Welcome to the questionnaire of the Supplier License Compliance Audit (SLCA)!

Please have a look at the following instructions.

Menu to jump to any group of answers in any order

After having read these instructions, you may click on the below button "Next" to go to the questionnaire.

You may explore or answer the questions in any order by using the "Question index" menu on the right hand side of every page. Just click on the group of questions you would like to explore or answer in order to have the related page displayed on screen. You may then select any other group of questions - even without entering any answers. You may, however, decide to store your anwers in memory by proceeding to the next page, but this requires that all mandatory questions have been answered.

Save answers and restore them at a later date

You may save your answers given so far by clicking on the button "Resume later" that is located at the bottom of each page. If you do so for the first time, you will be asked to provide a username and a password. If you also give your email address, a message will be sent to you with your details and a direct link to your unfinished survey. Next time you would like to save the current survey data just click "Resume later". You can resume by referring to the link in the previously sent email. Please note that your email address and your partially answered responses cannot be undisclosed completely. Thus, if you wish to retain your absolute privacy, you should use an email address such as anonymous@gmail.com (if this is not already taken!) that does not allow to derive your identity from the address.

Erase all answers or submit

You may erase all answers at any time by clicking on "Exit and clear survey" that is located at the bottom of every question page. Alternatively, if you have completed the entire questionnaire, you may submit your answers to the survey administrators by clicking on the button "Submit" on the last page. In the latter case, the data will be used for statistical purposes but certainly not to make any conclusion about your or your employers's legal compliance – even if your identity was disclosed. If you really would like to make sure that nobody knows who you are, please do not enter any information that would allow to derive your identity.

License

This questionnaire and the built-in relevance logic are made available under the

Section A: A. Preparation

A1. **Please describe your company and the major aspects of the processes you follow to ensure open source license compliance.**

A2. **How do you provide software to your customer?**

We provide software via internet download or via email. ☐

We ship software integrated as firmware in a product. ☐

We ship software on a medium customarily used for software interchange such as CD or DVD. ☐

We provide software training and support. ☐

Other ▼

Other

A3. **Does your software support include providing source code patches in form of so-called context diffs?**

Yes ☐

No ☐

Section B: B. Use Case Scenario

A software developer working for your company wants to use and possibly to pass on one or more components as part of the software you plan to supply to your client.

B1. **Do developers need to clear the software, i.e. get the "OK" from their superior/the legal department/etc. to be allowed to use and/or to pass on the software?**

Yes ☐

No ☐

B2. **Do you have a process in place to clear the use of components licensed under Free and Open Source software (FOSS) licenses?**

Yes ☐

No ☐

B3. **Please provide a description of the process you have in place as Annex #1 or upload it here.**

Section C: C. Questions - I. Organization - 1. Repository

Background of questions

FOSS compliance requires processing FOSS in an organized manner. Those actually writing software need to be enabled to handle FOSS in accordance with the license obligations. This requires a managed software register (repository) which is crucial to

have an overview which FOSS is used, to know where it comes from, and have the source code of this FOSS.

C1. **Do you use a central archive to store and describe software you might use/are using in your products/software solutions without exception?**

Yes ☐

No ☐

C2. **Does this central archive allow you to do a roll-back and find old versions of the code, i.e. can be used as a software repository?**

Yes ☐

No ☐

C3. **Do you use this software repository for**

FOSS ☐

Software your employees develop ☐

Software your suppliers develop ☐

Software other personnel (i.e. students; freelancers) develops for you? ☐

C4. **For which software are the above marked persons using the software repository?**

For all software ☐

Only if they use a development tool licensed under a FOSS license or if they use FOSS as the basis for their development ☐

C5. **Who is allowed to access the repository?**

Everyone in the company ☐

All software developers ☐

All software developers who are involved in the project the repository is set up for ☐

C6. **Who manages the repository?**

Everyone who can access the software repository ☐

The person that is in charge of the project ☐

The software repository does not need to be managed ☐

Other ▼

Other

C7. Do you train your employees how to use your repository (e.g. in-house training or external training)?

Yes ☐

No ☐

C8. Does the software repository log when FOSS is checked out to a computer for the purpose of changing the FOSS?

Yes ☐

No ☐

C9. Does the software repository log when FOSS is checked in back to the software repository?

Yes ☐

No ☐

C10. Does FOSS that is checked in back to the software repository automatically receive a new version number or is there an equivalent mechanism?

Yes ☐

No ☐

C11. Does the software repository document changes made to the FOSS?

Yes ☐

No ☐

C12. When documenting changes, which data does the software repository document?

```



```

C13. Is there a control mechanism concerning form and content of the commit comment?

