FOSSmatrix

Next Level Legal Compliance

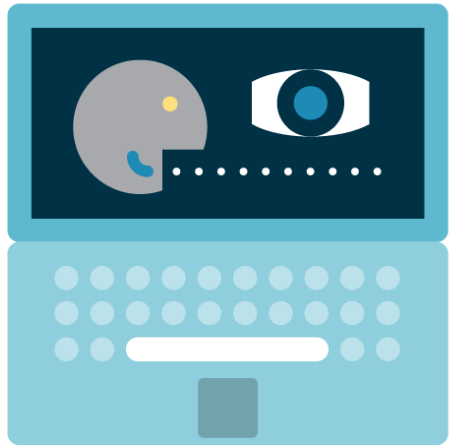
Bitkom Forum Open Source 2022

29. September 2022

Private & Confidential

Agenda

1 Einführung
2 Was ist die FOSSmatrix?
3 Funktionsweise
4 Zusammenfassung



1 Einführung

Einführung – Warum Legal Compliance?

- Warum eine Legal Compliance bei der Umsetzung von Open Source Compliance?
  - Übliches Vorgehen: Raussuchen von Lizenztext und Urhebervermerken, Mitliefern dieser Texte, fertig.
  - Das reicht nicht!
  - In vielen Fällen wird OSS unter Verstoß gegen Lizenzbedingungen eingesetzt!
  - Warum? Entwickler nehmen oft einfach „die neueste Lizenz“, ohne deren Pflichten zu prüfen und ohne sich über die Folgen im Klaren zu sein.
  - Beispiel:
    - Lizenzierung von iPhone-Apps unter der GPL-3.0
    - DRM-Verbot der (L/A)GPL-3.0 in Ziffer 3: Derjenige, der die Software vertreibt, darf kein Digital Rights Management (DRM) einsetzen. Genau das passiert jedoch beim iPhone – dennoch gibt es dafür zahlreiche Apps unter der (L/A)GPL-3.0.

Best Practice | Kompatibilitäts-Check

Bei einigen Lizenzen fehlen zudem Regelungen zur Rechtseinräumung. Bei anderen wird sogar klar darauf hingewiesen, dass Nutzungsrechte fehlen.

Beispiel: LibTomCrypt:

> *LibTomCrypt is public domain. As should all quality software be.*
>
> *All of the software was either written by or donated to Tom St Denis for the purposes of this project. The only exception is the SAFER.C source which has no known license status (assumed copyrighted) which is why SAFER,C is shipped as disabled.*

2 Was ist die FOSSmatrix?

FOSSmatrix – Schritt für Schritt zur Compliance

Lizenz-dokumentation

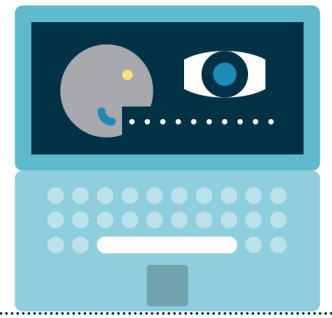
- Welche Rechte und Pflichten ergeben sich aus Lizenzen?

Entwicklung von Use Cases

- Wie wird die Software konkret verwendet?

Mapping von Use Cases

- Bei welchen Lizenzen gibt es Konflikte mit dem Use Case?



Was unterscheidet die FOSSmatrix von anderen Tools?

- Die FOSSmatrix fängt da an, wo die üblichen Scanning Tools aufhören:

  - Input:
    - Use Cases (einmal vorab definiert)
    - Lizenzliste (für jedes OSS-Projekt unterschiedlich
    - Wahl des Use Case
  - Output:
    - Überblick über Konflikte bei einzelnen Attributen der Lizenzen
    - Weitere Angaben zu den Attributen, verweise auf Literatur, Rechtsprechung, etc.

- Scanning Tools: Identifizierung von verwendeten OSS-Komponenten. Management von Compliance-Artefakten (also SBOM, Lizenztexte, Source Code)
- FOSSmatrix: Rechtliche Prüfung und Abgleich von Lizenzen mit konkretem Einsatzszenario (Use Case)

3 Funktionsweise

FOSSmatrix – Beispiel

Ausgangslage

- Ein App soll auf Android und iPhone vertrieben werden.
- Es gibt eine Liste der anwendbaren OSS-Lizenzen (händisch oder via Tool erstellt)

Frage an Legal:

Kann die App mit diesen Lizenzen vertrieben werden?

