Open Source Software Compliance

getting it right

Open Source Software Compliance – getting it right

FOSS – Free and Open Source Software has been described as “software distributed under a licensing agreement which permits code to be shared and edited by other parties”.

An overwhelmingly high percentage of companies use Open Source Software for their mission-critical projects, and for good reasons. Open Source Software is flexible, agile, adaptable, and scalable. It allows you to innovate without having to haggle over terms and conditions or wait for proprietary software to catch up. An eco-system community keeps it constantly refreshed and maintained and thereby helps you reduce time to market. And, while its acronym FOSS is misleading (Open Source Software is rarely free), it is generally far less expensive than proprietary software allowing companies to focus their investments on the aspects that differentiate their offerings.

For commercial projects, however, both technical and legal resources are needed to manage the use of Open Source Software in a fast-paced world. Due diligence must be applied to not find your mission-critical product or service inadvertently attracting unexpected costs or breaking the law. The Software Compliance Academy and KDAB have, supported by OpenChain and TÜV SÜD, teamed up to offer a package solution to protect against legal risks and unnecessary costs:

A FOSS Compliance Audit with optional ISO Certification

Licensing Agreements – ensuring full compliance with the law

Just like individually negotiated proprietary software licenses, Open Source Software licenses are linked to case-specific licensing conditions. These can be exceedingly complex, especially where multiple interacting software layers, including proprietary software and open-source components, are involved. Almost all companies active in the software industry receive software packages from elsewhere that are implemented in their products before being externally distributed. Selling commercial products, including Open Source components, makes companies responsible for ensuring compliance with applicable license obligations at the same time as protecting both their intellectual property and that of third-party suppliers and customers. Failure to comply with license obligations can result in severe consequences, such as loss of license, breach of contract, recall of shipped products, financial penalties and personal liability of corporate management. The **Software Compliance Academy** has many years of experience helping its clients to implement license and compliance strategies to mitigate these risks and reduce transaction costs in the software supply chain. Their interdisciplinary team offers legal, technical, and strategic advice as well as related training modules for your staff.

Source Code – ensuring best practices and detecting compliance risks

Multiple interacting code bases and diverse teams can increase the risk of inadvertent breaches in compliance when using Open Source Software. Not all developers are equally aware or educated on what is needed to ensure compliance at the code level. Best practices are not always followed to ensure open-source code is traceable, integrated, extended and maintained in compliant ways. These issues can be detected and overcome by having a source code technical audit conducted by a trusted expert. **KDAB** engineers have worked with Qt, one of the most extensive and most successful Open Source Software development toolkits, for over 20 years. In addition to being technical experts, KDAB is used to bridging the commercial and open-source worlds and helping customers select the right Qt licensing option. A KDAB audit will analyze your code for any compliance risks and questionable practices and give you a complete diagnostic report with recommended solution pathways and safeguards to bring it up to certification standard. KDAB can also offer best practice strategies, tooling and infrastructure suggestions, as well as training for your development team, should that be required. Compliance is an ongoing practice involving systematic checks and updates both at a legal and technical level. Together, KDAB and Software Compliance Academy will help you establish compliance best practices going forward, so your company remains up-to-date and compliant as your projects evolve. Having an established, best practice-based process in place to ensure ongoing compliance will speed up source code upgrades and updates, thus reducing the cost of your projects.

ISO Certification – proving you can be trusted

In a competitive market, it's not enough that your products and services are compliant. You need to prove that they are, both now and in the future. The newly established ISO/IEC 5230:2020 standard specifies the critical requirements of a quality Open Source license compliance program, thus providing a benchmark that builds trust between organizations exchanging software solutions comprised of Open Source software. The development and

implementation of an ISO 5230:2020 compliance program will help your company compete in innovative and evolving markets.

Certification of an ISO 5230:2020 compliance program will verify compliance and confirm that your company can effectively manage the use of Open Source Software in commercial products so that potential licensing conflicts can be avoided and legal risks minimized. As a final step, we recommend a request be made to TÜV SÜD for certification under ISO 5230:2020.

In Summary

With their combined expertise and experience, Software Compliance Academy and KDAB are uniquely able to audit your use of Open Source Software at the legal and technical level. They can find issues, suggest solutions, recommend best practices and suggest improvements to processes and software development infrastructure. Following the Software Compliance Academy and KDAB's guidance on Open Source Software compliance strategies and processes for your company, TÜV SÜD can certify your compliant use of Open Source Software, based on the ISO 5230:2020 standard, if you wish. The team will guide you through the entire process, from taking stock of the status quo until you hold your certification document in your hands.

The Software Compliance Academy is a private and independent institute specialized in software compliance. Their interdisciplinary team offers support to develop and implement effective and efficient compliance systems and related training modules. **https://www.scompliance.com/home.html**

The KDAB Group offers experienced software experts to help clients deliver functional, high-performing and innovative software across embedded, mobile and desktop platforms. ISO 9002 Certified KDAB offers consulting, development, workshops, mentoring, effective processes and tools, as well as market-leading training in Qt, modern C++, OpenGL and more. **https://www.kdab.com/**

TÜV SÜD Part of the German TÜV organizations, which test and certify road worthiness of German vehicles, as well as the safety and compliance of a wide variety of consumer goods, TÜV SÜD has been a leading authority in the field for the last 150 years. TÜV SÜD adds value to partners and customers through a comprehensive portfolio of testing, certification, auditing and advisory services. **https://www.tuvsud.com/en**

OpenChain ISO 5230 is the International Standard for Open Source Software license compliance. It is simple, effective and suitable for companies of all sizes in all markets. This standard is openly developed by a vibrant user community and freely available to all. It is supported by free online self-certification, extensive reference material and official service provider partners. **https://www.openchainproject.org/**

tQCS is a IT software consultancy company in Asia, providing comprehensive embedded software solutions from Europe via localized consulting excellency. Combining technology, solution and consultancy, tQCS provides the state-of-the-art embedded software experiences based on open source standardization for the customers in industrial, medical, defence and automotive industries in Asia-Pacific. **https://www.tQCS.io/**

For more information on the service, please https://www.tqcs.io or send your inquiry to project.compliance@tqcs.io
tQCS is an exclusive provider of ISO5230 certification in Asia-Pacific region to ensure customers can stay compliant with their choice of open-source licensing.