Yes ☐

No ☐

C14. **Please describe the control mechanism:**

C15. **When entering existing source code to the software repository do you identify and document the following?**

On which date the code was put in the software repository ☐

Who puts the code in the software repository ☐

Which website the code came from ☐

The license of the code ☐

The version of the FOSS component ☐

Cryptographically assumed identifier ☐

C16. **Do you freeze the software version after you received existing source code?**

Yes ☐

No ☐

C17. **Do you have means other than a software repository to secure and organize incoming code?**

Yes ☐

No ☐

C18. **Please name and describe your means:**

C19. **How do you handle the software which is not described and stored in such an archive?**

Section D: C. Questions - I. Organization - 2. Internal Organization/Roles/Responsibilities

Background of questions

The following questions focus on internal processes that a company may have established to ensure FOSS compliance.

D1. **Have you defined a process/processes that is/are designed to ensure FOSS license compliance?**

Yes ☐

No ☐

D2. **Is the process/are the processes available in form of a document?**

Yes ☐

No ☐

D3. **Please provide a copy of the document as Annex #2 or upload it here.**

D4. **Please describe the process/processes.**

D5. **Does the process/do the processes apply to**

everyone in the company ☐

everyone in the company involved in software development ☐

particular departments of the company other than software development ☐

software development and other departments, handled individually ☐

D6. **Is the process/are the processes based on a hierarchy?**

Yes, there is a single person ☐

Yes, there is a group of persons ☐

No hierarchy ☐

D7. **Which department does the person/does the group of persons work in?**

Legal department ☐

Sales and marketing department ☐

Development department ☐

Other

D8. **Is there a description of the role for each of these persons responsible for FOSS compliances describing his/her tasks?**

Yes ☐

No ☐

D9. **Please provide us with such description(s) as Annex #3 or upload it or them here.**

D10. **Is the single person/group of persons making the final decision about**

which FOSS can be used in your software solutions/products ☐

the conditions under which the FOSS can be used in your software solutions /products? ☐

D11. **The person(s) making the final decisions regarding FOSS use, were they hired specifically to oversee FOSS compliance in your company; e.g. from a FOSS-related foundation or because they have a FOSS-related educational/work background?**

Yes ☐

No ☐

D12. **Whom do the person(s) making the final decisions regarding FOSS use report to?**

D13. **Do the person(s) making the final decisions regarding FOSS use in your company get regular training on FOSS and related questions?**

Yes ☐

No ☐

D14. **How often?**

D15. **What does the expertise of the person leading such trainings result from?**

D16. **Do you employ an external lawyer for advice on FOSS compliance?**

Yes ☐

No ☐

D17. **Are your employees allowed to give feedback relating to the**

decision-making processes ☐

decision, whether FOSS can be used ☐

conditions under which FOSS can be used? ☐

D18. **Are there standard procedures how feedback can be given and on how such feedback is handled, e.g. request forms and the like?**

Yes ☐

No ☐

D19. **How can feedback be given? Please specify:**

D20. **Do you have a written procedure on how to deal with feedback delivered by employees or other people relating to the decision-making process?**

Yes ☐

No ☐

D21. **Please provide us with the documentation as Annex #4a or upload it here.**

D22. **How can your employees provide feedback regarding the decision-making process?**

D23. **Do you have a written procedure on how to deal with feedback delivered by employees or other people relating to the decision itself?**

Yes ☐

No ☐

D24. **Please provide us with the documentation as Annex #4b or upload it here.**

D25. **How do you handle possible protests of your employees regarding the decision that certain FOSS components cannot be used? How do you handle other feedback relating to the decision itself?**

D26. **Do you have a written procedure on how to deal with feedback delivered by employees or other people relating to the conditions under which FOSS can be used?**

Yes ☐

No ☐

D27. **Please provide us with the documentation as Annex #5 or upload it here.**

D28. **How do you handle feedback relating to the conditions under which FOSS can be used?**

Section E: C. Questions - I. Organization - 3. Education

Background of questions

Lack of knowledge about FOSS licensing is a major reason for compliance problems.

Therefore, staff needs to have a certain level of knowledge to be able to recognize compliance issues and to handle questions.

To obtain this knowledge, regular education is crucial.

Please make sure that the auditors can review such in-house knowledge management system during the audit.

Please make sure that our auditors can review such internal documentation or information during the audit.

E1. **Do you train and educate your software developers/software engineers on how to handle FOSS and on regularly occurring problems regarding the handling of FOSS?**

Yes ☐

No ☐

E2. **How often do you do that?**

E3. **How is the trainer qualified ?**

Lawyer ☐

Technician ☐

Other ▼

Other

E4. **Do you train all employees involved in software development or only some?**

All ☐

Some ☐

E5. **Please name the criteria how do you choose the employees who get the training:**

E6. **Do you have an in-house knowledge management system regarding the handling of FOSS?**

Yes ☐

No ☐

E7. **Do you have internal documentation or information regarding problems related to FOSS or the handling of FOSS (such as scripts, handouts, charts, checklists etc.), which you hand out to your employees?**

Yes ☐

No ☐

Section F: C. Questions - II. Participation and Collaboration - 1. Participation

F1. **Do you participate in FOSS projects?**

Yes ☐

No ☐

F2. **Do you specifically try to hire personnel from FOSS projects?**

Yes ☐

No ☐

F3. **Do you specifically try to hire personnel that is also maintainer of FOSS projects?**

Yes ☐

No ☐

F4. **Would you prefer to hire software developers that are active in the FOSS community over those that have never been involved in any FOSS project?**

Yes ☐

No ☐

F5. Would you prefer software developers that have never been involved in any FOSS project over those that are active in the FOSS community?

