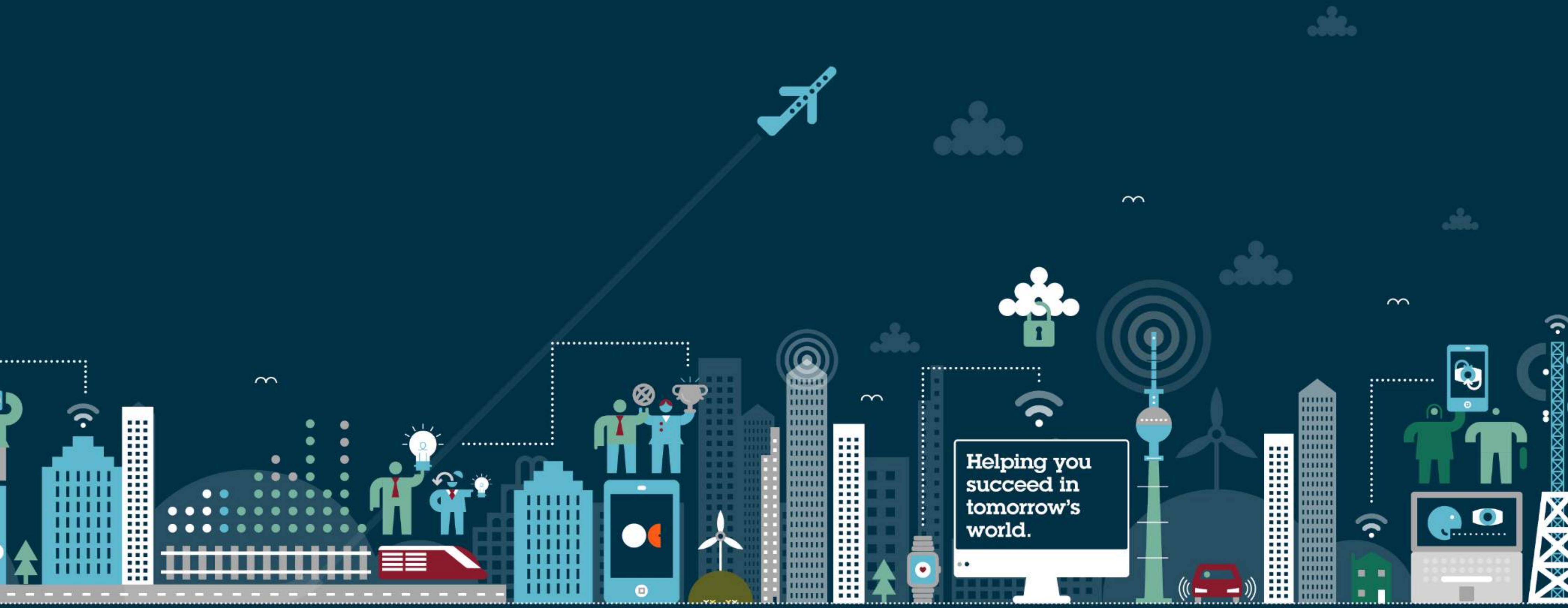
Open Source Compliance Report

Current Figures on Compliance Processes and Specific Measures in Germany

Detailed Assessment of the BITKOM Open Source Monitor



Content

Editor

Osborne Clarke Rechtsanwälte Steuerberater Partnerschaft mbB
Nymphenburger Strasse 1
80335 Munich
Germany

Contact

Dr. Hendrik Schöttle
hendrik.schoettle@osborneclarke.com

Interested in our German language version of this report?
Please visit osborneclarke.com/oss

9D85122103102116

1 Introduction

When using Open Source Software (OSS), there is no way around OSS compliance. Besides IT security, this primarily includes compliance with license requirements. Anyone involved in Open Source Compliance knows that implementing this is anything but easy. In particular, Open Source Compliance does not come for free.

In many cases, there is a gap between expectation and reality in the area of OSS compliance. Full compliance is barely affordable, but the risks of legal disputes in cases of violations of OSS license terms cannot be dismissed. Difficult times for compliance officers approaching this issue.

