

Basic Playbook for SAAS Open Source Compliance

Keep track of what you are using. Someday you will have to provide a list of what you are using, and you will wish you had kept track along the way. Most open source software downloads have a file called “license.txt” in them. You should keep a copy of the license file, and note what software it covers, so you know what license terms you need to follow. Most small companies do this with a simple spreadsheet. If you are playing catchup, try using FOSSOLOGY, a free software tool. It will not find all open source code in your product, but it will find most of the license notices. <http://www.fossology.org/projects/fossology>. There are many other tools available, particularly for Java and other high-level code, such as White Source and TLDR Legal. This is a quickly moving field, and there are new tools all the time. Let me know if you want introductions to any tool providers.

SAAS makes it easier to comply. For SAAS use, almost none of the major open source licenses have any conditions. There are some exceptions, but they are relatively rarely used. They are:

- Affero GPL
- Academic Free License
- Open Software License
- CPAL (Common Public Attribution License)
- Mozilla Exhibit B licenses such as the SugarCRM Public License. These are licenses that add an “Exhibit B” with attribution requirements to the Mozilla Public License. They are rarely used.

Someday you will distribute. Almost all SAAS companies eventually distribute their software - to a customer who wants to maintain a private instance, to an affiliate, or in an asset sale. With this in mind, you should develop a full open source compliance program that will make it possible to distribute your product without rewriting it. The main objective is not to integrate GPL and LGPL code into your product except in ways in which you could, theoretically, distribute in compliance with the licenses. For GPL, this means using the code as a stand-alone program, and for LGPL, this means using the code as a dynamically linked library. An easy guideline to follow is that for most open source code, if you don’t modify it, you will not be likely to violate the license. So, you can limit your review to code that you modify.

Client Side Scripts. SAAS and cloud systems all distribute some software elements -- most notably Javascript. For those elements, be sure to follow the license conditions. Because most client-side code is scripting code (i.e. it executes in source code form), compliance will mainly consist of including a license notice. If you have minified the code (such as by deleting whitespace), you may be asked to provide the unminified source code, but such requests are rare.

Mobile Apps. This is a special instance of distributed software. Only use software under permissive licenses. It is difficult to abide by the requirements of LGPL or GPL in mobile apps, given the rules of the app stores, so avoid code under those licenses. Include all the notices for the open source software in your apps, preferably in a notices file or page accessible by the app user on the device without internet connectivity.

Don't use code with no license terms. No license terms means no license. If you find code with no license, ask the author to apply a permissive license, like MIT or even CC0 (a public domain dedication).

Contributions and Releases

Do not sign a contribution license, contribute to an open source project run by someone else, or release your software under an open source license without talking to your lawyer first.

Contributing and releasing code may be the right choice for your business, but you need to make the choice wisely. Once you make a contribution or release, the IP rights you had in the software probably will never again be a basis for valuation of your company.

Basic Playbook for Use of Open Source in Mobile Apps*

Keep track of what you are using. Someday you will have to provide a list of what you are using, and you will wish you had kept track along the way. Most open source software downloads have a file called “license.txt” in them. You should keep a copy of the license file, and note what software it covers, so you know what license terms you need to follow. Most small companies do this with a simple spreadsheet. If you are playing catchup, try using FOSSOLOGY, a free software tool. It will not find all open source code in your product, but it will find most of the license notices. <http://www.fossology.org/projects/fossology>. There are many other tools available, particularly for Java and other high-level code, such as White Source and TLDR Legal. This is a quickly moving field, and there are new tools all the time. Let me know if you want introductions to any tool providers.

No GPL or LGPL. It is virtually impossible to comply with these licenses in mobile applications. Only use code under permissive licenses like BSD, MIT, or Apache, or code in the public domain. It is also OK to use code under Mozilla Public License or Eclipse Public License, but relatively little code under these licenses is used in mobile app development.

Don’t use code with no license terms. No license terms means no license. If you find code with no license, ask the author to apply a permissive license, like MIT or even CC0 (a public domain dedication).

Mobile Apps are Distribution. All code in a mobile app is considered to be distributed for the purposes of open source compliance..

Do it Right the First Time. Once your app is in the store, if you have used open source code without complying with the license, the author of the code can issue a takedown request to the store. The company running the store (such as Apple) can take the code down from the store if it decides you have not complied. You don’t want your app to be gone from the store, so be sure to get it right.

Notices. Put all of your license notices in a place that is accessible to the user (such as via button on the home screen for your app). This should include a copy of all the licenses for the open source code you used.

*Note: this playbook overlaps with the “Playbook for SAAS Open Source Compliance.”