

Open Source Monitor 2025



bitkom

Open Source Monitor 2025

DOI

10.64022/2025-open-source-monitor

Mit freundlicher Unterstützung von



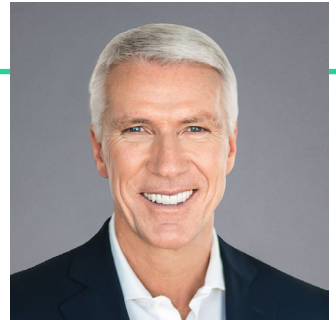
Vorwort

Open Source hat im Jahr 2025 weiter an Aufmerksamkeit gewonnen. Ohne Open-Source-Lösungen würde der Datenverkehr im Internet stillstehen, ein Großteil der digitalen Dienste und Plattformen im Internet würde nicht funktionieren und auch unsere Smartphones kommen nicht ohne Open-Source-Komponenten aus. Die Open-Source-Community ist zudem ein Innovationstreiber, etwa bei Cloud-Technologien oder Künstlicher Intelligenz.

Woran es manchmal noch fehlt, ist ein vertieftes Verständnis für Open Source – hier wollen wir mit der vierten Auflage unseres »Open Source Monitor« ansetzen. Für ihn haben wir mehr als 1.100 Unternehmen repräsentativ befragt und zusätzlich ein Stimmungsbild unter rund 100 Organisationen des Public Sector erhoben. Dabei zeigt sich: Open Source ist aus der deutschen Wirtschaft und Verwaltung nicht mehr wegzudenken. Rund drei Viertel der Unternehmen nutzen auf die eine oder andere Art bewusst Open Source, im Public Sector sind es zwei Drittel der Behörden und Organisationen.

Diese breite Nutzung liegt an den ganz konkreten und direkten Vorteilen von Open Source, etwa geringeren Kosten, individuell angepassten Lösungen oder auch der Möglichkeit, die Sicherheit selbst zu überprüfen. Darüber hinaus profitieren Unternehmen und Verwaltungen von einer lebendigen Entwickler-Community, die kontinuierlich neue Funktionen und Verbesserungen bereitstellt. Die Bedeutung von Open Source für unsere Wirtschaft und Gesellschaft geht aber weit darüber hinaus. Durch den Zugang zum Quellcode und die Möglichkeit, selbst Änderungen vorzunehmen, kann Open Source uns helfen, dem Ziel der Digitalen Souveränität näherzukommen, indem wir die Hoheit über die eingesetzte Software behalten oder zurückgewinnen. 6 von 10 Unternehmen wünschen sich, dass der Staat aufgrund der aktuellen geopolitischen Lage stärker in Open Source Software investiert. Allerdings zeigt sich auch, dass Unternehmen weiterhin vor Herausforderungen beim Einsatz von Open Source stehen – von fehlenden IT-Fachkräften über unklare Gewährleistungsfragen bis hin zu rechtlichen Unsicherheiten bei der Lizenzierung.

Open Source muss strategisch angegangen werden. Das bedeutet, Ziele zu definieren, Zuständigkeiten festzulegen und Open Source fest in der digitalen Gesamtstrategie zu verankern. Und hier können wir noch nachlegen, denn eine Mehrheit von 6 von 10 Unternehmen hat keinerlei Open-Source-Strategie entwickelt. Es bleibt also bei allen Fortschritten weiter viel zu tun – für die Open-Source-Community, Unternehmen und die öffentliche Verwaltung. Mit diesem »Open Source Monitor 2025« wollen wir einen Beitrag dazu leisten.



Dr. Ralf Wintergerst
Präsident
Bitkom

Wichtigste Erkenntnisse

Nutzung & Haltung in Unternehmen

- Die Mehrheit der Unternehmen steht Open Source Software (OSS) positiv gegenüber: 24 Prozent sind »sehr aufgeschlossen«, 37 Prozent »eher aufgeschlossen«. 42 Prozent erwarten, dass die Bedeutung künftig zunimmt.
- 73 Prozent setzen OSS ein – vor allem intern ohne Quellcode-Anpassung (67 Prozent), 35 Prozent nehmen Anpassungen vor. 25 Prozent integrieren OSS in Produkte, 7 Prozent entwickeln eigenständige OSS-Lösungen.
- Dennoch verfügen 60 Prozent über keine OSS-Strategie; 37 Prozent haben eine dokumentierte Strategie zur Nutzung (30 Prozent) oder Beteiligung (21 Prozent).

