License compliance and related company processes

Basic lecture: OSADL License Compliance Audit (LCA) and common pitfalls

Caren Kresse

Open Source Automation Development Lab (OSADL) eG

COMPACT OSADL ONLINE LECTURES

Open Source Automation Development Lab eG

Why license compliance?

- Software is protected by **copyright law**.
- Whether a software is Open Source is determined by its **license**.
- Open Source licenses give **unrestricted and unconditional permission to run, analyze and modify** the software.
- **Copying and distribution** are permitted provided that **license conditions** are complied with.

Why license compliance?

- Compliance with legal provisions and regulations includes license compliance.

→ To prevent copyright infringement, protected works may only be copied and distributed when a valid license is obtained.

What is the LCA?

- A **product audit** with analysis of **company processes**
- To support companies in fulfilling **Open Source license obligations** and organize the compliant distribution of **embedded Linux systems**
- An audit of **GPL-2.0 (Linuxkernel)** and **LGPL-2.1 (GNU C Library)**
- Representative for general Open Source license compliance

Procedure

- The product is presented to the auditor as it is distributed (including all documentation).
- The **license obligations** of (L)GPL are checked:
  - Information obligations
  - Disclosure obligations
  - License obligations for modified software
  - Documentation and contracts
  - Additional obligations of LGPL
  - Tivoization
- A report with the results and possible error analysis is created.

Information obligations

GPL-2.0 Art. 1; LGPL-2.1 Art. 1

a) Delivering license texts

b) Delivering copyright notices

c) Delivering the Disclaimer of Warranty

a) Delivering license texts

GPL-2.0 Art. 1; LGPL-2.1 Art. 1

- License text of **GPL-2.0 WITH Linux-syscall-note**
- License text of **LGPL-2.1**
- Informing recipient on where to find the license texts

a) Delivering license texts

GPL-2.0 Art. 1; LGPL-2.1 Art. 1

- License text of **GPL-2.0 WITH Linux-syscall-note**
- License text of **LGPL-2.1**
- Informing recipient on where to find the license texts

- **On paper or on medium (CD, USB drive) or on the system; not a URL**
- ***Additional note:*** **The license texts of all licenses in the Linux kernel must be included.**

b) Delivering copyright notices

GPL-2.0 Art. 1; LGPL-2.1 Art. 1

- “conspicuously and appropriately publish on each copy an appropriate copyright notice”
- Informing recipient on where to find the copyright notices

b) Delivering copyright notices

GPL-2.0 Art. 1; LGPL-2.1 Art. 1

- “conspicuously and appropriately publish on each copy an appropriate copyright notice”
- Informing recipient on where to find the copyright notices

- **If the source code is not delivered along with the product, all copyright notices must be extracted and delivered separately.**

c) Delivering the Warranty Disclaimer

GPL-2.0 Art. 1; LGPL-2.1 Art. 1

- “conspicuously and appropriately publish on each copy an appropriate [...] disclaimer of warranty”
- Warranty disclaimer in favor of the original authors
- It is not sufficient to be included in the license text.

c) Delivering the Warranty Disclaimer

GPL-2.0 Art. 1; LGPL-2.1 Art. 1

- “conspicuously and appropriately publish on each copy an appropriate [...] disclaimer of warranty”
- Warranty disclaimer in favor of the original authors
- It is not sufficient to be included in the license text.

- **Must be delivered separately**

Disclosure obligations

GPL-2.0 Art. 3; LGPL-2.1 Art. 6

- Disclosure of the **“Complete Corresponding Source Code“ (CCSC)** including modifications
- Either: Delivery along with the product
- Or: Written offer for delivery
  - Valid for 3 years, to any 3rd party, no profit
  - Requires processes to be able to handle incoming requests
- On customary medium

Disclosure obligations

GPL-2.0 Art. 3; LGPL-2.1 Art. 6

- Disclosure of the **“Complete Corresponding Source Code“ (CCSC)** including modifications
- Either: Delivery along with the product
- Or: Written offer for delivery
  - Valid for 3 years, to any 3rd party, no profit
  - Requires processes to be able to handle incoming requests
- On customary medium
- **Including build instructions**
- **Rebuild is tested on independent system**

License obligations for modified software

GPL-2.0 Art. 2; LGPL-2.1 Art. 2

- Modification notices (e.g. **Patches**)
- Correct licensing of modifications

- Changes from the vanilla kernel are identified with the **Linux kernel delta scan**.

