Open Source License Best Practices

QUICK REFERENCE

SPDX License IDs

- One new comment line per file
- Human & machine readable
- Uses the SPDX License List
- Add to **every** file

```
// SPDX-License-Identifier: MIT
/* SPDX-License-Identifier: MIT OR Apache-2.0 */
#  SPDX-License-Identifier: GPL-2.0-only
```

https://spdx.org/ids
https://spdx.org/licenses

Choose Your License

- Standard / OSI Approved
- Project / OSPO Policy
- Permissive or Copyleft
- The right license for the file
- Copyright Notice ≠ License

License Type

- Source Code (E.g. Apache 2.0)
- Documentation (E.g. CC-BY-4.0)
- Specification (E.g. Community-Spec-1.0)
- Data (E.g. CDLA-Permissive-2.0)

Don't use a source code license for docs, specs or data!

Open Source License Basics

- Use, copy, and modify the source code
- Redistribute and create derivative works
- Typically NO warranty
- Usually required to give attribution
- Copyleft license terms extend to derived works

Not Open Source

- Source Available
- Fair Source
- Has Use Restrictions
- Closed Source (even if viewable)
- No License Specified

Important Tips

- Do not copy code with an unknown license
- Don't remove others' copyright or license info
- Use a DCO for your project
- Your OSPO is your friend, talk to them
- Add an SPDX License ID to every file possible

License Obligations

A License May Require:

- Attribution
- Redistribution
- Allow Reverse Engineering
- Make Source Code and Modifications Available
- Release Under Same License

Common License Conflicts

- Copyleft with Permissive Source (some cases)
- Copyleft with Closed Source (most cases)
- Use Restrictions (e.g. non-commercial)
- Source Available with Open Source

Policy Best Practices

- Set a clear policy for both inbound & outbound open source code
- Use an SCA tool to find & track all licenses
- Scan both Source & Dependencies
- Comply with all License Obligations including Attribution requirements
- Generate a Build SBOM in your CI/CD pipeline

External Resources

- **SPDX:** System Package Data Exchange - spdx.dev
- **OSI:** Open Source Initiative - opensource.org
- **OSPO:** Open Source Program Office - todogroup.org
- **DCO:** Developer Certificate of Origin - developercertificate.org
- **SBOM:** Software Bill of Materials - cisa.gov/sbom
- **OpenChain:** openchainproject.org
- **REUSE Software:** reuse.software
- **GitHub License Selector:** choosealicense.com

Disclaimer: This is not legal advice, please consult your own legal counsel.
Information provided here is a summary, please follow the links for additional information.

https://linuxfoundation.org/licensebestpractices