Yes ☐

No ☐

Section G: C. Questions - II. Participation and Collaboration - 2. Collaboration

G1. Do the people responsible for FOSS compliance in your company collaborate (e.g. form a joint committee)?

Yes ☐

No ☐

G2. Is there an established collaboration/ communication process between the people responsible for FOSS compliance in your company (e.g. regular meetings, jour fixes)?

Yes ☐

No ☐

G3. Please specify:

Section H: C. Questions - II. Participation and Collaboration - 3. Exchanging Software

H1. Do companies within your group provide software and/or software-related services to other companies within your group?

Yes ☐

No ☐

H2. Please describe how software is provided between companies as Annex #6 or upload the document here.

H3. Are license obligations followed when you provide FOSS to another company of your group?

Yes ☐

No ☐

Section I: C. Questions - II. Participation and Collaboration - 4. Merger & Acquisition

I1. **Do you ever buy other companies?**

Yes ☐

No ☐

I2. **Is FOSS compliance a subject of the due diligence when acquiring another company?**

Yes ☐

No ☐

I3. **Please provide us with the documentation of what is checked during a due diligence as Annex #7 or upload it here.**

Section J: C. Questions - III. Incoming Code - 1. Provenance of code - a. Downloading FOSS

Background of questions

To be able to fulfill FOSS license requirements, internal company processes need to be in place to collect the necessary information about which FOSS components are used, which FOSS licenses apply, what is the origin of the code and how the FOSS components are used. The company needs to control the incoming code and set standards how the code has to be handled to be actually able to fulfill FOSS license requirements.

Background of questions on downloading FOSS:

a) A typical mistake is that binaries are downloaded but the corresponding source code is not downloaded along with the binary. Or, source code is downloaded, but is not completely corresponding to the binaries. In such cases there is a risk for license violations if the FOSS license requires offering of the source code. Furthermore, without the complete corresponding source code it is very difficult to review the software for license compatibility and unknown licenses of subcomponents.

b) To the origin of the code is needed

to provide evidence where the code comes from, to contact rightholders in case of unclear licenses.

c) It is difficult to detect some license issues without a scan of the software. Scanning is a necessary but not sufficient step to collect the necessary information for further analysis.

J1. **Do you compile the software you distribute?**

Yes ☐

No ☐

J2. **Do you distribute downloaded FOSS in compiled form only?**

Yes ☐

No ☐

J3. **Do you distribute such downloaded FOSS in compiled form only as you downloaded it (i.e. without any modifications)?**

Yes ☐

No ☐

J4. **Do you always download the source code for FOSS that you have downloaded in compiled form?**

Yes ☐

No ☐

J5. **When do you download the source code?**

At the same time when the component is downloaded in compiled form ☐

Right before the software is about to be distributed ☐

Other ▼

Other

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

J6. **Do you perform a rebuild to see if the downloaded source code and the downloaded compiled code match?**

Yes ☐

No ☐

J7. **Do you inspect FOSS you have downloaded?**

Yes ☐

No ☐

J8. **Do you use a scanning tool for such inspections of the FOSS components?**

Yes ☐

No ☐

Section K: C. Questions - III. Incoming Code - 1. Provenance of code - b. Incoming FOSS from other sources

Background of questions

Suppliers need the necessary legal position to use the software that is developed on their behalf. If the license applicable to incoming code does not allow a company to use and/or pass on the software as needed and/or to license it under a FOSS license this might cause copyright infringement. In particular, the company needs to have the right to license such code under a Copyleft license to meet the license requirements of Copyleft licenses.

Incoming FOSS from employees
Freelancers Background of questions

Under most jurisdictions the employer has comprehensive rights in the software developed by employees (e.g. work made for hire, sec. 69b German Copyright Act). This is not necessarily true for software developed by freelancers and other third parties. Therefore, license agreements are needed to assure that necessary rights are transferred to the company to relicense this software as FOSS (if needed).

Unknown FOSS components in software developed by freelancers might cause incompatibilities.