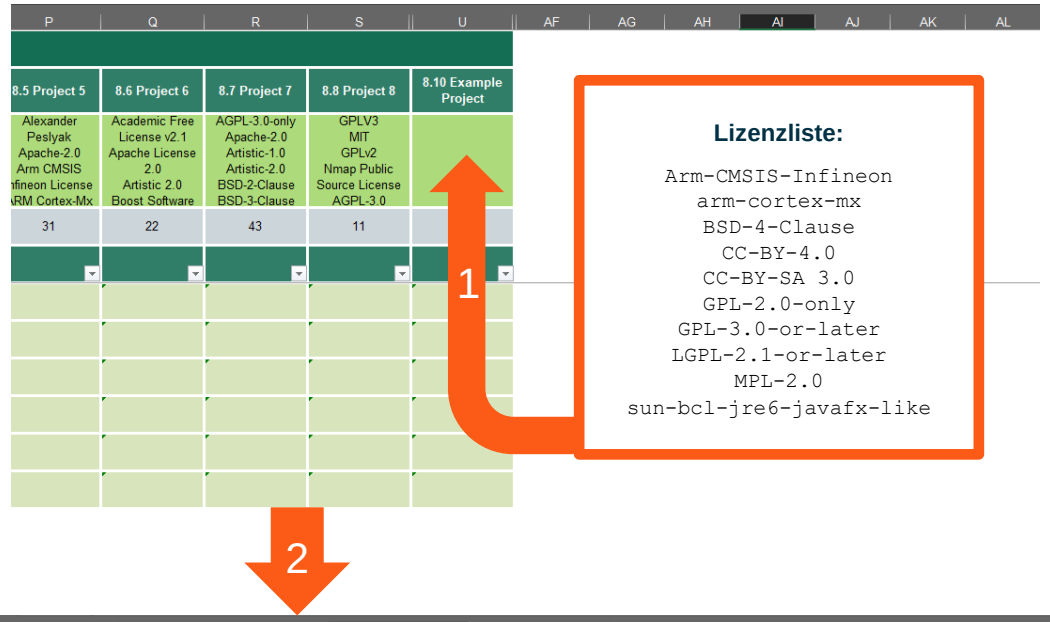
Lizenzliste:

```
Arm-CMSIS-Infineon
arm-cortex-mx
BSD-4-Clause
CC-BY-4.0
CC-BY-SA 3.0
GPL-2.0-only
GPL-3.0-or-later
LGPL-2.1-or-later
MPL-2.0
sun-bcl-jre6-javafx-like
```