Noncompliance can result from breaches of license obligations, but also from the incompatibility of licenses. The consequences of such infringements are manifold and can range from a formal warning to the removal of products from the market. In the recent past, we have observed a qualitative increase as well as an increase in the number of violations being prosecuted by individual developers. We have also noticed that more and more companies have recently been asking their suppliers to provide evidence of OSS compliance measures in order to protect themselves. However, since the cost of comprehensive OSS compliance is high, many companies shy away from the effort altogether – even though there are solutions that can help to get the major risks under control at reasonable expense.

For a long time, no figures existed on the topic of OSS compliance. Companies looking for orientation, wanting to compare themselves with their peer group, were left in the dark and could only get an approximate picture by questioning their own contacts. What measures should I take? Should I ignore the issue and let it go by, or should I proactively take action? If so, in what way? Where do I stand in comparison to others? Statistically backed answers to these questions did not exist.

This gap has now been closed with a study commissioned by BITKOM and financed by Osborne Clarke and other partners[1]: In the course of the BITKOM Open Source Monitor, 804 companies based in Germany, each with 100 employees or more and from various industries, were interviewed with regard to their handling of OSS. Osborne Clarke was involved in the drafting of the study. The key figures of this study on the topic of OSS compliance are summarised and evaluated in this report. Additionally, this report contains further figures which cannot be found in the BITKOM Open Source Monitor, but which are based on the underlying raw data.[2]

> With this report, companies for the first time can see how they perform in the field of OSS compliance – not only with regard to the general question of whether compliance processes exist, but also in a detailed way, specifically with regard to individual compliance measures. The study also allows for a direct comparison with one's own peer group, as the presentation distinguishes the surveyed companies by size, according to the number of employees.
>
> *Dr. Hendrik Schöttle, Partner, Osborne Clarke*

[1] Other partners of the study were Boehmert & Boehmert, DataStax, PwC, Red Hat, SAP, SUSE, Synopsis and the Technische Universität Berlin. Source for all following figures: BITKOM Research 2019.

[2] The study which was released in spring 2020, distinguishes between companies of different sizes, depending on the number of employees. In the study, the results were weighted according to the interviewed base groups in order to adjust the number of cases to the actual distribution within the economy. The results of the study presented here may thus deviate from the absolute results of the interviews.

2 Key Figures at a Glance

69.3 % of all companies interviewed use OSS, but only 11 % have an OSS policy (see 4.2)

76 % of the respondents believe that all companies somehow use OSS, but are often unaware of it (3.1)

Fun Fact: At least 3.2 % of respondents say they do not use OSS, but at the same time believe that this statement cannot be correct (3.1)

Almost 20 % of all surveyed companies use OSS for development or as part of their own products and solutions for their customers and modify the source code (3.2)

42.9 % of the respondents have a compliance process in place (4.3)

46.7 % of the respondents think that there is a great need to introduce or improve compliance processes (4.3)

As far as compliance measures are concerned, there is a significant backlog with regard to their correct prioritisation: the most important measure when transferring OSS, the bill of materials, ranks lowest within the compliance measures most frequently mentioned on average (5.1)

7.6 % of all surveyed companies using, integrating, developing/amending or participating in OSS have been involved in legal disputes (6.3)

Among companies with 2,000 or more employees that develop/enhance OSS, 17.7 % have been involved in legal disputes related to OSS.

59.1 % of the companies against which legal action has been taken have set up a compliance process in response. In one case, a product has been withdrawn from the market (6.5)

More than 69% of all companies surveyed are using open source software – but less than 21% of them have a strategy for dealing with OSS and only 11% of those using OSS have an OSS policy.

Companies still need to catch up in the area of OSS compliance. Although they use OSS, many companies do not ensure that the license conditions for deployment are met. Strategies, OSS policies and compliance processes are often lacking. Such structural deficits can affect not only the company itself, but in the worst case also the management in person.

In many cases there is a lack of OSS policies and compliance processes. But even where compliance processes exist at a company, they often fail to focus on the proper issues. Especially in the area of information and documentation requirements, many gaps are still to be closed.

Legal disputes do occur, providing another argument for taking OSS compliance seriously. Anyone exposed to a legal dispute must immediately achieve OSS compliance – especially where preliminary injunctions are lurking. It is all the better if this demanding project can be addressed without time pressure.