Incoming FOSS from personnel other than employees or freelancers
Incoming FOSS from suppliers

K1. **Do you receive software from other sources than a download from the Internet?**

Employees ☐

Freelancers ☐

Personnel other than Employees/Freelancers ☐

Suppliers ☐

K2. **Do at least one of your employees develop software in their free time?**

Yes ☐

No ☐

K3. **Do you scan the software your employees develop for you/as part of their job?**

Yes ☐

No ☐

K4. **Does at least one of your employees contribute to FOSS projects?**

Privately ☐

As representative of your company in external FOSS projects ☐

Own FOSS projects of your company ☐

Other ☐

K5. **Please specify:**

K6. **Please name the FOSS projects your employees contribute to (if more than three, please name the three most important ones):**

K7. **Do you care whether your employees are maintainers of FOSS projects?**

Yes ☐

No ☐

K8. **Are any of your employees maintainers of FOSS projects?**

Yes ☐

No ☐

K9. **Do freelancers develop software for you?**

Yes ☐

No ☐

K10. **Is there a written contract with freelancers containing a licensing clause?**

Yes ☐

No ☐

K11. **Please provide an example of the contract with the freelancer(s) and/or the regulations on licensing before the on-site audit as Annex #8 or upload it here.**

K12. **Have you asked the freelancer whether there is pre-existing FOSS code contained in his/her code delivered to you?**

Yes ☐

No ☐

K13. **Which license information is to be provided by the freelancer, please provide as Annex #9 or upload it here.**

K14. **Do you scan the code freelancers deliver to you?**

Yes ☐

No ☐

K15. **Do you require that freelancers scan the code they deliver to you?**

Yes ☐

No ☐

K16. **Do you require they do an automated scan?**

Yes ☐

No ☐

K17. **Do you require they use certain scanning tools?**

Yes ☐

No ☐

K18. **Please name the scanning tools and version you require them to use:**

K19. **Do you require your freelancers to use other methods than scanning to inspect incoming software?**

Yes ☐

No ☐

K20. **Please specify the methods you require them to use:**

K21. **Do you require your freelancers to use certain search strings?**

Yes ☐

No ☐

K22. **Which search strings do you require your freelancers to use?**

K23. **How do you ensure the required scan was conducted?**

K24. **Have you agreed with your freelancers on a copyright notice?**

Yes ☐

No ☐

K25. **Please provide an example of such a copyright notice(s) you use:**

K26. **Does the freelancer have to provide source code in any case?**

Always ☐

Only, if the applicable license requires source code disclosure. ☐

K27. **If the freelancer uses FOSS, does he/she have to provide**

Binary code ☐

Source code ☐

License texts ☐

Copyright notice ☐

Other ▼

Other

K28. **Do you perform a rebuild to make sure that source code and binary code delivered by a freelancer match?**

Yes ☐

No ☐

K29. **Do you ask the freelancer whether he/she has conducted a rebuild?**

Yes ☐

No ☐

K30. **Does personnel other than employees/freelancers develop software for you?**

Undergraduates ☐

Students ☐

Doctoral candidates ☐

Working students ☐

Other ▼

Other

K31. **Is there a written contract with such personnel?**

Yes ☐

No ☐

K32. **Does such agreement contain a licensing clause?**

Yes ☐

No ☐

K33. **Please provide an example of such agreement and/or the licensing provision(s) before the on-site audit as Annex #10 or upload it here.**

K34. **Do you ask such personnel whether there is FOSS code contained in the code delivered to you?**

Yes ☐

No ☐

K35. **Do you scan the code delivered by this personnel?**

Yes ☐

No ☐

K36. **Have you agreed with this personnel on a copyright notice?**

Yes ☐

No ☐

K37. **Please provide an example of such a copyright notice before the on-site audit as Annex #11 or upload it here.**

K38. **Does such personnel have to provide source code in any case?**

Always ☐

Only, if the applicable license requires source code disclosure. ☐

K39. **If such personnel uses FOSS, does he/she has to provide**

Binary code ☐

Source code ☐

License texts ☐

Copyright notice ☐

Other ▼

Other

K40. **Do you perform a rebuild to make sure that source code and object code match?**

Yes ☐

No ☐

K41. **Do you use and distribute software supplied by other companies?**

Yes ☐

No ☐

K42. **Is there a written contract with such suppliers?**

Yes ☐

No ☐

K43. **Does such agreement contain a licensing clause?**

Yes ☐

No ☐

K44. **Please provide an example of this agreement before the on-site audit as Annex #12 or upload it here.**

K45. **What kind of software does the company supply?**

FOSS ☐

Proprietary licensed software ☐

K46. **How do you receive the FOSS code?**

Source code ☐

Binary code ☐

K47. **How do you receive the proprietary licensed code?**

Source code ☐

Binary code ☐

K48. **Do you exclude certain FOSS licenses in the agreement with your supplier?**

Yes ☐

No ☐

K49. **Do you ask suppliers whether there is FOSS code contained in the code delivered to you?**

Yes ☐

No ☐

K50. **Do you scan the code delivered by suppliers?**

Yes ☐

No ☐

K51. **Have you agreed with the supplier on a copyright notice?**

Yes ☐

No ☐

K52. **Please provide an example of such a copyright notice before the on-site audit as Annex #13 or upload it here.**

K53. **Does the supplier have to provide source code in any case?**

Always ☐

Only, if the applicable license requires source code disclosure. ☐

K54. **If the supplier uses FOSS, does he/she has to provide**

Binary code ☐

Source code ☐

License texts ☐

Copyright notice ☐

Other ▼

Other

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

K55. **Do you perform a rebuild of the source code delivered to you to make sure that source code and object code match?**

Yes ☐

No ☐

Section L: C. Questions - III. Incoming Code - 2. Form of code

L1. **Which form of incoming code are you dealing with?**

Binary code ☐

Source code ☐

Section M: C. Questions - III. Incoming Code - 3. Inspection and Approval

InspectionApproval

M1. **Do you inspect incoming**

binary code ☐

source code ☐

known proprietary software from third parties ☐

known FOSS? ☐

M2. **Is there a particular kind of software that you do not inspect?**

Yes ☐

No ☐

M3. **Please specify:**

M4. **Why do you not inspect them all?**

M5.

