Deutsche Stiftung für Recht und Informatik

Open-Source-Software-Compliance in dem öffentlichen Sektor

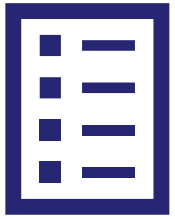
Vissarion Petrikis
Capgemini Invent Deutschland

Herbstakademie 2023

Rechtliche und regulatorische Grundlagen

Urheberrecht

Open-Source-Lizenzen



Architekturrichtlinie der IT des Bundes

Open-Source-Software ist urheberrechtlich geschützt

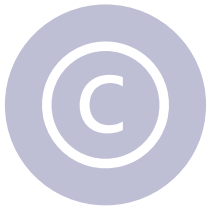
Urheberrecht

Open-Source-Lizenzen

Architekturrichtlinie der IT des Bundes

- § 69a ff. UrhG: Urheberrechtlicher Schutz von Open-Source-Software
- § 69c UrhG: Zustimmungsbedürftige Handlungen
- § 60c Nr. 1: Vervielfältigung / bloße Benutzung der Software
- § 31 Abs. 2 UrhG: Einräumung von Nutzungsrechten

Die Open-Source-Lizenzen gewähren umfangreiche Nutzungsrechte



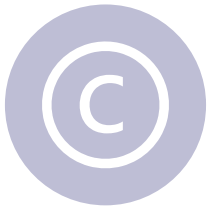
Urheberrecht

Open-Source-Lizenzen

Architekturrichtlinie der IT des Bundes

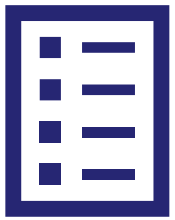
- Gewährung umfangreicher Nutzungsrechte
- Lizenzbedingungen
- Copyleft-Lizenzen
- Non-Copyleft-Lizenzen

Die Architekturrichtlinie der IT des Bundes priorisiert den Einsatz von Open-Source-Software



Urheberrecht

Open-Source-Lizenzen



Architekturrichtlinie der IT des Bundes

- Konzeption, Architekturentscheidungen und Umsetzung von IT-Projekten in der Verwaltung
- Priorisierung des Einsatzes von Open-Source-Software

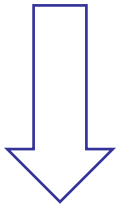
Risiken aus dem unkontrollierten Einsatz von Open-Source-Software

Rechtliche Risiken

IT-Sicherheitsrisiken

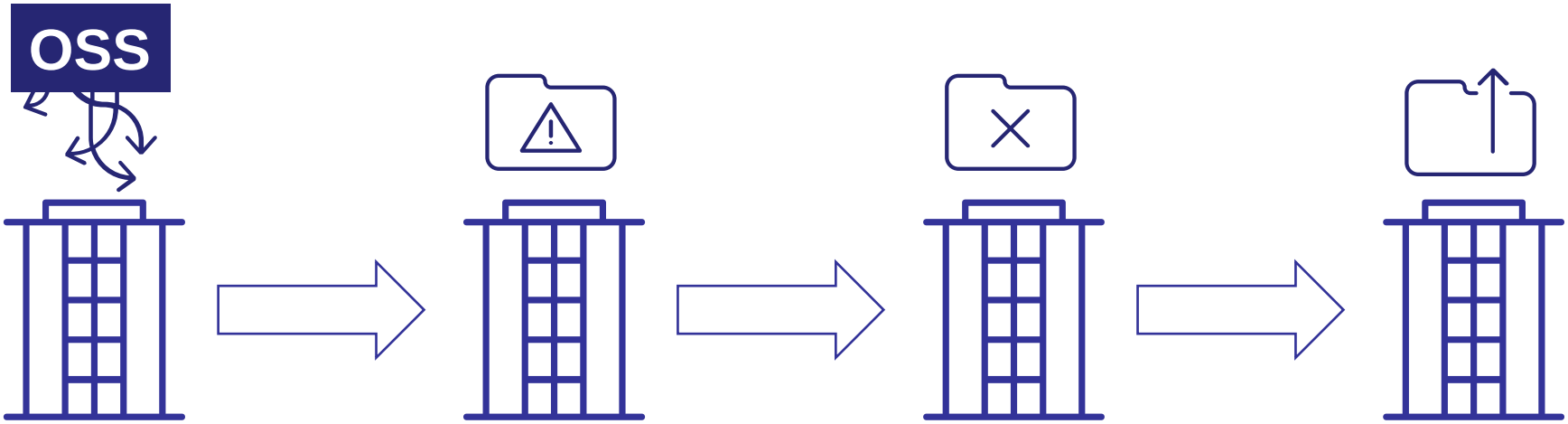
Rechtliche Risiken

- Durchsetzbarkeit von Open-Source-Lizenzen in Deutschland => Welte/Sitecom, 2004
- Bestehen urheberrechtliche Ansprüche, wenn die Lizenzbedingungen nicht eingehalten werden?
- Führt die Lizenzverletzung zum Erlöschen der gewährten Nutzungsrechte?
  - Copyleft-Lizenzen: § 158 Abs. 2 BGB
  - Non-Copyleft-Lizenzen: § 314 Abs. 2 BGB



