain the license text or is further research necessary?
 - Typical example: Unicode Terms of Use

Source: https://www.unicode.org/Public/12.0.0/ucd/EmojiSources.txt

| Subservineire Sussess | | | | | | | | |
|--|---|---|---|---|--|---|---|--|
| 523 523 539 530 ook | | | 160 | Sec. | | No. 3 3 No. We 3 No. 100 Day. Day. Day. Day. Day. | | No. |
| ELUVARION trail trail trail | 1 | | 1 | | | m m m m m m m m m m m m m m m m m m m m m | 1 | 1 |
| | No. No. <td> No. No.</td> <td> No. No.</td> <td> Sec. Sec. </td> <td> </td> <td>No. 100 101 101 101 101 101 101 101 101 10</td> <td>Ten. Men. Men. Men. Men. Men. Men. Men. M</td> <td> N N N N N N N N N N</td> | No. | No. | Sec. | | No. 100 101 101 101 101 101 101 101 101 10 | Ten. Men. Men. Men. Men. Men. Men. Men. M | N N N N N N N N N N |
| migg B_LCause B_LCause B_LCause Biggsi | 6 70 80 </td <td>No. One One<td>No. No. No.<td> Sec. Sec. </td><td> </td><td>Sec Sec Sec<td>Ten Des Des Des Des Des Des Des Des Des Des</td><td>8 10 10 10 10 10 10 10 10 10 10 10 10 10</td></td></td></td> | No. One One <td>No. No. No.<td> Sec. Sec. </td><td> </td><td>Sec Sec Sec<td>Ten Des Des Des Des Des Des Des Des Des Des</td><td>8 10 10 10 10 10 10 10 10 10 10 10 10 10</td></td></td> | No. No. <td> Sec. Sec. </td> <td> </td> <td>Sec Sec Sec<td>Ten Des Des Des Des Des Des Des Des Des Des</td><td>8 10 10 10 10 10 10 10 10 10 10 10 10 10</td></td> | Sec. | | Sec Sec <td>Ten Des Des Des Des Des Des Des Des Des Des</td> <td>8 10 10 10 10 10 10 10 10 10 10 10 10 10</td> | Ten Des | 8 10 10 10 10 10 10 10 10 10 10 10 10 10 |
| 0.3 Claine 0.3 Claine Open HR 0.4 Claine 0.4 Claine UC | No. | No. Unit | 15 | Sec. | 6 6 6 6 6 6 6 7 6 7 6 7 | Mr. Va. Dr. Mr. Mr. <td>No. Unit Unit</td> <td> No No No No No No No No</td> | No. Unit | No No No No No No No No |
| Elimpophia ELIV MELIVI | No | No. On. On. <td> 10</td> <td></td> <td>No. On. On.<td>the time that the time the time that the time the time the</td><td></td><td> No No No No No No No No</td></td> | 10 | | No. On. On. <td>the time that the time the time that the time the time the</td> <td></td> <td> No No No No No No No No</td> | the time that the time the time that the time the time the | | No No No No No No No No |
| 27. 27. 27. | No. | | No. | Dec Dec | | Max Max <td> No. No.</td> <td> No No No No No No No No</td> | No. | No No No No No No No No |
| π. « | 1 | | | | 1 | No. 200 Sec 50 S | 1 | 1 |
| 120 120 121 121 121 | No. | | | 2 2 New York Yes New York Yes Yes New York | 1 | No. No. <td></td> <td> No. No.</td> | | No. |
| 01.12 02 04 04 | | | Ten | Text | Max San San <td>Sec. Sec. <th< td=""><td> </td><td> 1</td></th<></td> | Sec. Sec. <th< td=""><td> </td><td> 1</td></th<> | | 1 |
| 04400 M | No. No. <td> No. No.</td> <td> Ten</td> <td>7 7 8s 7s 1s 2s 2s</td> <td> 1</td> <td>On 7 2 8 1 8 8 1 8</td> <td>Inc. Inc. <th< td=""><td> No No No No No No No No</td></th<></td> | No. | Ten | 7 7 8s 7s 1s 2s | 1 | On 7 2 8 1 8 8 1 8 | Inc. Inc. <th< td=""><td> No No No No No No No No</td></th<> | No No No No No No No No |
| LLAndr State Compage you will be a second to the second to | 7 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 | No. 2 No. 1 No. No. No. 2 No. No. 1 No. No. 2 No. No. No. 2 No. | | 7 7 Nex Cop. See Mes Nex Mes Mes Mes Mes | | | | |
| Liver by | 7 1 1 2 200 Corp. 150 Min. 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 | | | | | | | 1 |
| | No. Dec. | No. No. <td>Re Ver Ver</td> <td> Max</td> <td> </td> <td> Tell Tell </td> <td>Rec. Dec. <th< td=""><td>9 No. 10 No. 10</td></th<></td> | Re Ver | Max | | Tell | Rec. Dec. Dec. <th< td=""><td>9 No. 10 No. 10</td></th<> | 9 No. 10 |
