revenera

A USER'S GUIDE TO

Open Source License Compliance

Not all open source licenses are the same. Users must adhere to individual license requirements, like preserving copyrights and license text and providing attribution in About boxes, documentation and source code. Below are popular licenses and a high-level view into compliance obligations.

AGPL 3.0
Any code modifications require you to give users access to the corresponding source via a network server
Strong Copyleft

GPL v3
Derivative work must be distributed with same license terms; users can modify the source code if used in a consumer product
Strong Copyleft

GPL v2
May distribute code in product if you meet all license obligations despite any conflicting obligations
Strong Copyleft

LGPL v3
Users must make available complete source code of licensed works and modifications under the same license
Weak Copyleft

LGPL v2.1
Must release this library's source if you distribute it with your product
Weak Copyleft

EPL -or- MPL
Must release this library's original source code and any modifications if distributing with product
Weak Copyleft

Apache 2.0
Can use code for any purpose but must preserve copyright, patent, trademark and/or attribution
Permissive, Non-Copyleft

BSD -or- MIT
Can use, distribute, or modify code for any purpose but must preserve copyright message/attribution
Permissive, Non-Copyleft

Creative Commons (CC)
Various licenses; all allow creators to retain copyright while others use the work; obligations vary depending on which CC license is used
From Strong Copyleft to Public Domain

Public Domain
Contains no legal, copyright, or editing restrictions; can be publicly modified and distributed

Commercial
Must respect the terms of the commercial license this code is under (typically involves payment and NDAs)

No License Seen
No permission to use this source code for any purpose without an explicit license from author

Open Source Compliance Checklist

- [ ] Do we have an open source usage policy?
- [ ] Do we have an up-to-date list of ALL the open source and commercial libraries we are using?
- [ ] Does this list include all libraries brought in through repository managers? (e.g. Maven/Ruby Gems/npm, etc.)
- [ ] Do we have a whitelist of approved open source licenses?
- [ ] Do we have a list of all the web services we depend on? (e.g. credit card processors, stock price lookup, etc...)
- [ ] Do we have open source disclosures from our commercial suppliers and third-parties?
- [ ] Are we minifying our JavaScript?
- [ ] Where are the originals kept?
- [ ] Do we preserve copyright and license statements?
- [ ] Do we have a policy for the proper usage and attribution of code snippet Cut and Pastes?
- [ ] Do we publish the component and license disclosures as required by our open source libraries?
- [ ] Do we send along all required License and Notice files as required by our open source libraries?
- [ ] Could we quickly comply with a request for our GPL/LGPL source code?
- [ ] Do we check our open source libraries for known vulnerabilities on the National Vulnerability Database?