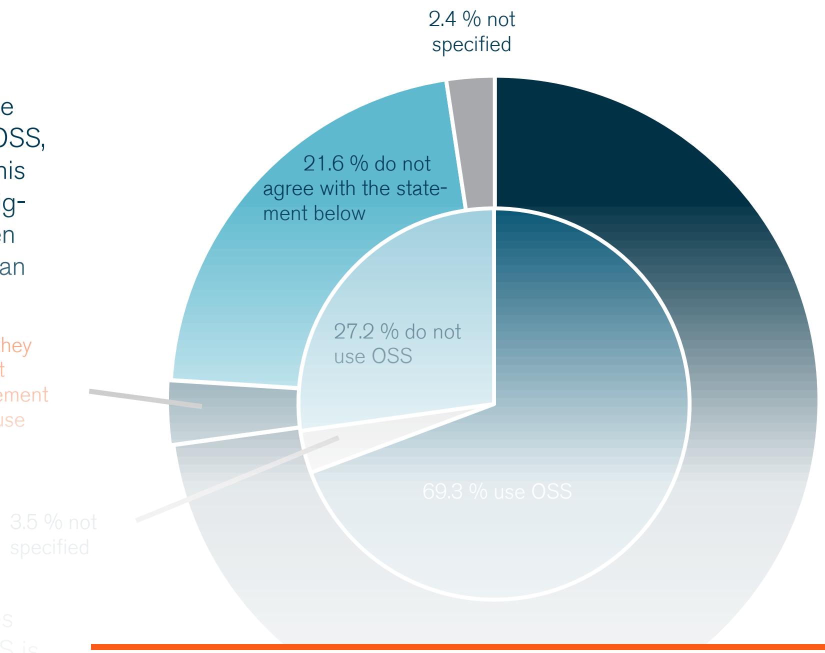
However, nowadays solutions are available to get the matter of OSS compliance under control at reasonable expense. As in many cases, the usual 80/20 approach helps: Within the course of a risk analysis, the actual risks in the area of OSS compliance are identified and specifically addressed. Compliance processes and policies are then tailored to the individually identified risk, thereby minimizing the necessary effort as far as possible.

Dr. Hendrik Schöttle, Partner, Osborne Clarke

3 How is OSS Used?

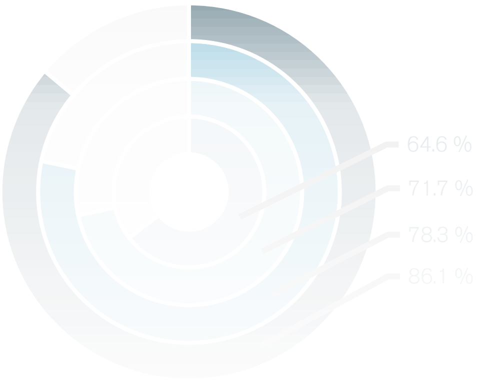
3.1 Is OSS Used at all?

69.3 % of all respondents said that they use OSS in their company. 27.2 % do not use OSS, while 3.5 % did not answer the question. This finding is not surprising, although the real figures for the use of OSS are likely to be even higher. According to other surveys, more than 95 % of software examined in 2018 contained open source software components. Assuming that every company surveyed uses software in some form – be it the operating system of the employee's smartphones – the figure of 69.3 % is probably too low. In practice, it can still be observed that many companies continue to be unaware of the fact that OSS is being used.



At least 3.2 % say they do not use OSS, but agree with the statement that all companies use OSS in some way.

Across all company sizes, one in five respondents said that they use OSS to develop or as part of their own products and solutions for customers, without making adjustments to the source code (22.3 %). For large companies with more than 2,000 employees, the number rises further to around a third of those surveyed (33.3 %). Overall, OSS is used much more frequently for all purposes, including those that go beyond the foregoing, in 86.1 % of all companies with more than 2,000 employees.