Policy & Compliance

- In 78 Prozent der Fälle ist der CIO für OSS zuständig. Nur 14 Prozent haben ein Open Source Program Office (OSPO), 12 Prozent planen es.
- Eine OSS-Policy fehlt bei 62 Prozent der Unternehmen; 36 Prozent haben eine dokumentierte Regelung. 52 Prozent verfügen über keinen Compliance-Prozess für Mitarbeitende.
- Treiber für Compliance-Anpassungen sind v. a. CER (61 Prozent), CRA (57 Prozent) und PLD (44 Prozent).

Zukunftsaussichten & KI

- 51 Prozent halten Open-Source-KI-Modelle für empfehlenswert, 45 Prozent sehen darin eine Möglichkeit, Abhängigkeiten zu vermeiden.
- 73 Prozent sehen OSS als Instrument zur Stärkung digitaler Souveränität; 60 Prozent wünschen verstärkte staatliche Investitionen, 57 Prozent unterstützen die Sovereign Tech Agency. Allerdings haben nur 17 Prozent digitale Abhängigkeiten vollständig analysiert und reduziert.

Öffentlicher Sektor

- Auch die Verwaltung steht OSS überwiegend positiv gegenüber (52 Prozent aufgeschlossen). 63 Prozent nutzen OSS, durchschnittlich mit 4 Vollzeitäquivalenten für das Management (Wirtschaft: 1,9).
- 37 Prozent haben eine OSS-Strategie, 60 Prozent eine Policy. 57 Prozent verfügen über einen Compliance-Prozess für Mitarbeitende.
- Als Vorteile nennen Verwaltungen v. a. Kosteneinsparungen (19 Prozent) und Quellcodezugriff (12 Prozent), als Nachteil vor allem Fachkräftemangel (33 Prozent).
- OSPOs sind mit 25 Prozent häufiger etabliert als in der Wirtschaft.

Inhalt

Vorwort	3
Wichtigste Erkenntnisse	4
1 OSS im Einsatz von Unternehmen	10
1.1 Grundhaltung zu Open Source Software	10
1.2 Strategie für Open Source Software	11
1.3 Einsatz von Open Source Software	12
1.4 Auswahlkriterien bei Open Source Software	13
1.5 Beteiligung an der (Weiter-)Entwicklung von OSS	15
1.6 Vorteile von Open Source Software	16
1.7 Nachteile von Open Source Software	17
1.8 Gründe gegen den Einsatz von OSS	18
1.9 Personelle Ressourcen für Open Source Software	19
2 Policy & Compliance	21
2.1 Zuständigkeit für Open Source Software	21
2.2 OSS-Policy	22
2.3 Europäische Compliance-Vorgaben	23
2.4 Compliance-Maßnahmen und -Instrumente	24
2.5 OSS-Standards in der Supply Chain	25
2.6 Budget für Compliance-Maßnahmen	26
3 Zukunftsaussichten, Politik & KI	28
3.1 KI in der Softwareentwicklung	28
3.2 Open-Source-KI-Modelle	29
3.3 Nutzung von und Bedenken gegenüber KI-Code-Generatoren	30
3.4 Open-Source-KI-Modelle	31

4	Open Source im Public Sector	33
4.1	Grundhaltung zu Open Source Software	33
4.2	Einsatz von Open Source Software	34
4.3	Auswahlkriterien bei Open Source Software	35
4.4	Strategie für Open Source Software	37
4.5	Beteiligung an der (Weiter-)Entwicklung von OSS	38
4.6	Vorteile von OSS	39
4.7	Nachteil von Open Source Software	40
4.8	Open Source Program Offices (OSPOs)	41
4.9	OSS-Policy	42
4.10	Compliance-Prozess für Mitarbeitende	43
4.11	OSS als Instrument für Digitale Souveränität	44
4.12	KI in der Softwareentwicklung	45
4.13	Open-Source-KI-Modelle	46
5	Case Studies	48
5.1	OCCTET: Open Source Compliance für den CRA – kostenlos und praxisnah	48
5.2	Open Source Compliance in der Supply Chain	49
5.3	Brücken und Betriebssysteme – über das Unsichtbare, das uns alle trägt	50
5.4	Open Source ist allgegenwärtig – und ab 2027 auch reguliert	51
5.5	Open Source ermöglicht weitere Wertschöpfung und Digitale Souveränität	52
5.6	Mit Open Source zur transparenten KI-Nutzung	53
5.7	NeoNephos Foundation: Open Source für Europas Digitale Souveränität	54
5.8	Experten-Statement	55
5.9	Software automatisiert prüfen mit dem Badgesystem	56
6	Methodik & Anhang	57

