**OPEN SOURCE COMPLIANCE**

Empfohlene Vorgehensweisen für Compliance Professionals

horizontal line

* Compliance wird auf Einzel-Produkt-Basis überprüft: Wenn eine Open-Source-Komponente zur Benutzung in einem Produkt freigegeben ist, bedeutet das nicht zwangsweise, dass damit eine Vorab-Freigabe für die Nutzung in anderen Produkten vorliegt.
* Jeder Sourcecode muss frühestmöglich und oft gescannt werden. Damit können Compliance-Probleme mit deren Auftreten identifiziert, Lösungen dafür mit akzeptablem Zeitverzug bereitgestellt und ein inkrementeller Compliance-Aufbau ermöglicht werden
* Alle Dateien oder Snippets, die vom Scan-Tool gekennzeichnet werden, müssen geprüft und (problem-)behandelt werden.
* Im Zweifelsfall müssen die Scanergebnisse mit der Entwicklung diskutiert werden.
* Alle im Produkt enthaltenen Komponenten und Snippets, deren Herkunft und Lizenzen sind zu identifizieren.
* Neuere Versionen von früher freigegebenen Paketen sollten erneut gescannt werden.
* Wenn das Scan-Tool GPL-lizensierten Quellcode erkennt, der (zum Beispiel) in eine proprietäre Komponente integriert ist, melden Sie es an die Entwicklung und fordern Sie eine Korrektur ein. Scannen Sie den Code erneut, nachdem die Entwicklung das Problem gelöst hat, um eine gesicherte Bestätigung zu erhalten, dass der GPL-Code ersetzt wurde.
* In Vorbereitung einer rechtlichen Prüfung sind der Rechtabteilung alle Lizenzinformationen bereitzustellen, die in der Komponente festgestellt wurden. Für Open-Source-Komponenten umfasst dies auch die COPYING-, README-, oder LICENSE-Dateien.
* Falls Konflikte existieren oder eine Compliance-Erfüllung nicht möglich ist:
  1. Entfernen / Austauschen: Kann das Produkt ohne den fraglichen Code leben? Gibt es ein alternatives Projekt mit gleicher Funktion unter einer anderen Lizenz?
  2. Neuentwicklung: Kann eine Umgehungslösung geschaffen werden?
  3. Versions-Tracking: Gibt es eine neue (oder ältere) Version des fraglichen Codes unter einer anderen Lizenz?
  4. Neulizenzierung: Können die Autoren mit der Bitte um eine andere Lizenzierung kontaktiert werden?
* Das schriftliche Angebot und die Open-Source-Hinweise müssen präzise abgefasst werden und müssen jegliche im Produkt enthaltene Open Source einbeziehen.