| c draid draid draid draid draid draid draid draid draid draid | No. No. No. Line Line No. No. Line No. No.< | No. | No. | Sec | No. One One <td>No. 2 7 No. 20 2 Tex No. No. No. No. No. No. No.</td> <td>No. No. No.<td> No No No No No No No No</td></td> | No. 2 7 No. 20 2 Tex No. No. No. No. No. No. No. | No. No. <td> No No No No No No No No</td> | No No No No No No No No |
| ALLINES ALLINES ALLINES ALLINES | 1 | | | | 5 | The Control of the Co | 1 1 1 1 1 1 1 1 1 1 | a to |
| regin 2.0 dil managan 2001,01 | 10 10 10 10 10 10 10 10 | | 10: 10: 10: 10: 10: 10: 10: 10: 10: 10: | | | Dec. No. No. No. No. No. No. No. No. No. No | | No No No No No No No No |
| grant la | | | | | | Max Max <td>Des. Des. <th< td=""><td> </td></th<></td> | Des. Des. <th< td=""><td> </td></th<> | |
| | 7 1 7 1 8 1 8 1 8 1 7 7 7 7 7 7 7 7 7 7 | 7 | 7 2 80 80 80 80 1 2 80 80 80 80 80 80 80 80 80 80 80 80 80 | | | | | 9 10 2 2 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 |
| 195_10 196_10 196_10 | | | 1 | 1 | | 1 1 2 2 3 1 2 3 3 3 3 3 3 3 3 3 | | 1 |
| 2014 2014 | No. | No. | No. | | 10 10 10 10 10 10 10 10 | | No. 104 | No No No No No No No No |
| erati | 10 | | 10 | | 1 | No. No. Exp. E | | No No No No No No No No |
| LEAD IN THE PROPERTY IN THE PR | 15 | | 10 | | | | | |
| 1000 M 100 M 1000 M 1000 M 1000 M | ten fine the New Mar Mar New York Ten Sen 1 | No. On. On. <td> No. No.</td> <td>Des Nes Nes See See See See See Nes Nes Nes Nes</td> <td>un de de de de de de de de de de</td> <td>No. 100 100 100 100 100 100 100 100 100 10</td> <td>Bit Bit Bit<td> Reg Reg</td></td> | No. | Des Nes Nes See See See See See Nes Nes Nes Nes | un de | No. 100 100 100 100 100 100 100 100 100 10 | Bit Bit <td> Reg Reg</td> | Reg |
| 10_16860230 | ten de de Ver <mark>de de d</mark> | No. On. On. <td> Tes Tes</td> <td> The The</td> <td> 10</td> <td>One One Column Column</td> <td> No. No.</td> <td> 1</td> | Tes | The The | 10 | One One Column | No. | 1 |
| 10_000011 | les les les les lites lites lites lites les lites les lites | Me Me< | | No. No. | the time to be the time to be the time to be | | The ties the | N |
| hoderskeped Se | tion tion tion to the tion to the tion to the tion tion tion tion to the tion tion tion tion tion tion tion tion | This Nos Nos Nos Nos Nos Nos Nos Nos Nos No | | | | No. | No. One One <td> 10 10 10 10 10 10 10 10</td> | 10 10 10 10 10 10 10 10 |
| principality principality license and ne- ricinal proprint DSE is only linked ther particular proprintary license #1 life the particular proprintary license #1 | Mon. Mon. <th< td=""><td>10</td><td> </td><td> Transfer Transfer</td><td> </td><td>H</td><td> </td><td> N</td></th<> | 10 | | Transfer Transfer | | H | | N |
| ter particular proprietary license #1 30 | 10 No. 10 | De | To the test test test test test test test | Yes No. 100 No. 100 No. 100 No. 100 No. 100 | 10 No | N N N N N N N N N N N N N N N N N N N | De D | 8 No. 100 No. 100 No. 2 No. 100 No. 10 |

License compatibility

- Licenses within one component
- Which component is linked to which other components -> dependency tree helpful
- Dual licensing or "any later version" licensing e.g. MPL-1.1 is not compatible with GPL-2.0 but MPL-2.0 is -> documentation of relicense or dual license options
- Automated compatibility check? -> OSADL compatibility matrix
 (https://www.osadl.org/html/CompatMatrix-noexpl.html) but: still work to do

Integrating curation data

- OSSelot the open source curation database
- Contains SPDX-files with curated data of components (currently 337 packages)
- https://github.com/Open-Source-Compliance/package-analysis/
- License: CC0-1.0
- Integration in scan tools would be helpful (either trusting or control)



Any Questions?

Dr. Till Jaeger - <u>jaeger@jbb.de</u>

JBB

JBB Rechtsanwälte Jaschinski Biere Brexl Partnerschaft mbB

Christinenstraße 18/19 10119 Berlin

Tel. +49 30 443 765 0

Web www.jbb.de