**Curious about the rest?
Simply send an e-mail to
oss@osborneclarke.com
for the complete report.**

8 FOSSmatrix. Legal Tech Add-On for OSS Compliance

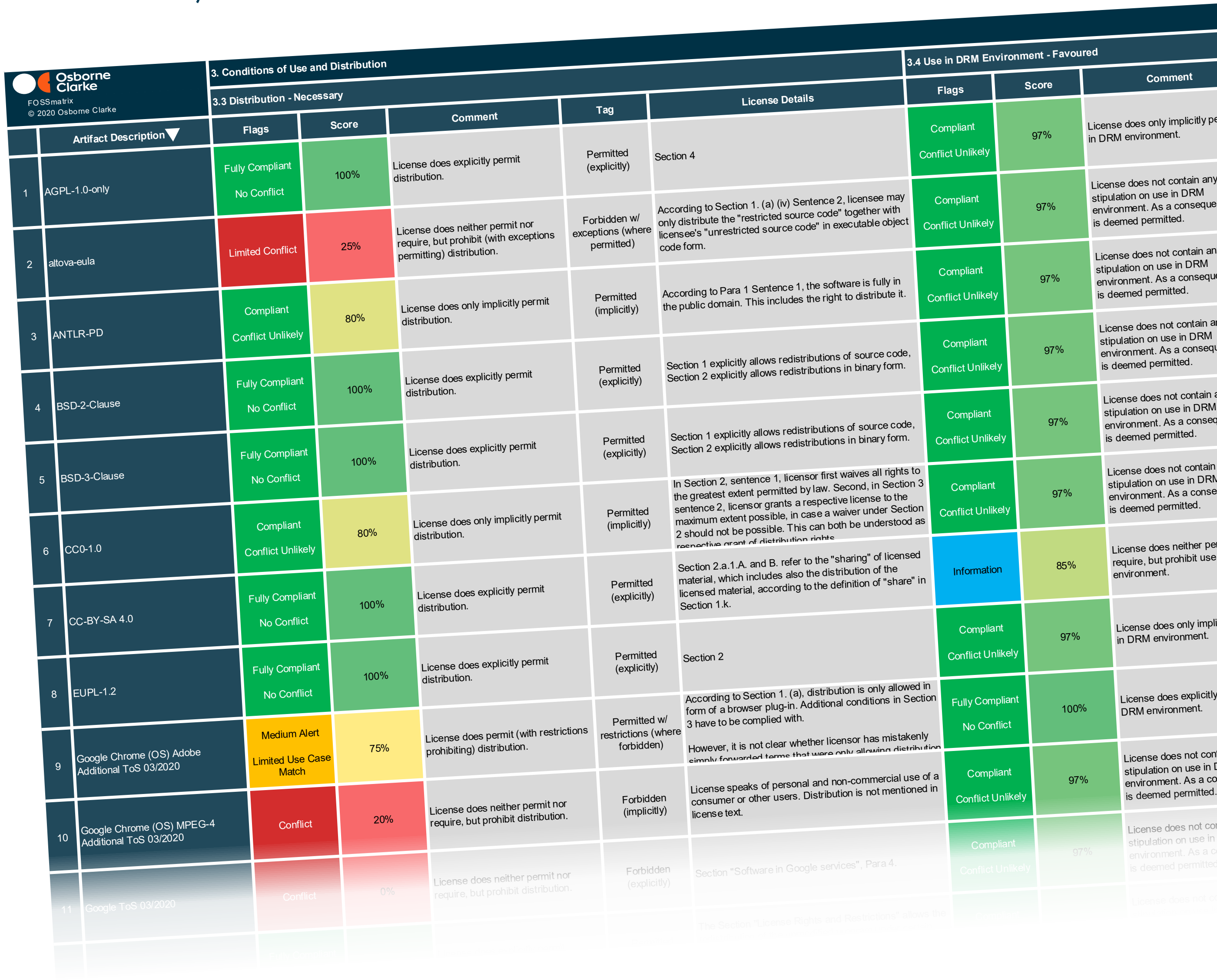
The Legal Factor in the Compliance Process – Measurable, Automatable and Auditable

Basis is a standardized legal assessment of proprietary and open source licenses and components. Legally compliant and fully documented. Even in view of complex legal issues.