Digression: Delta scan

https://github.com/armijnhemel/compliance-scripts/tree/master/osadl-audit/

- Assumption: All files of official Linux kernel releases from kernel.org are correctly licensed.
- **Hashcodes** are generated and stored in a **database** for all files of all kernel versions from kernel.org.
- Hashcodes are also generated for the kernel that is to be analyzed and compared with the database.
- **Only those files that are not in the database have been modified or added and must be checked individually.**
- This reduces the license clearance process enormously.

Digression: Delta scan (example)

https://github.com/armijnhemel/compliance-scripts/tree/master/osadl-audit/

```
$ ./osadlaudit.py -s linux-5.4.77/ -c audit.config
SCANNING 52536 files
4 FILES NOT FOUND IN DATABASE
DETERMINING LICENSE OF FILES NOT FOUND
linux-5.4.77/[...]/am335x-wega-bw.dts  ScanCode: ['GPL-2.0-only'] FOSSology: ['GPL-2.0']
linux-5.4.77/[...]/kirkwood-wut.dts    ScanCode: ['GPL-2.0-only'] FOSSology: ['GPL-2.0']
linux-5.4.77/[...]/bmp280-core.c       ScanCode: ['GPL-2.0-only'] FOSSology: ['GPL-2.0']
linux-5.4.77/[...]/weather.c       ScanCode: ['GPL-2.0-or-later'] FOSSology: ['GPL-2.0']
```

Documentation and contracts

GPL-2.0 Art. 6; LGPL-2.1 Art. 10

- “You may not impose any further restrictions on the recipients' exercise of the rights granted herein.“

Documentation and contracts

GPL-2.0 Art. 6; LGPL-2.1 Art. 10

- “You may not impose any further restrictions on the recipients' exercise of the rights granted herein.“
- **Terms of Use, EULAs, etc. may not contradict Open Source licenses.**

Documentation and contracts

GPL-2.0 Art. 6; LGPL-2.1 Art. 10

- “You may not impose any further restrictions on the recipients' exercise of the rights granted herein.“
- **Terms of Use, EULAs, etc. may not contradict Open Source licenses.**
- It is recommended to add a section on Open Source to existing documents:
  “The application contains components which are licensed as Open Source software. The components to which this relates and the respective license terms are enclosed with this license text. The licensee is granted a non-exclusive right of use for the Open Source software by the respective right holders; the conditions stipulated by the respective valid license terms apply. The license terms of this license only apply to the components which are not listed as Open Source software.“

Additional obligations of LGPL

LGPL-2.1 Art. 6

a) Permission for modification and reengineering

b) Notice of use and license of the library

c) Relinking with modified library

a) Permission for modification and reengineering

LGPL-2.1 Art. 6

- For proprietary applications linking the glibc, **permission to modify and reengineer the application** to debug such modifications must be given, e.g.
  “Modifications of this software for the user's own use and reverse engineering for debugging such modifications are herewith permitted.“
- But may be limited:
  “However, forwarding the knowledge acquired during reverse engineering or debugging to third parties is prohibited. Furthermore, it is prohibited to distribute modified versions of this software. In any case, warranty claims on this software will expire, as long as the customers cannot prove that the defect would also occur without these modifications.“

a) Permission for modification and reengineering

LGPL-2.1 Art. 6

- **Third-party software from external suppliers:**
  - Permission must also be given if the glibc is used
  - If the suppliers do not deliver the library, they are not obligated by copyright law to give the permission.
  - Should be considered before buying third-party software
    → **Dependency scan**

- OSADL Legal Assessment: “Licence obligations under the LGPL-2.1 when used with proprietary third-party applications or libraries“

b) Notice of use and license of the library

LGPL-2.1 Art. 6

- “You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License.“
- **“This software uses the GNU C Library licensed under the LGPL-2.1.“**

c) Relinking with modified library

LGPL-2.1 Art. 6

- It mus be made possible to relink the proprietary application with a modified version of the library.
- Either: A shared library mechanism is used, i.e. **dynamic linking.**

c) Relinking with modified library

LGPL-2.1 Art. 6

- It mus be made possible to relink the proprietary application with a modified version of the library.
- Either: A shared library mechanism is used, i.e. **dynamic linking.**
- **Or: If glibc is statically linked, the proprietary application must be provided in linkable form (.a file).**

Tivoization

GPL-2.0 Art. 3; LGPL-2.1 Art. 6

- “[…] plus the scripts used to control compilation and installation of the executable.“