Abbildungen

1	Abbildung 1: Grundhaltung der Unternehmen zu Open Source Software	10
2	Abbildung 2: Erwartete Bedeutung von OSS in den Unternehmen	10
3	Abbildung 3: Strategien zur Nutzung und Beteiligung an OSS	11
4	Abbildung 4: Einsatzformen von OSS in Unternehmen	12
5	Abbildung 5: Auswahlkriterien für OSS: Sicherheit, Funktionalität und regulatorische Vorgaben	13
6	Abbildung 6: Auswahlkriterien für OSS: Lizenzen, Support und Community-Aspekte	14
7	Abbildung 7: Beteiligung von Unternehmen an der Entwicklung und Weiterentwicklung von OSS	15
8	Abbildung 8: Wahrgenommene Vorteile von OSS für Unternehmen	16
9	Abbildung 9: Wahrgenommene Nachteile von OSS für Unternehmen	17
10	Abbildung 10: Gründe gegen den Einsatz von OSS: Recht & Sicherheit	18
11	Abbildung 11: Gründe gegen den Einsatz von OSS: Ressourcen & Fachkräfte	18
12	Abbildung 12: Gründe gegen den Einsatz von OSS: Wirtschaftlichkeit & Akzeptanz	18
13	Abbildung 13: Personelle Zuständigkeiten und Ressourcen für OSS-Management in Unternehmen	19
14	Abbildung 14: Anzahl der Beschäftigten, die sich im Unternehmen schwerpunktmäßig mit OSS-Management beschäftigen	19
15	Abbildung 15: Zuständigkeiten für OSS im Unternehmen	21
16	Abbildung 16: Anteil der Unternehmen mit Open Source Program Offices	21
17	Abbildung 17: Compliance-Prozesse für Mitarbeitende im Umgang mit OSS	22
18	Abbildung 18: OSS-Policy in Unternehmen	22
19	Abbildung 19: Beginn der Beschäftigung mit Compliance-Fragen	23
20	Abbildung 20: Einfluss europäischer Vorgaben (CER, CRA, PLD, DORA, NIS2) auf Compliance-Prozesse	23
21	Abbildung 21: Eingesetzte Compliance-Maßnahmen und -Instrumente im OSS-Management	24
22	Abbildung 22: Einsatz von SBOMs in Unternehmen	25
23	Abbildung 23: Verbreitung von Standards in der Supply Chain (ISO 5230, ISO 18974, BSI 03183)	25
24	Abbildung 24: Entwicklung der Budgets für OSS-Compliance	26
25	Abbildung 25: Einsatz von KI in der Softwareentwicklung in Unternehmen	28
26	Abbildung 26: Einschätzungen zu Open-Source-KI-Modellen	29
27	Abbildung 27: Wahrgenommene Risiken durch KI-generierten Code	30
28	Abbildung 28: Nutzung von KI-Code-Generatoren in Unternehmen	30
29	Abbildung 29: Zustimmung zu Aussagen über OSS als Instrument für Digitale Souveränität	31
30	Abbildung 30: Grundhaltung gegenüber OSS: Wirtschaft vs. öffentlicher Sektor	33
31	Abbildung 31: OSS- und Personaleinsatz im Vergleich: Wirtschaft vs. öffentliche Verwaltung	34
32	Abbildung 32: Auswahlkriterien für OSS im Public Sector: Sicherheit, Funktionalität, Rechte	35

33	Abbildung 33: Auswahlkriterien für OSS im Public Sector: Community und Support-Struktur	36
34	Abbildung 34: Strategien für OSS: Wirtschaft vs. öffentliche Verwaltung	37
35	Abbildung 35: Beteiligung an der Entwicklung und Weiterentwicklung von OSS: Wirtschaft vs. Verwaltung	38
36	Abbildung 36: Wahrgenommene Vorteile von OSS in der öffentlichen Verwaltung	39
37	Abbildung 37: Wahrgenommene Nachteile von OSS in der öffentlichen Verwaltung	40
38	Abbildung 38: Anteil der Organisationen mit OSPOs im Public Sector	41
39	Abbildung 39: Vorhandensein einer OSS-Policy im Public Sector vs. Wirtschaft	42
40	Abbildung 40: Compliance-Prozesse für Mitarbeitende im Public Sector vs. Wirtschaft	43
41	Abbildung 41: Zustimmung zu Aussagen über OSS als Instrument für Digitale Souveränität in der öffentlichen Verwaltung	44
42	Abbildung 42: Einsatz von KI in der Softwareentwicklung im Public Sector vs. Wirtschaft	45
43	Abbildung 43: Einschätzungen zu Open-Source-KI-Modellen in der öffentlichen Verwaltung	46