Features

- **Mapping** of individually tailored use cases against licences with clear indication of conflicts, display of risks and reference to individual sources at the level of individual licence obligations
- **Parameterization** of individual factors, allowing for different weighting (conservative approach vs. risk-taking approach)
- **Risk assessment with percentage values**: not just yes/no, but partially fine gradations in percentage range, tracking and visualising cases of doubt

> We start where traditional tools stop: legal classification and assessment of licenses. More than "just" creating a Bill of Materials and fulfilling information requirements



Osborne Clarke FOSSmatrix © 2020 Osborne Clarke		3. Conditions of Use and Distribution							
		3.3 Distribution - Necessary					3.4 Use in DRM Environment - Favoured		
	Artifact Description ▼	Flags	Score	Comment	Tag	License Details	Flags	Score	Comment
1	AGPL-1.0-only	Fully Compliant No Conflict	100%	License does explicitly permit distribution.	Permitted (explicitly)	Section 4	Compliant Conflict Unlikely	97%	License does only implicitly pe in DRM environment.
2	altova-eula	Limited Conflict	25%	License does neither permit nor require, but prohibit (with exceptions permitting) distribution.	Forbidden w/ exceptions (where permitted)	According to Section 1. (a) (iv) Sentence 2, licensee may only distribute the "restricted source code" together with licensee's "unrestricted source code" in executable object code form.	Compliant Conflict Unlikely	97%	License does not contain any stipulation on use in DRM environment. As a conseque is deemed permitted.
3	ANTLR-PD	Compliant Conflict Unlikely	80%	License does only implicitly permit distribution.	Permitted (implicitly)	According to Para 1 Sentence 1, the software is fully in the public domain. This includes the right to distribute it.	Compliant Conflict Unlikely	97%	License does not contain an stipulation on use in DRM environment. As a conseque is deemed permitted.
4	BSD-2-Clause	Fully Compliant No Conflict	100%	License does explicitly permit distribution.	Permitted (explicitly)	Section 1 explicitly allows redistributions of source code, Section 2 explicitly allows redistributions in binary form.	Compliant Conflict Unlikely	97%	License does not contain ar stipulation on use in DRM environment. As a consequ is deemed permitted.
5	BSD-3-Clause	Fully Compliant No Conflict	100%	License does explicitly permit distribution.	Permitted (explicitly)	Section 1 explicitly allows redistributions of source code, Section 2 explicitly allows redistributions in binary form.	Compliant Conflict Unlikely	97%	License does not contain a stipulation on use in DRM environment. As a conseq is deemed permitted.
6	CC0-1.0	Compliant Conflict Unlikely	80%	License does only implicitly permit distribution.	Permitted (implicitly)	In Section 2, sentence 1, licensor first waives all rights to the greatest extent permitted by law. Second, in Section 3 sentence 2, licensor grants a respective license to the maximum extent possible, in case a waiver under Section 2 should not be possible. This can both be understood as respective grant of distribution rights	Compliant Conflict Unlikely	97%	License does not contain stipulation on use in DRM environment. As a conse is deemed permitted.
7	CC-BY-SA 4.0	Fully Compliant No Conflict	100%	License does explicitly permit distribution.	Permitted (explicitly)	Section 2.a.1.A. and B. refer to the "sharing" of licensed material, which includes also the distribution of the licensed material, according to the definition of "share" in Section 1.k.	Information	85%	License does neither pe require, but prohibit use environment.
8	EUPL-1.2	Fully Compliant No Conflict	100%	License does explicitly permit distribution.	Permitted (explicitly)	Section 2	Compliant Conflict Unlikely	97%	License does only impli in DRM environment.
9	Google Chrome (OS) Adobe Additional ToS 03/2020	Medium Alert Limited Use Case Match	75%	License does permit (with restrictions prohibiting) distribution.	Permitted w/ restrictions (where forbidden)	According to Section 1. (a), distribution is only allowed in form of a browser plug-in. Additional conditions in Section 3 have to be complied with. However, it is not clear whether licensor has mistakenly simply forwarded terms that were only allowing distribution	Fully Compliant No Conflict	100%	License does explicitly DRM environment.
10	Google Chrome (OS) MPEG-4 Additional ToS 03/2020	Conflict	20%	License does neither permit nor require, but prohibit distribution.	Forbidden (implicitly)	License speaks of personal and non-commercial use of a consumer or other users. Distribution is not mentioned in license text.	Compliant Conflict Unlikely	97%	License does not con stipulation on use in D environment. As a co is deemed permitted.
11	Google ToS 03/2020	Conflict	0%	License does neither permit nor require, but prohibit distribution.	Forbidden (explicitly)	Section "Software in Google services", Para 4.	Compliant Conflict Unlikely	97%	License does not co stipulation on use in environment. As a c is deemed permitted
		Fully Compliant				The Section "License Rights and Restrictions" allows the			License does not c