Tivoization

GPL-2.0 Art. 3; LGPL-2.1 Art. 6

- “[. . .] plus the scripts used to control compilation and installation of the executable.“
- **Installing modified versions must be allowed (on request).**

Tivoization

GPL-2.0 Art. 3; LGPL-2.1 Art. 6

- “[. . .] plus the scripts used to control compilation and installation of the executable.“
- **Installing modified versions must be allowed (on request).**
- Best Practices, e.g. for encrypted systems:
  - Password on request
  - Send-in-solution
  - Expiration of warranty, guaranty and safety certification
  - Removal of trademarks should be requested

Additional note: Updates

- Updates are a **separate distribution**.
  → License obligations must be fulfilled separately and completely.
- Publicly downloadable firmware updates are the preferred **target of GPL trolls**.

LCA report

- *License obligation*
  - Result
  - (Cause of error)
  - (Correction of error)
  - (Possible improvements)
  - Conclusion

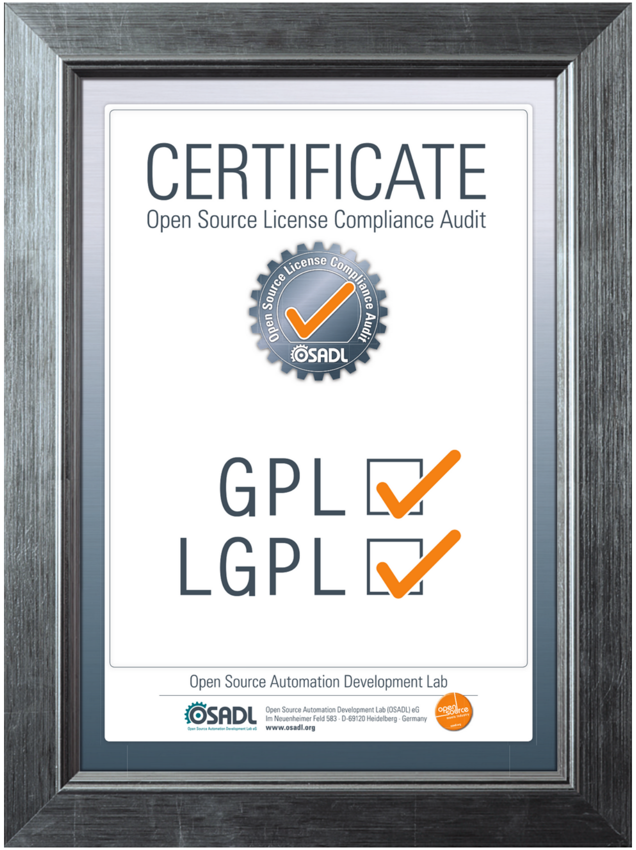
Follow-up audit

- *License obligation*
  - Result
  - **Cause of error**
  - **Correction of error**
  - (Possible improvements)
  - Conclusion

Follow-up audit

LCA certificate

- *License obligation*
  - Result
  - (Possible improvements)
  - Conclusion



CERTIFICATE

Open Source License Compliance Audit

Open Source License Compliance Audit
OSADL

GPL ☑

LGPL ☑

Open Source Automation Development Lab

OSADL Open Source Automation Development Lab (OSADL) eG Im Neuenheimer Feld 583 · D-69120 Heidelberg · Germany www.osadl.org

Conclusion

- To achieve license compliance and avoid common pitfalls:
  - Implement **company processes**
  - Use **license checklists** (e.g. *osadl.org/OSLOC*)
  - Test the **rebuild** on an independent system
- Build systems (e.g. Yocto, Buildroot) support with collecting compliance material (e.g. CCSC, licenses), but a manual check of automatically generated material is recommended.
- Some license obligations can never be fulfilled automatically (e.g. documentation, contracts, licensing).

  → **License compliance always requires manual action!**

Conclusion: FOSS-Policy

- Compliance is organized with a **FOSS-Policy**:
  - to avoid copyright infringements
  - to create and maintain **processes** within a company
  - to establish **understanding** of concepts related to FOSS
  - to provide **control** about licensing of a company's IP
  - to meet **customer requirements**

→ **OSADL Open Source Policy Template** (*osadl.org/os-policy*)

→ **OpenChain Project** (*openchainproject.org*)

COMPACT OSADL ONLINE LECTURES

The OSADL License Compliance Audit (LCA) and common pitfalls
COOL – Compact OSADL Online Lectures
Wednesday, December 16, 2020

Open Source Automation Development Lab eG