FOSSmatrix – Beispiel

1. Auswahl der Lizenzn
2. Auswahl des Use Case
3. Prüfung der Ergebnisse

FOSSmatrix – Beispiel: Auswahl der Lizenzen

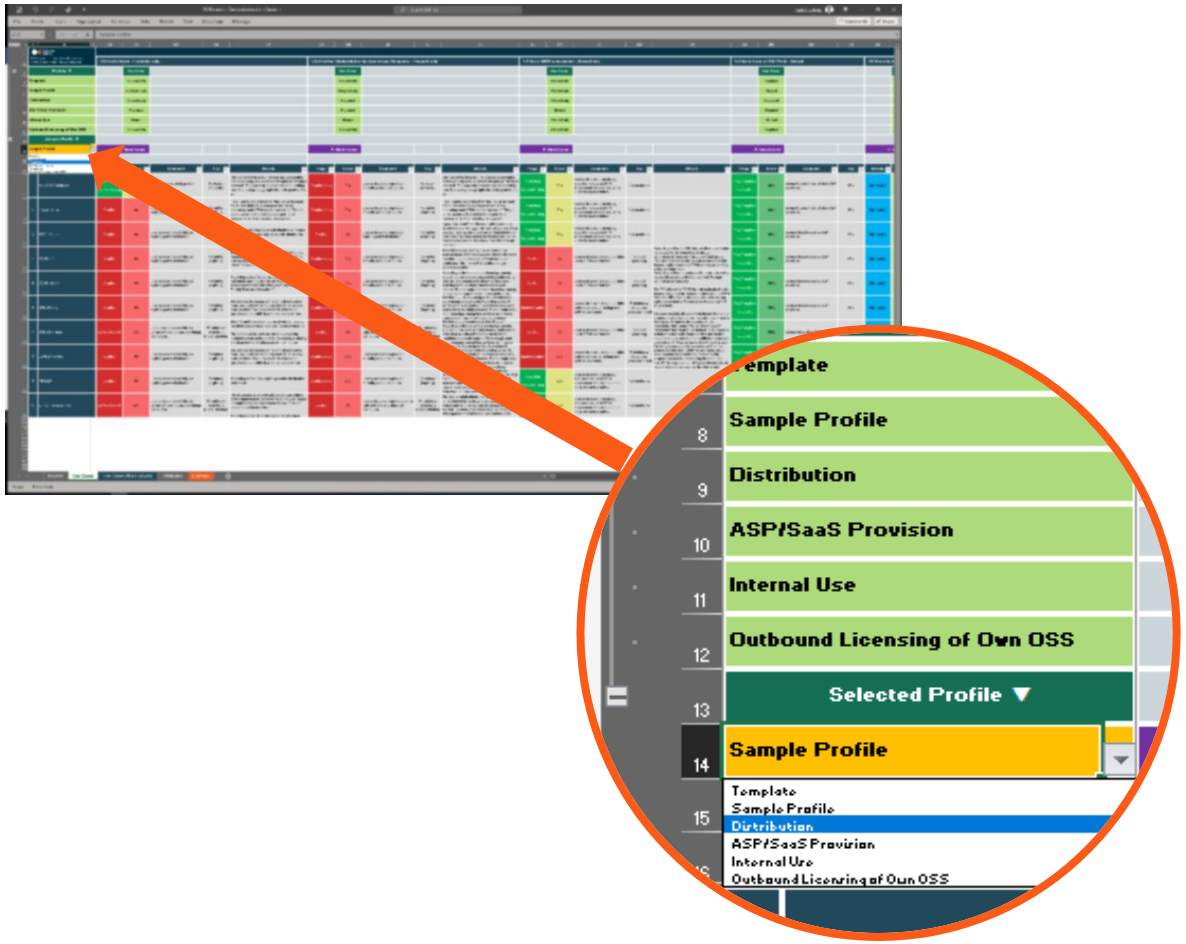


- Die FOSSmatrix verarbeitet händisch oder automatisch zusammengestellte Lizenzlisten.
- Jenseits von SPDX: Viele abweichende Schreibweisen werden erkannt.
- Alle bekannten, relevanten Lizenzen werden dem Projekt zugeordnet.

FOSSmatrix – Beispiel

1. Auswahl der Lizenzn
2. Auswahl des Use Case
3. Prüfung der Ergebnisse

FOSSmatrix – Beispiel: Auswahl des Use Case



- Vordefinierte Use Cases,beispielsweise
  - Distribution
  - ASP/SaaS Provision
  - Internal Use
  - Outbound Licensing of OSS
- Use Cases können auch individuell zusammengestellt werden.
- Beliebig viele Use Cases möglich