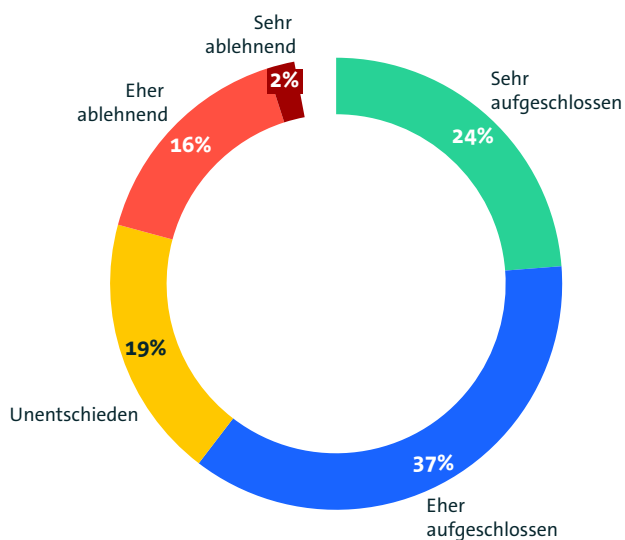
1 OSS im Einsatz von Unternehmen

1 OSS im Einsatz von Unternehmen

Unter Open Source Software verstehen wir Software, wie z. B. Programm-Module, Quellcode und Bibliotheken, Programmierwerkzeuge sowie komplette Betriebssysteme oder Software-Lösungen, deren Quellcodes offengelegt sind und deren Lizenz es den Lizenznehmenden erlaubt, die Software frei auszuführen, sie zu analysieren, anzupassen und sowohl in unveränderter als auch veränderter Form weiterzugeben. Voraussetzung hierfür ist neben dem offen zugänglichen Quell- bzw. Sourcecode auch Lizenzgebührenfreiheit.

1.1 Grundhaltung zu Open Source Software

Wie steht Ihr Unternehmen generell zum Thema Open Source Software?

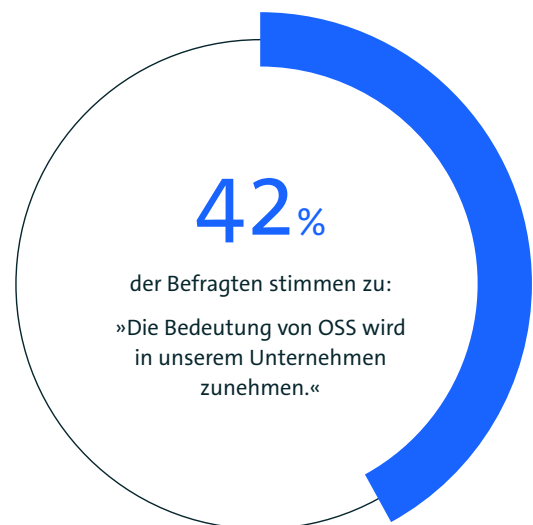


Basis: Alle Befragten (n=1.152) | Rest: »Weiß nicht/keine Angabe« | Quelle: Bitkom Research 2025

Abbildung 1: Grundhaltung der Unternehmen zu Open Source Software

Die Mehrheit der Unternehmen steht dem Thema Open Source Software (OSS) grundsätzlich positiv gegenüber. 24 Prozent bezeichnen ihre Haltung als »sehr aufgeschlossen« und weitere 37 Prozent als »eher aufgeschlossen«. Damit sind insgesamt mehr als sechs von zehn Unternehmen offen für OSS. 19 Prozent zeigen sich unentschieden, während eine kleinere Gruppe ablehnend eingestellt ist: 16 Prozent sind »eher ablehnend« und lediglich 2 Prozent »sehr ablehnend«.

42 Prozent der befragten Unternehmen erwarten, dass die Bedeutung von Open Source Software (OSS) in ihrem Unternehmen künftig zunehmen wird. Damit sieht knapp jedes zweite Unternehmen OSS als einen wachsenden Faktor für die eigene Arbeit und Strategie an.