- Urheberrechtliche Ansprüche: Beseitigungsansprüche, Unterlassungsansprüche, Schadenersatzansprüche und Auskunftsansprüche

Fehlende oder mangelhafte Compliance-Verfahren können zu Datenschutzverletzungen führen...



Equifax integrierte OSS in ihre Codebasis ohne ein klares Compliance-Verfahren, sodass unter anderem nicht nachvollziehbar war, welche Software in welcher Umgebung verwendet wurde

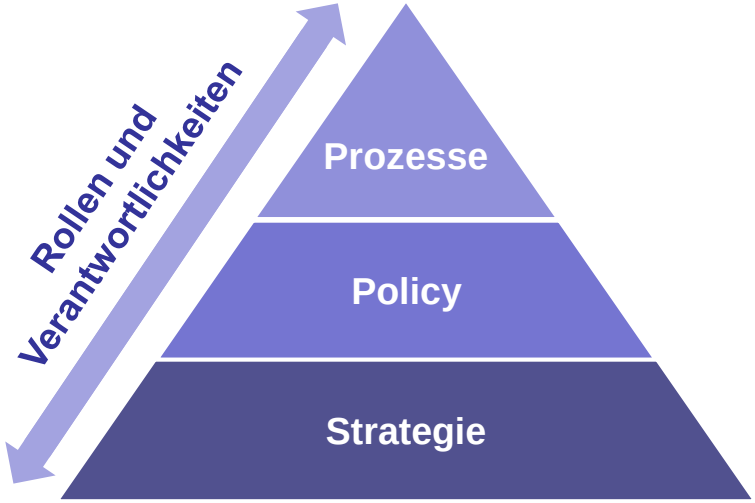
Unter anderem wurde Apache Struts integriert, eine Komponente mit einem erheblichen Sicherheitsproblem, das zu einem Sicherheitsverstoß führen könnte

Obwohl eine Fehlerbehebung zur Verfügung stand, hat Equifax diese aufgrund eines Fehlers in den internen Prozessen nicht angewendet

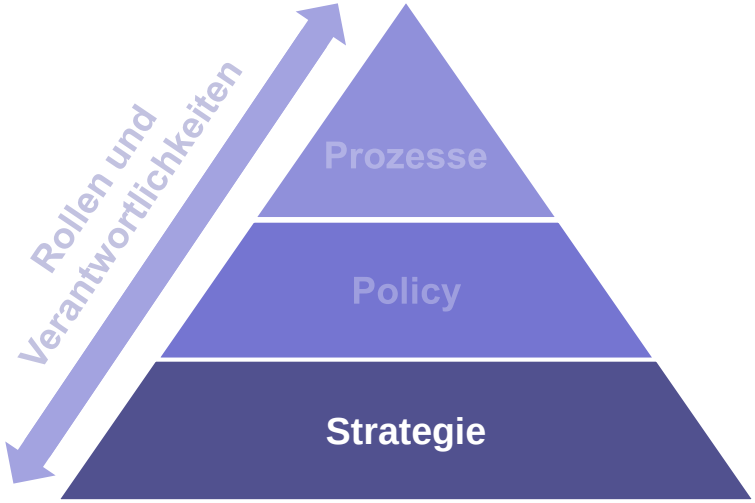
Die Sicherheitslücke wurde ausgenutzt und führte zum Verlust der persönlichen Daten von mehr als 147 Millionen Menschen

...und zu enormen finanziellen und rufschädigenden Schäden

Grundlage der Open-Source-Software-Compliance

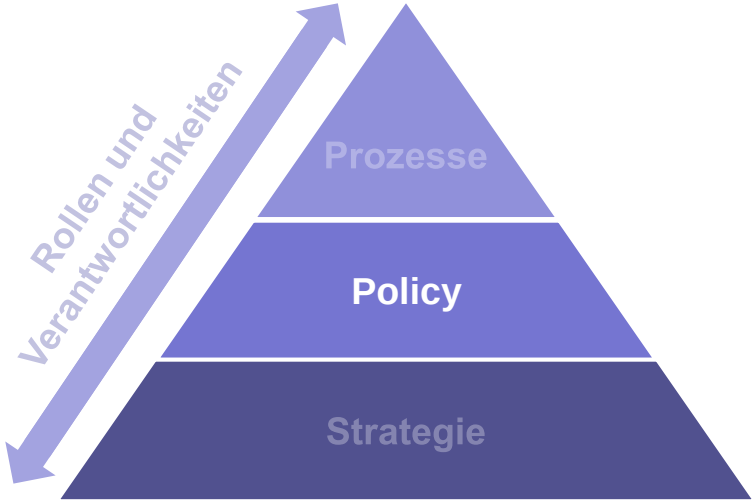


Die Open-Source-Strategie schafft das Fundament der Open-Source-Software-Compliance