What we do

- **Use Case Development**: We tailor customized use cases. Based on our experience we describe together with our clients how software is used

- **Licence assessment**: Based on the identified licences (if necessary, we assist with the identification), we assess the rights and obligations of these licences

- **Matching**: We check use cases for conflicts with the rights and obligations of the identified licences

Our Service Packages

- **Standard Package:** Result of the use case matching, which shows the compliance/non-compliance of use cases with licences in a clear way

- **Extended Package:** Additional, in-depth explanation of the rights and obligations of the individual licences regarding the use cases - a legal memo in tabular form

Optional

- **Assessment of individual software components:** Can be necessary for the licensor's understanding of the licence - this may differ from the general understanding of the licence

- **Graphical evaluation** of the audit results

License Obligations Concerning ASP Use
ASP Provision Allowed
ASP Provision Triggers Main Obligations
0,00%
35,00%
5,00%
47,00%
42,00%
51,50%
100,00%
100,00%
0,00%
100,00%
100,00%
5,00%
53,00%
100,00%
68,00%
34,50%
48,00%
81,00%
34,50%
50,00%
24,50%
63,00%
48,00%
47,00%
35,00%
53,00%
35,00%
48,00%
48,00%
44,00%

9 Support from Osborne Clarke for Open Source

Osborne Clarke is one of the leading commercial law firms in IT and data protection law, with long-standing experience in providing comprehensive advice on OSS, offering the following solutions in the area of OSS compliance:

Training

- In-house training on OSS compliance and licence management
- Development of know-how within the company
- Overview of the basic principles of OSS, the most important licences and their obligations as well as basic compliance requirements

Compliance Policies, Process Implementation

- Establishment and implementation of compliance policies and processes
- Development of a specific risk profile
- Definition of the necessary steps, setup of an open source policy and support in the actual implementation of this policy
- Creation of standardized checklists

Software Clearing

- Scanning of individual components
- Compilation of the necessary information and documents for these components
- Legal check of individual licences, components and types of use of components

Sample Documentation, Quick Check

- Support in compliance with relevant licensing requirements through sample documentation
- Whether embedded software, Internet of things, devices without user interface: support for the implementation of compliance requirements in special cases

Contributions and Own Open Source Projects

- Support in choosing an OSS licence for licensing your own software as OSS
- Strategic consulting for setting up your own OSS projects
- Creation and testing of Contributor License Agreements and Contribution Policies

Support in Legal Proceedings Regarding OSS Licence Violations

- Assistance in the event of dispute
- Support for short-term implementation of compliance measures in the context of disputes

osborneclarke.com/oss

We help to break down the compliance effort into economically reasonable pieces, build a customized concept and provide support during its implementation.

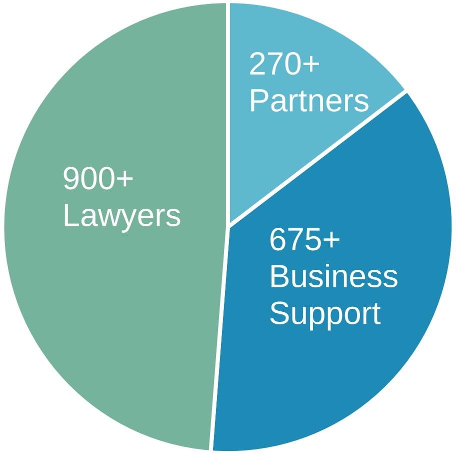
The use of OSS itself is almost unavoidable, but risk control is feasible. In the long term, a company can avoid costs and gain efficiency by introducing and implementing compliance measures.