FOSSmatrix – Beispiel

1. Auswahl der Lizenzn
2. Auswahl des Use Case
3. Prüfung der Ergebnisse

FOSSmatrix – Beispiel: Use Cases

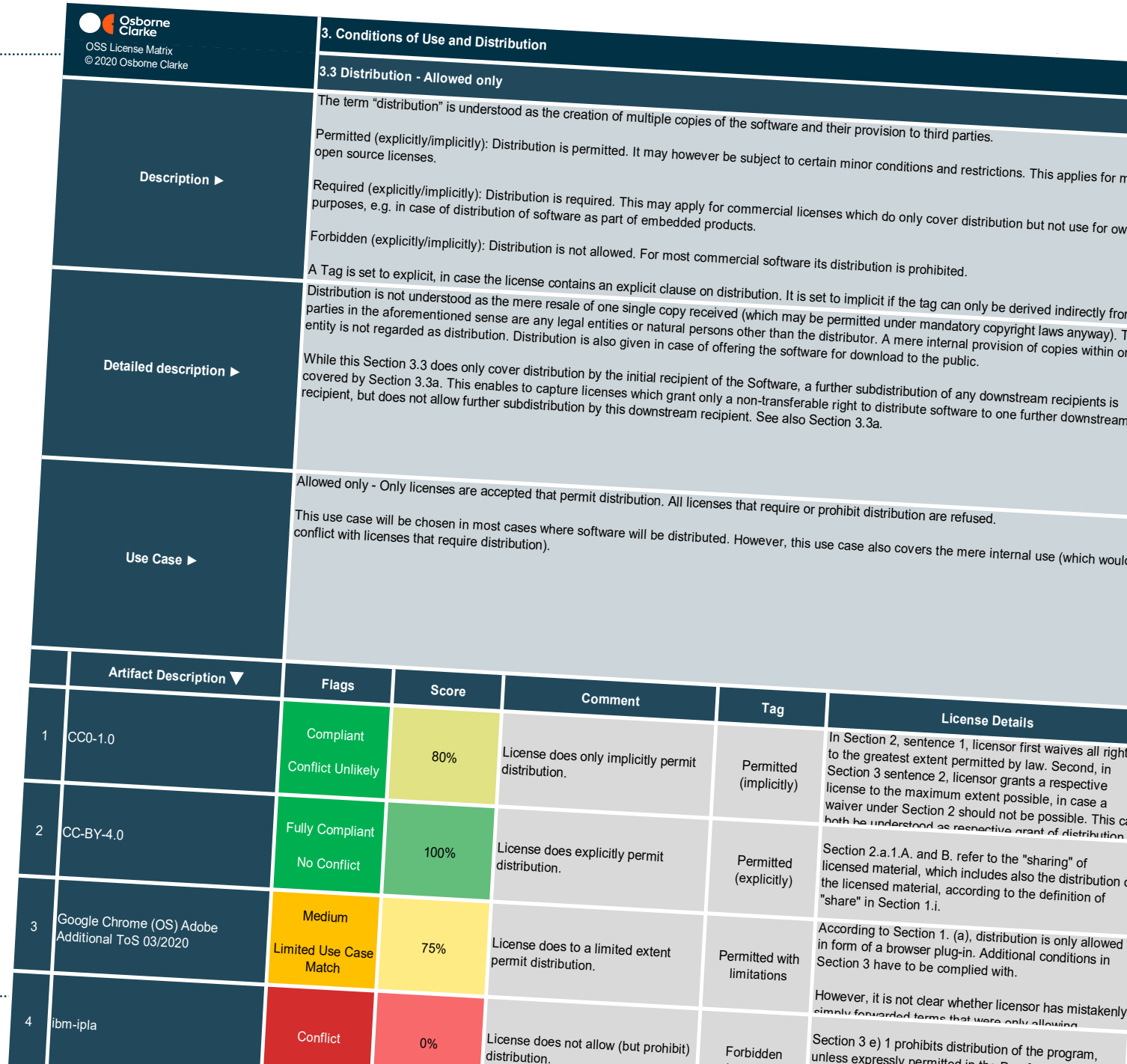
- Risikoanalyse auf der Basis vordefinierter oder individueller Score-Werte
- Eingängige Farbcodierung zur schnellen Risikoanalyse
- Detaillierte Texte zur Erläuterung einzelner Lizenzmerkmale bzw. Risiken des einzelnen Use Case inkl. Quellenangaben

4 Zusammenfassung

FOSSmatrix – Funktionen

Standardisierte Bewertung einzelner Lizenzpflichten

- **Auswertung von Lizenzen**, standardisiert, vollständig dokumentiert und parametrisierbar mit Prozentangaben zur automatischen Weiterverarbeitung
- Derzeit knapp 200 Lizenzen, klassifiziert nach insgesamt 75 Attributen (inkl. Stammdaten). Sowohl „Klassiker“, als auch Exoten und kommerzielle Lizenzen
- Use Case Mapping gegen die jeweiligen Lizenzen mit automatischer Konfliktprüfung
- Keine mehrseitigen Memos – sondern Rechtsberatung als strukturierte Daten
- Mehr als 10 Jahre Erfahrung zu OSS



Osborne Clarke
OSS License Matrix
© 2020 Osborne Clarke

	3. Conditions of Use and Distribution
	3.3 Distribution - Allowed only
Description ▶	The term “distribution” is understood as the creation of multiple copies of the software and their provision to third parties. Permitted (explicitly/implicitly): Distribution is permitted. It may however be subject to certain minor conditions and restrictions. This applies for m open source licenses. Required (explicitly/implicitly): Distribution is required. This may apply for commercial licenses which do only cover distribution but not use for ow purposes, e.g. in case of distribution of software as part of embedded products. Forbidden (explicitly/implicitly): Distribution is not allowed. For most commercial software its distribution is prohibited. A Tag is set to explicit, in case the license contains an explicit clause on distribution. It is set to implicit if the tag can only be derived indirectly fro
Detailed description ▶	Distribution is not understood as the mere resale of one single copy received (which may be permitted under mandatory copyright laws anyway). T parties in the aforementioned sense are any legal entities or natural persons other than the distributor. A mere internal provision of copies within or entity is not regarded as distribution. Distribution is also given in case of offering the software for download to the public. While this Section 3.3 does only cover distribution by the initial recipient of the Software, a further subdistribution of any downstream recipients is covered by Section 3.3a. This enables to capture licenses which grant only a non-transferable right to distribute software to one further downstream recipient, but does not allow further subdistribution by this downstream recipient. See also Section 3.3a.
Use Case ▶	Allowed only - Only licenses are accepted that permit distribution. All licenses that require or prohibit distribution are refused. This use case will be chosen in most cases where software will be distributed. However, this use case also covers the mere internal use (which would conflict with licenses that require distribution).

