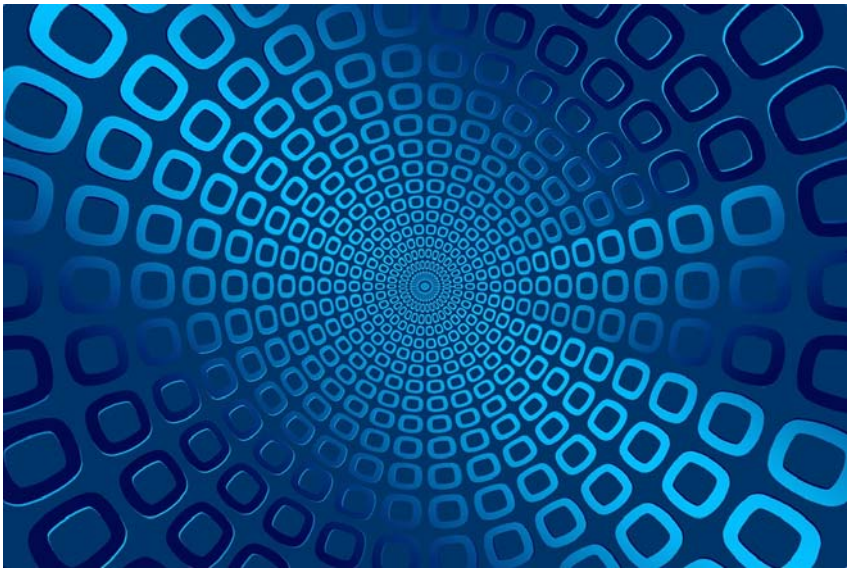
PREPARED BY

GalkinLaw

internet law · new media law · technology law



Preparing Open Source Software Compliance Guidelines

GOT QUESTIONS ABOUT OPEN SOURCE SOFTWARE?

CONTACT US FOR A FREE CONSULTATION AT

WWW.GALKINLAW.COM | INQUIRIES@GALKINLAW.COM | (410) 484-2500

PREPARING OPEN SOURCE SOFTWARE COMPLIANCE GUIDELINES

INTRODUCTION

The purpose of these Open Source Software Compliance Guidelines (Guidelines) is to provide guidance in the development of procedures designed to verify compliance with the license requirements of various open source software applications and code (OSS) used internally or included in products for distribution.

1. BASIC COMPLIANCE COMPONENTS

The output of these Guidelines should be (1) an Open Source Software Compliance Policy (OSS Policy) that describes the policies and procedures applicable to the company's use of OSS, and (2) an inventory (OSS Inventory) of all OSS approved for use within the company.

The OSS Policy must be designed with the company's culture and specific way of operating in mind in order to be effective. The OSS Policy should also be reviewed and updated on a regular basis.

The OSS Inventory is the ultimate output of these Guidelines and the OSS Policy. However, it will also serve as a ready document, in modified form, that can be provided to customers that may request a listing of OSS contained in distributed products and to a potential partner or acquirer which is performing due diligence.

It is important to note that 3rd party proprietary software will often contain OSS components. Therefore, particularly when such software is being included in a distributed product, it is necessary to have the vendor identify all OSS components so that they can be considered along the lines as set forth below.

2. DESIGNATED GATEKEEPER

A person or committee should be designated for approval of all OSS proposed to be used internally or included in products for distribution. In order for this procedure to be effective, notice must be provided to relevant company personnel that the company requires prior approval of all OSS utilized in any manner within the company. Such notice must be conspicuous and repeated at regular intervals. In addition, supervisors must also be instructed to reinforce this requirement. Special attention must be paid to development teams which are accustomed to pulling OSS from various places, and usually operate subject to tight deadlines.

3. REQUEST FOR APPROVAL

Requests for approval should be submitted within the amount of time prior to use/implementation as stated in the OSS Policy. The approval process should be initiated with the submission of a document that contains at least the following information:

1. Name/Version Number/Source of Open Source Software
2. Name of Applicable License (e.g., GNU General Public License v.2, zlib, BSD), and Source Address for the License
3. Name of Entity/Person Granting License
4. Source Address from which OSS will be Obtained
5. Description of How OSS will be Used (e.g., internally, as a development tool, embedded in distributed product, etc.)
6. If included in distributed product, description of the manner in which these OSS will interact with the company's proprietary source code (i.e., will the OSS be compiled and/or linked statically or dynamically with the company's proprietary source code?)
7. The manner in which the OSS will be implemented (e.g., modified vs. unmodified, standalone, statically linked, dynamically linked, etc.).
8. Description of whether the OSS will be modified
9. Statement as to whether the OSS is a key product component
10. Statement as to whether the OSS is well-known and widely used
11. Target date for OSS use/implementation

4. APPROVAL PROCESS

The approval process involves examining risk areas relating to using the particular OSS. Risk areas may include:

1. Does the OSS license require making modified source code publicly available?

2. Does the OSS license require that source code for company's proprietary software be made publicly available? (e.g., will there be static linking of GPL code with company's proprietary software?)

3. Has there been litigation or other issues relating to the subject OSS?

4. Does the OSS license contain ambiguous terms, thereby potentially placing a cloud on company's rights to use the OSS in a certain manner?

5. Will lack of warranties and intellectual property indemnification pose a risk to company vis-à-vis customer expectation and demands?

It is important that the approval process be conducted quickly, and the expected time period for approval should be set forth in the OSS Policy. Otherwise, users and developers are likely to get frustrated and find ways to get around the procedures as deadlines approach.

When new versions of approved OSS are used, an expedited approval process should take place. This allows the OSS Inventory to be kept up to date, and will prevent gaps forming in the inventory that could end up becoming large holes.

5. COMPLIANCE

The goal of an OSS Policy is to achieve compliance with each OSS license. Depending upon the licenses involved, compliance may include any of the following:

1. Inclusion in appropriate documentation of warranty disclaimers, liability exclusions, author attribution, and proprietary rights notices.

2. Inclusion in appropriate documentation of the applicable OSS end user license agreement.

3. Public delivery or availability of source code for the unmodified version or the modified version.

4. Public delivery or availability of source code for company's proprietary software if linked to a "copyleft" open source software code in a manner that requires this result.

5. Marking of modifications made to the OSS source code.

6. AUDITS

On a periodic basis, at least annually, an audit should take place to verify that the OSS Inventory is accurate and up to date. The audit process can be as simple as distributing the OSS Inventory to key personnel who will sign off on it, or as complex as installing monitoring software that will identify OSS on the company's computer system. The extent of the audit will depend upon company's needs and the volume of open source OSS in use.

7. OSS TRAINING

Current and new employees should participate in an OSS Policy training session to ensure that they are aware of the company's procedures and requirements in this area.