How do you verify one of the reasons/cases, in which you are not required to inspect the software?

M6. **Do you have specified and/or documented criteria for this?**

Yes ☐

No ☐

M7. **Please provide such criteria before the on-site audita as Annex #14 or upload it here.**

M8. **Do you inspect the incoming code using scan tools?**

Yes ☐

No ☐

M9. **Which tool(s) do you use for scanning?**

M10. **Which version of these tool(s) are you using?**

M11. **Please provide a documentation about what words/phrases/strings you are searching the software for as Annex #15 or upload it here.**

M12. **Do you use other methods than scanning to inspect incoming software?**

Yes ☐

No ☐

M13. **Please specify the methods you use:**

M14. **Do you check the source code manually for license information and/or copyright notices?**

Yes ☐

No ☐

M15. **What search strings are you using?**

M16. **Please describe how you conduct the search:**

M17. **Does software (in source or binary form) have to be approved before it is used in your development process?**

Yes ☐

No ☐

M18. **Please describe the parameters for such approval as Annex #16 or upload it here.**

M19. **Do you differentiate between approving FOSS and other software?**

Yes ☐

No ☐

M20. **Please describe how you differentiate as Annex #17 or upload it here, e.g. copy of your policy.**

M21. For what kind of software do you make exceptions (i.e. what kind of software can get into your company without going through an approval procedure)?

M22. Is there a point in time during the development process that FOSS needs to be approved at?

When entering your company ☐

Before products/software solutions are given to third parties (i.e. customers) ☐

Other ▼

Other

M23. Is there an approval procedure for incoming (FOSS and other) software, such as some kind of quality gate?

Yes ☐

No ☐

M24. Please provide the documentation of such procedure before the on-site audit as Annex #18 or upload it here.

M25. Does all software have to go through this procedure, before it can be used by your developing staff?

Yes ☐

No ☐

M26. Do you have to have

FOSS approved, before staff is allowed to use it in your development process? ☐

FOSS approved, before you can use it in your products/software solutions? ☐

other software approved, before you can use it? ☐

M27. What is the educational background of the person approving software you want to use?/ Which department(s) approve software you want to use?

Legal ☐

Sales and marketing ☐

Development/technical ☐

Other

Other

| | | | | | | | | | | | | | | | | | | |

M28. **Do you also scan the outgoing FOSS?**

Yes ☐

No ☐

M29. **Is there software that is generally forbidden from being used in your company?**

Yes ☐

No ☐

M30. **Do you exclude certain types of licenses (in other words: Is it forbidden to use software licensed under certain types of licenses)?**

Yes ☐

No ☐

M31. **Do you have a written policy with regard to allowed/forbidden licenses?**

Yes ☐

No ☐

M32. **Please provide the policy before the on-site audit as Annex #19 or upload it here.**

M33. **Please describe which software you exclude (e.g. FOSS/copyleft software)?**

M34. **Please describe why such software is forbidden from being used in your company:**

N1. **Do you treat FOSS intented to be exclusively used in-house in the same way as FOSS to be passed on to third parties, e.g. in your products?**

Yes ☐

No ☐

N2. **Do you pass on software which is licensed under the following licenses?**

GNU General Public License (GPL) ☐

Lesser GNU General Public License (LGPL) ☐

Eclipse Public License (EPL) ☐

Affero General Public License (AGPL) ☐

Mozilla Public License (MPL) ☐

Common Public License (CPL) ☐

Common Development and Distribution License (CDDL) ☐

Berkeley Software Distribution License (BSD) ☐

Other FOSS license(s) ☐

N3. **Please specify:**

N4. **Do you have any restrictions with regard to licenses of FOSS components to be used in your company?**

Yes ☐

No ☐

N5. **Which licenses are excluded from use in your company?**

Section O: C. Questions - III. Incoming Code - 5. Documentation

O1. **What do you document when you receive incoming FOSS?**

Website you downloaded it from ☐

Date of download ☐

Who downloaded it ☐

License ☐

License version ☐

Version of incoming FOSS ☐

Package name ☐

File name ☐

Cryptographic checksum ☐

Others, please specify: ☐

O2. **Please specify which item not in the above list you document:**

O3. **Do you have a company policy how FOSS used in your products and/or your development process needs to be documented?**