Basis: Alle Befragten (n=1.152) | Quelle: Bitkom Research 2025

Abbildung 2: Erwartete Bedeutung von OSS in den Unternehmen

1.2 Strategie für Open Source Software

Die Mehrheit der befragten Unternehmen verfügt derzeit über keine Strategie zur Verwendung oder Beteiligung an Open Source Software (OSS). So geben 60 Prozent an, dass es keinerlei OSS-Strategie in ihrem Unternehmen gibt. Immerhin 37 Prozent haben jedoch entsprechende Pläne ausgearbeitet.

Dabei existieren Strategien zur Nutzung von OSS etwas häufiger als Strategien zur aktiven Beteiligung: 30 Prozent verfolgen eine Strategie zur Verwendung, während 21 Prozent eine Beteiligungsstrategie vorweisen.

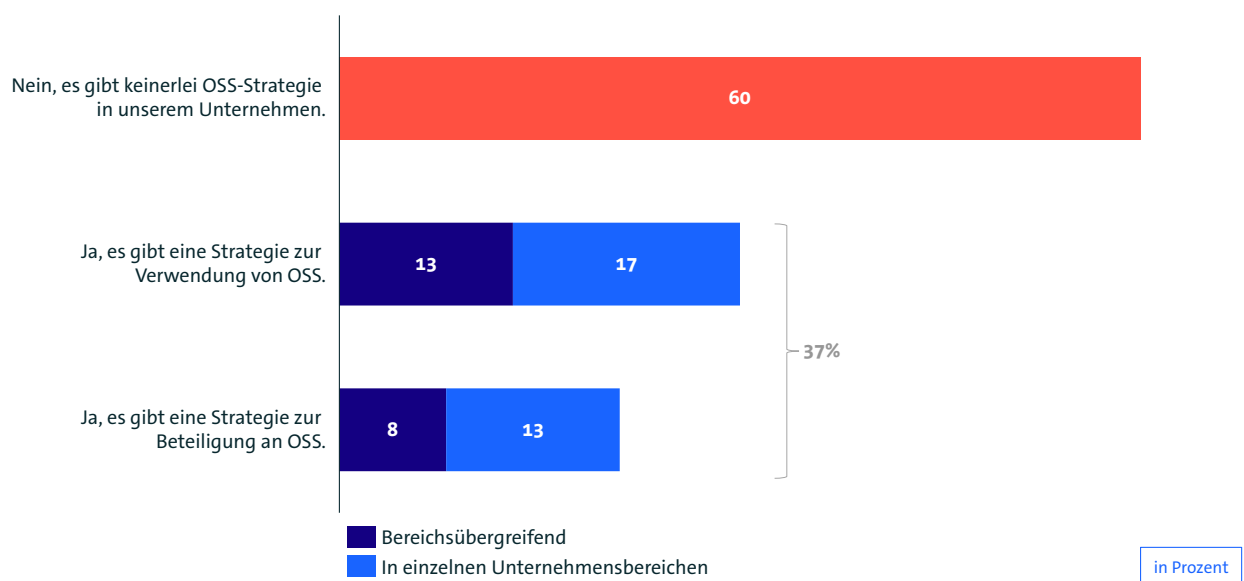
Unterschiede zeigen sich zudem zwischen einer bereichsübergreifenden und einer auf einzelne Unternehmensbereiche beschränkten Strategie.

Bei der Verwendung von OSS setzen 17 Prozent auf Konzepte in einzelnen Bereichen und 13 Prozent auf unternehmensweite Ansätze. Bei der Beteiligung sind es 13 Prozent in einzelnen Bereichen und 8 Prozent bereichsübergreifend. Insgesamt zeigt sich somit, dass zwar ein Drittel der Unternehmen OSS-Strategien verfolgt, aber ein Großteil noch ohne strukturierten Ansatz bleibt.

Die Anzahl der Unternehmen mit OSS-Strategie steigt von Jahr zu Jahr:

2021 hatten 25 Prozent eine Strategie zur Verwendung bzw. Beteiligung an OSS, 2023 lag der Wert schon bei 32 Prozent, und in 2025 stieg der Anteil auf 37 Prozent an.

Gibt es in Ihrem Unternehmen eine Strategie* zur Verwendung bzw. zur Beteiligung an OSS?