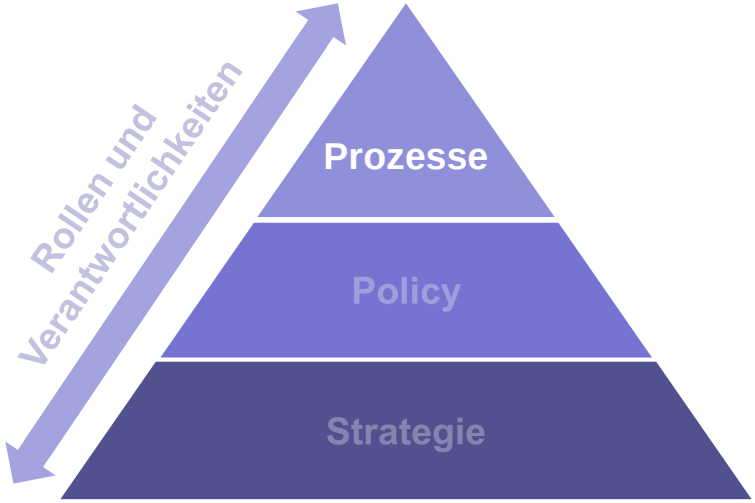
- Das Fundament der Open-Source-Software-Compliance
- Wie soll Open-Source-Software verwendet werden?
- Welche Geschäftsziele werden mit der Nutzung von OSS verfolgt?
- Welche Maßnahmen werden ergriffen, um die Ziele zu erreichen?
- Wie gestaltet sich das Engagement mit der Community?

Die Open-Source-Policy bestimmt die Strategie und schafft die Compliance-Basis



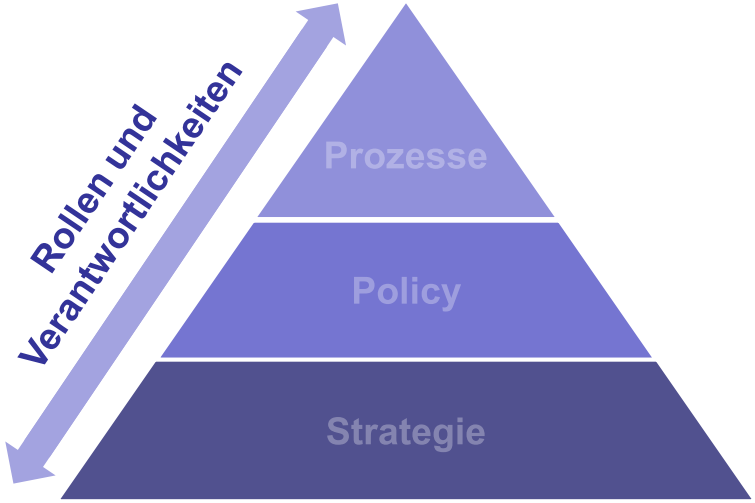
- Eine Policy bestimmt die Schritte, die zur Erreichung der Ziele führen.
- Geltungsbereich der Policy
- Lizenzüberprüfung
- Identifikation
- Wartungs- und Support-Ansatz

Die Prozessen detaillieren den Compliance-Alltag



- Detaillierte Prozesse für jeden Abschnitt der Policy
- Feste Schritte und Verantwortlichkeiten

Die Open-Source-Software-Compliance wird von zwei Teams durchgeführt



- Kernteam: Open-Source-Review-Board
- Erweitertes Team: agiert in dem peripheren Bereich des Kernteams

Die zentrale Durchführung der Open-Source-Software Compliance bringt erhebliche Vorteile

- Erstellung von zentralen Richtlinien
- Erfassung und Verwaltung aller regelmäßig genutzten Open-Source-Software-Projekte
  - IT-Sicherheitsrisiken zentral identifizieren und beheben
  - Schneller Identifikation der Open-Source-Software-Projekte
  - Unterstützung bei der Entscheidung, welche Open-Source-Software-Projekte unterstützt werden sollen
- Unterstützung der Open-Source-Software-Projekte im Bereich Governance
  - Gewährleistung der Interesse der Verwaltung
  - Schnellere Meldung von Bugs oder neuen gewünschten Funktionalitäten
- Zentrale Verfolgung von IT-Sicherheitsmeldungen