Yes ☐

No ☐

O4. **Please provide this policy before the on-site audit as Annex #20 or upload it here.**

O5. **Where do you document information about incoming code? Do you have a library or a special storage space for such documentation? Please specify:**

O6. **Who takes care of the documentation?**

Someone particular who is responsible ☐

Each employee for him or herself ☐

Section P: C. Questions - IV. License Obligations - 1. Checking for Applicable Licenses

Background of questions Most license violations are resulting from insufficient review of license obligations. FOSS licenses have to be reviewed systematically and the license obligations have to be extracted. If license obligations are not identified properly, they cannot be fulfilled. Common mistakes when fulfilling license obligations are that source code is not provided even though the license requires the licensee to do so when distributing code, or that applicable license texts and/or copyright notices are not distributed with the software.

P1. **Do you check which license is applicable to incoming FOSS?**

Yes ☐

No ☐

P2. **How do you do that?**

Scan ☐

Manually ☐

P3. **What is the educational background of the person checking which license is applicable to the incoming FOSS?**

Legal department ☐

Sales and marketing department ☐

Development department ☐

I don't know ☐

Other ▼

Other

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

P4. **Where does this person look to identify the license that applies to the FOSS?**

[ ]

P5. **Do you identify and secure the precise version of the license?**

Yes ☐

No ☐

P6. **Are most employees who are dealing with FOSS aware of Software Package Data Exchange (SPDX)?**

Yes ☐

No ☐

P7. **Is SPDX mandatory in your company?**

Yes ☐

No ☐

P8. **Do you require suppliers to give you SPDX information?**

Yes ☐

No ☐

P9. **Do you require your freelancers to give you SPDX information?**

Yes ☐

No ☐

P10. **Do you demand your coders to generate SPDX files of your own software?**

Yes ☐

No ☐

P11. **Do you otherwise identify and / or use the SPDX information?**

Yes ☐

No ☐

P12. **If the applicable license is only referred to on the FOSS projects website, do you identify and secure the applicable license, especially the license text in any other way than by writing down the license's name?**

Yes ☐

No ☐

P13. **How do you do that?**

P14. **Do you download the FOSS license text corresponding to the FOSS you download?**

Yes ☐

No ☐

Section Q: C. Questions - IV. License Obligations - 2. Identifying License Requirements

Q1. **Does anyone in your company actually read the license texts of FOSS components?**

Yes ☐

No ☐

Q2. **Does the person responsible for identifying license obligations actually read the license texts of FOSS components?**

Yes ☐

No ☐

Q3. **What is the educational background of the person reading the license texts?**

Legal department ☐

Sales and marketing department ☐

Development department ☐

I don't know ☐

Other ▼

Other

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Q4. **Does the person reading the license texts identify and document the license requirements?**

Yes ☐

No ☐

Q5. **Please provide an example of such documentation before the on-site audit as Annex #21 or upload it here.**

Q6. **Is the documentation of license requirements prepared for use by**

Staff with legal background ☐

Staff with marketing and advertising background ☐

Staff with development / technical background ☐

I don't know. ☐

Q7. **Do you have pre-formulated checklists for certain licenses which sum up the license obligations?**

Yes ☐

No ☐

Q8. **Are there different checklists for different kinds of FOSS licenses?**

Yes ☐

No ☐

Q9. **Please specify as Annex #22 or upload the checklists here.**

Section R: C. Questions - IV. License Obligations - 3. License Texts

R1. **Do you ship license texts for FOSS components with your software?**

Always ☐

Sometimes ☐

Never ☐

R2. **Under which condition do you ship license texts? Please specify:**

R3. **How do you ship license texts to your customers?**

As paper copy together with the product/software solution containing FOSS ☐

On a data carrier together with the product/software solution containing FOSS ☐

Providing a download link refering to a server managed by the company ☐

Providing a download link refering to a server managed by someone else ☐

Providing access through a GUI of the product/software solution containing FOSS ☐

R4. **Please describe how you ensure the same license texts are shipped in all ways:**

R5.

Where do the license texts given in the GUI come from?

Stored in the product/software solution containing FOSS ☐

Downloaded from an external server ☐

Other ▼

Other

R6. **Do you name the licenses applicable to your software (e.g. in a handbook or other documentation)?**

Yes ☐

No ☐

R7. **Do you refer to the name of the FOSS component when providing FOSS licenses?**

Yes ☐

No ☐

R8. **Please describe, how you ensure that people are able to find the license texts:**

Section S: C. Questions - IV. License Obligations - 4. Source Code

S1. **Do you provide source code together with your product/software solution?**

Always ☐

Sometimes ☐

Never ☐

S2. **Do you provide a written offer to ship the source code on request?**

Yes ☐

No ☐

S3. **Please provide the text you use for offering source code as Annex #23 or upload it here.**