	Artifact Description ▼	Flags	Score	Comment	Tag	License Details
1	CC0-1.0	Compliant Conflict Unlikely	80%	License does only implicitly permit distribution.	Permitted (implicitly)	In Section 2, sentence 1, licensor first waives all right 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 ca both be understood as respective grant of distribution
2	CC-BY-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 o the licensed material, according to the definition of "share" in Section 1.i.
3	Google Chrome (OS) Adobe Additional ToS 03/2020	Medium Limited Use Case Match	75%	License does to a limited extent permit distribution.	Permitted with limitations	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
4	ibm-ipla	Conflict	0%	License does not allow (but prohibit) distribution.	Forbidden	Section 3 e) 1 prohibits distribution of the program, unless expressly permitted in the Program

FOSSmatrix – Mandanten

VORWERK

DAX-30-Konzern

Einer der weltweit größten Autozulieferer

…

FOSSmatrix – Live-Demo

Gerne stellen wir Ihnen die Möglichkeiten der FOSSmatrix in einem persönlichen Termin live vor, gerne auch virtuell.

Hendrik.Schoettle@osborneclarke.com

Mehr Informationen zu OSS Compliance und Osborne Clarke:

osborneclarke.com/oss

Osborne Clarke Deutschland –Team Open Source

Dr. Hendrik Schöttle
Partner I Fachanwalt für IT-Recht
Germany
+49 89 5434 8046
hendrik.schoettle@osborneclarke.com

Dr. Lina Böcker
Partnerin I Rechtsanwältin
Germany
+49 30 72621 8095
lina.boecker@osborneclarke.com

Cédric Ludwig
Senior Associate I Rechtsanwalt
Germany
+49 89 5434 8142
cedric.ludwig@osborneclarke.com

Philine Töpper
Associate I Rechtsanwältin
Germany
+49 30 7262 18110
philine.toepper@osborneclarke.com

Kontakt FOSSmatrix

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

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

„Im Bereich Open Source ein Spitzenname“

Wettbewerber, JUVE-Handbuch 2021/2022

Dr. Hendrik Schöttle berät im IT- und Datenschutzrecht.

Hendrik Schöttle wurde in den letzten Jahren wiederholt sowohl vom Handelsblatt und von Best Lawyers als auch von der Wirtschaftswoche und vom Kanzleimonitor als einer der besten Anwälte bzw. als mehrfach empfohlener Anwalt im IT-Recht genannt. Laut JUVE-Handbuch 2021/2022 ist er „im Bereich Open Source ein Spitzenname“. Das Kanzleihandbuch Legal 500 Deutschland empfiehlt ihn, weil er durch „sehr gute IT-Kenntnisse besticht, auch wenn es sich um exotische Fragen handelt“ und durch ein „sehr schnelles Verständnis technischer Details“.

Er hat langjährige Erfahrung bei der Beratung, Vertragsgestaltung und Verhandlung von komplexen IT-Projekten. Seine Schwerpunkte sind IoT, Digitalisierung und Cloud Computing. Er berät zu Software-Lizenzmodellen, insbesondere zu Open-Source-Software, und im Datenschutzrecht. Zu seinen Mandanten gehören international tätige Technologiekonzerne sowie namhafte IT- und E-Business-Unternehmen.

Hendrik Schöttle arbeitet seit 2005 als Rechtsanwalt, seit 2007 im Münchner Büro von Osborne Clarke. Er war mehrfach im Rahmen von Secondments in Rechtsabteilungen von IT-Unternehmen tätig. Zudem hat er mehrere Jahre als Software-Entwickler am Institut für Rechtsinformatik der Universität des Saarlandes gearbeitet. Seine praktische Erfahrung und sein technisches Know-how kommen seinen Mandanten bei der technologienahen Beratung zugute.

Er ist Autor zahlreicher Veröffentlichungen, Mitautor mehrerer Handbücher und Kommentare, unter anderem des Beck’schen Handbuchs IT- und Datenschutzrecht und des juris Praxiskommentars zum BGB.

Hendrik Schöttle ist Dozent der Deutschen Anwaltakademie für den Fachanwaltslehrgang IT-Recht und hält regelmäßig Vorträge zu Themen des IT-Rechts.

Er ist Mitglied im Vorstand des Arbeitskreises Open Source des BITKOM, Mitglied des Ausschusses Datenschutzrecht der Bundesrechtsanwaltskammer (BRAK), der Arbeitsgemeinschaft Informationstechnologie im Deutschen Anwaltverein (DAV) und der Deutschen Gesellschaft für Recht und Informatik (DGRI).