10 Osborne Clarke International

More than

1,850

employees



26

International locations

Europe:

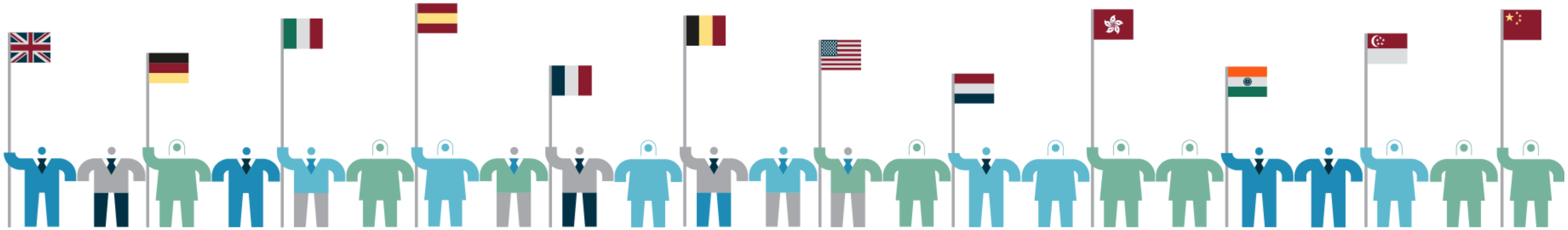
Belgium: Brussels
France: Paris
Germany: Berlin, Cologne, Hamburg, Munich
Italy: Brescia, Busto Arsizio, Milan, Rome
Netherlands: Amsterdam
Spain: Barcelona, Madrid, Zaragoza
UK: Bristol, London, Reading

Asia:

China: Shanghai
India:* Bangalore, Mumbai, New Delhi
Singapore

USA:

New York, San Francisco, Silicon Valley



*Services in India are provided by a relationship firm

11 Contact

„*Top name in the field of Open Source*“

Competitor,
JUVE Handbook
2019/2020

Dr. Hendrik Schöttle
Rechtsanwalt, Partner,
Fachanwalt für IT-Recht

Germany

+49 89 5434 8046
hendrik.schoettle@osborneclarke.com

Dr. Hendrik Schöttle advises on IT and data protection law.

Hendrik is named in 2019 and 2018 by Handelsblatt, by Best Lawyers and by Wirtschaftswoche, as one of the best lawyers for IT law. The JUVE handbook 2019/2020 recommends him as "leading name in the area of open source". In Kanzleimonitor 2018/2019 and 2017/2018 he is listed as a repeatedly recommended lawyer for IT law. He is also recommended by Legal 500 Germany, due to his "very good IT knowledge, even regarding exotic questions" and his "very fast understanding of technical details". In 2015 he received the International Client Choice Award from Lexology and the International Law Office, winning the IT & Internet Law category.

He has many years of experience with consulting, drafting and negotiating of complex IT projects. He focuses on legal matters regarding IoT, digitalisation and cloud computing. He advises on software licensing models, in particular relating to open source software and in the field of data protection law. His clients include international technology groups and well-known IT and e-business companies.

Hendrik became a lawyer in 2005 and joined the Munich office of Osborne Clarke in 2007. He was seconded to legal departments of IT companies several times. In addition, he spent a number of years as a software developer at the Institute for Legal Informatics of Saarland University. His clients benefit from his practical experience and his technical know-how when advising on technology-oriented matters.

He is the author of numerous publications and co-author of several handbooks and commentaries, including the Beck'sches Handbuch IT- und Datenschutzrecht (Handbook on IT law and data protection law) and the juris Praxiskommentar BGB (a commentary on the German Civil Code).

Hendrik is a lecturer in IT law at the Deutsche Anwaltakademie (German Lawyers' Academy) and a frequent speaker on topics relating to IT law.

He is a board member of the BITKOM Working Group Open Source, a member of the Data Protection Law Committee of the German Federal Bar Association, a member of the information technology working group of the German Lawyers Association (DAV), and a member of the German Society for Law and Computer Science.