S4. **How do you provide source code?**

Providing a download link refering to a server managed by the company ☐

Providing a download link refering to a server managed by someone else ☐

Stored in the product/software solution containing FOSS ☐

On a data carrier together with the product/software solution containing FOSS ☐

Other ▼

Other

S5. **Do you check that the source code matches with the binary you will pass on?**

Yes ☐

No ☐

Section T: C. Questions - IV. License Obligations - 5. Copyright Notices

T1. **Do you provide copyright notices with the product containing FOSS?**

Yes ☐

No ☐

T2. **Do you scan the source code for copyright notices?**

Yes ☐

No ☐

T3. **Please explain why you do not scan source code for copyright notices.**

T4. **What tool do you use to scan source code for copyright notices?**

T5. **Please provide documentation about what words/phrases/strings you are searching the software for as Annex #24 or upload it here.**

T6. **Do you scan all software?**

Yes ☐

No ☐

T7. **Why do you not scan it all?**

T8. **How do you verify that the above-mentioned reasons/cases apply?**

T9. **Do you manually search the source code for copyright notices?**

Yes ☐

No ☐

T10. **Do you use other methods than scanning to inspect incoming software?**

Yes ☐

No ☐

T11. **Please specify the methods you use:**

T12. **What search strings are you using?**

T13. **Please describe how you conduct the search:**

T14. **Do you extract copyright notices from the header files?**

Yes ☐

No ☐

T15. **Do you extract copyright notices from the web pages from which you downloaded the software?**

Yes ☐

No ☐

T16. **Do you do something else to extract copyright notices?**

Yes ☐

No ☐

T17. **Please specify:**

Section U: C. Questions - IV. License Obligations - 6. Modification Information

U1. **Do you provide modification information in the header of modified files?**

Always ☐

Never ☐

If required by the applicable FOSS license ☐

U2. **Please provide us with an example as Annex #25 or upload it here.**

U3. **Do you provide modification information elsewhere than in the header of modified files?**

Yes ☐

No ☐

U4. **Please specify:**

U5. **Do you provide modification information in form of context diff patches?**

Yes ☐

No ☐

Section V: C. Questions - IV. License Obligations - 7. Application Service Provider/Software as a Service

V1. **Do you offer Software as a Service (SaaS) solutions?**

Yes ☐

No ☐

V2. **Do you check which FOSS licenses apply for SaaS products/software solutions?**

Yes ☐

No ☐

V3. **Do you check, if license obligations have to be fulfilled?**

Yes ☐

No ☐

V4. **Do you handle software that is being offered via SaaS differently from software that is being delivered to your customers?**

Yes ☐

No ☐

V5. **Does incoming code designed and bound to be offered via SaaS have to fulfill the same requirements as the ones listed above for FOSS?**

Yes ☐

No ☐

V6. **Please describe how it is treated differently as Annex #26 or upload it here.**

V7. **Do you have a written policy regarding the process such software has to go through?**

Yes ☐

No ☐

V8. **Please provide it before the on-site audit as Annex #27 or upload it here.**

Section W: C. Questions - V. Handling Copyleft Licenses and License Compatibility - 1. Copyleft Licenses

Background of questions

If FOSS licensed under a copyleft license is changed or combined with other software in a way that a derivative work is created that work needs to be licensed under the copyleft license.

The legal effect is twofold:

Copyright is infringed in the case that the changes are not licensed under a copyleft license or the changes are not properly licensed in accordance with the requirements set forth by the copyleft license (e.g. with regard to LGPL). Copyright is infringed in the case that the licenses covering the software combined are not compatible.

W1. **Do you pass on FOSS that uses a license with a copyleft clause (e.g. GPL)?**

Yes ☐

No ☐

W2. **Do you use code licensed under the following licenses?**

GNU General Public License (GPL) ☐

Lesser GNU General Public License (LGPL) ☐

Eclipse Public License (EPL) ☐

Affero General Public License (AGPL) ☐

Common Public License (CPL) ☐

Other

Other

W3. **Do you have to have FOSS licensed under a copyleft license approved before you use it?**

Yes ☐

No ☐

W4. **Do you have written guidelines on how to handle FOSS licensed under a copyleft license?**

Yes ☐

No ☐

W5. **Please provide the guidelines before the on-site audit as Annex #28 or upload it here.**

W6. **Do you have written guidelines when changes to and/or combinations of and/or linking FOSS etc. is considered a derivative work?**

Yes ☐

No ☐

W7. **Please provide the guidelines before the on-site audit as Annex #29 or upload it here.**

W8. **Do you consider it necessary to license your own code under the GPL when linked with a GPL library?**

Yes ☐

No ☐

W9. **Do you consider it necessary to license your own code under the EPL when linked with an EPL library?**

Yes ☐

No ☐

W10. **Do you use any tools to get a better understanding how components interact with each other, for example using a linking dependency graph?**

Yes ☐

No ☐

W11. **Please provide an example as Annex #30 or upload it here.**

X1. **Is license compatibility something you have to deal with in your company?**

Yes ☐

No ☐

I don't have ever heard of that ☐

I know what it is, but I don't know whether we have to deal with it ☐

X2. **Please explain why you do not have to deal with it:**

X3. **Do you check, if**

the FOSS licenses applicable to the software are compatible? ☐

the FOSS licenses applicable to your software affect the rights the licenses applicable to other third-party components need to grant? ☐

the FOSS licenses applicable to your software affect the rights the licenses applicable to components newly developed by you need to grant? ☐

X4. **Do you have your own personnel perform such check or use external expertise or consulting?**

Own personnel ☐

External consultant ☐

X5. **What is the educational background of the person checking the license compatibility?**

Legal department ☐

Sales and marketing department ☐

Developmental department ☐

I don't know ☐

Other ▼

Other

X6. **Do you have a written policy regarding how to handle that licenses applicable to your software are found to be incompatible?**

Yes ☐

No ☐

X7. **Please provide before the on-site audit as Annex #31 or upload it here.**

X8. **Do you have an unwritten policy regarding how to handle that licenses applicable to your software are found to be incompatible?**

Yes ☐

No ☐

X9. **Please describe:**

X10. **Is there a common practice how those findings are handled?**

Yes ☐

No ☐

X11. **Please specify:**

X12. **How do you handle licenses applicable to your software being found to be incompatible? Please specify:**

X13. **Do you have a license matrix regarding which licenses are compatible?**

Yes ☐

No ☐

X14. **Please provide these guidelines or the matrix before the on-site audit as Annex #32 or upload it here.**

Section Y: C. Questions - VI. Outbound Licensing and Product/ Software Solution review

Background of questions:

Distribution agreements and licensing of own code are a source for license violations. This is the case, e.g. of LGPL requiring to allow re-engineering of linked applications. Quality management before distribution helps to avoid license violations by mistake.

Y1. **Do you inform your customers that your products/ software solutions include FOSS?**

Yes ☐

No ☐

Y2. **Do you provide a Bill of Materials (BOM) with FOSS components for all your products/ software solutions?**

Yes ☐

No ☐

Y3. **Is this BOM given to your customers?**

Yes ☐

No ☐

Y4. **Which format do you use for your BOM?**

One of the usual spread sheet formats ☐

SPDX files ☐

Text files ☐

Other ▼

Other

Y5. **How is this file generated?**

Automatcally by the build system ☐

Manually ☐

Y6. **Do your customer agreements (distribution contracts and license agreements) include a clause/clauses regarding FOSS?**

Yes ☐

No ☐

Y7. Please provide an exemplary contract before the on-site audit (as Annex #33 or upload it here).

Y8. Do you check your software with regard to the fulfillment of FOSS license requirements before it leaves your company?

Yes ☐

No ☐

Y9. Do you have an established procedure for checking the software?

Yes ☐

No ☐

Y10. Please provide the documentation for this procedure as Annex #34 or upload it here.

Y11. What is the educational background of the person(s) responsible for checking the software with regard to the fulfillment of FOSS license requirements?

Legal ☐

Sales and marketing ☐

Development/technical ☐

Quality management ☐

Y12. Does the person(s) responsible for checking the software with regard to the fulfillment of FOSS license requirements receive special training?

Yes ☐

No ☐

Y13. Do you have checklists containing criteria to be fulfilled before software is distributed?

Yes ☐

No ☐

Y14. Please provide a copy before the on-site audit as Annex #35 or upload it here.

Section Z: C. Questions - VII. Maintenance Handling

Background of questions:

We can observe that sometimes there are compliance efforts for the original product/ software solution but updates or upgrades are not taken into consideration (e.g. complete corresponding source code is missing).

Z1. **Do you provide updates/upgrades for your software?**

Yes ☐

No ☐

Z2. **Please provide us with information how the update process is handled before the on-site audit as Annex #36 or upload it here.**

Z3. **Do you provide context diff patches for your software?**

Yes ☐

No ☐

Z4. **Do you equip your patches with licensing information?**

Yes ☐

No ☐

Z5. **Do you provide hotfixes for your binary software?**

Yes ☐

No ☐

Z6. **Do you provide licensing information with your hotfixes?**

Yes ☐

No ☐

Section AA: C. Questions - VIII. Patent Issues

AA1. **Do you perform any kind of patent research before using code?**

Yes ☐

No ☐

AA2. **Please describe the educational background of the person performing the research:**

Legal ☐

Development/technical ☐

Other ▼

Other

AA3. **Do you employ patent attorneys to help you?**

Yes ☐

No ☐

AA4. **Do you have standard procedures for licensing in place, if you want to use patented code?**

Yes ☐

No ☐

AA5. **Please provide a description before the on-site audit as Annex #37 or upload it here.**

AA6. **Are you a member of a defensive organization that provides a mutual non-infringement contract such as the Open Invention Network (OIN)?**

Yes ☐

No ☐

AA7. **Which one(s)?**

OIN ☐

Other(s) ☐

AA8. **Please specify:**

___

Thank you for using the Supplier License Compliance Audit (SLCA).