*Mit Strategie meinen wir in einem Dokument niedergeschriebene Ziele und Pläne zur Verwendung bzw. Beteiligung an OSS in Ihrem Unternehmen. Basis: Alle Befragten (n=1.152) | Mehrfachnennungen möglich | Nicht dargestellt: »Weiß nicht/keine Angabe« | Quelle: Bitkom Research 2025

Abbildung 3: Strategien zur Nutzung und Beteiligung an OSS

1.3 Einsatz von Open Source Software

Der Einsatz von Open Source Software (OSS) erfolgt in den meisten Unternehmen primär intern. So setzen 67 Prozent OSS innerhalb des eigenen Unternehmens ein, ohne Anpassungen am Quellcode vorzunehmen. Weitere 35 Prozent nutzen OSS intern, passen den Quellcode jedoch an ihre Bedürfnisse an.

Ein Viertel der Unternehmen (25 Prozent) integriert OSS in eigene Produkte oder Lösungen für die Kundschaft – teils ohne Veränderungen am Quellcode, teils mit Anpassungen. Eigenständige OSS-Produkte oder -Lösungen für externe

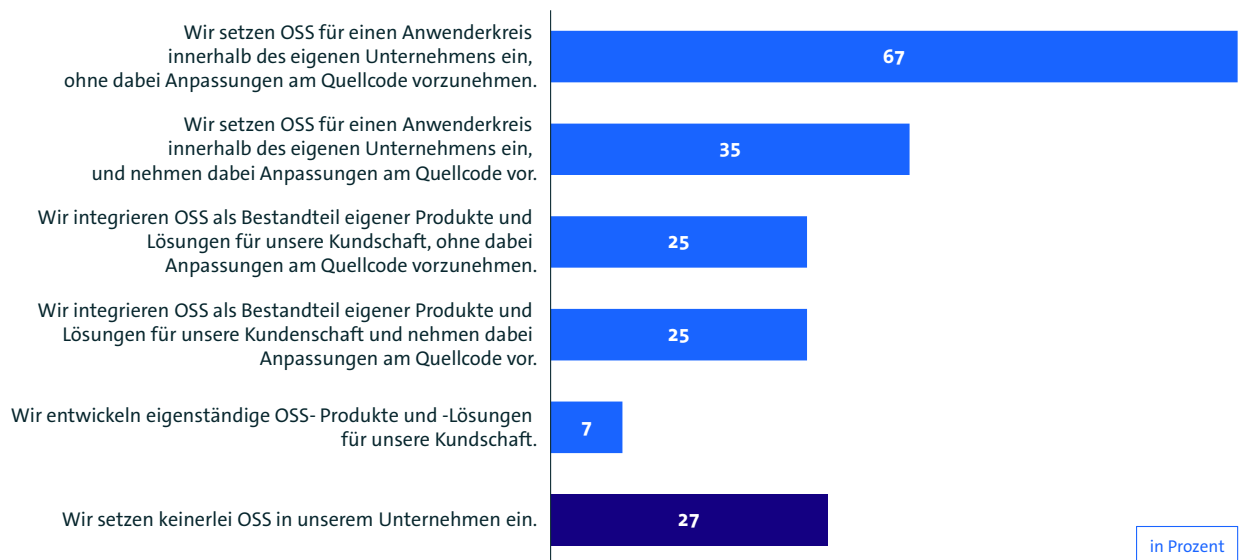
Kunden entwickelt hingegen nur eine kleine Minderheit von 7 Prozent. Auffällig ist außerdem, dass 27 Prozent angeben, keinerlei OSS in ihrem Unternehmen einzusetzen.

Insgesamt zeigt sich: OSS wird überwiegend als interne Lösung verwendet, während eine Integration in Kundenprodukte oder gar eine eigenständige Entwicklung bisher nur von einer kleineren Gruppe umgesetzt wird.

Die Anzahl der Unternehmen, die Open Source Software einsetzen, liegt stabil bei um die 70 Prozent:

2021 gaben 71 Prozent an, OSS einzusetzen. 2023 waren es 69 Prozent der Befragten, und in 2025 lag der Anteil bei 73 Prozent.

Setzt Ihr Unternehmen OSS ein?



Basis: Alle Befragten (n=1.152) | Nicht dargestellt: »Weiß nicht/keine Angabe« | Mehrfachnennungen möglich | Quelle: Bitkom Research 2025

Abbildung 4: Einsatzformen von OSS in Unternehmen

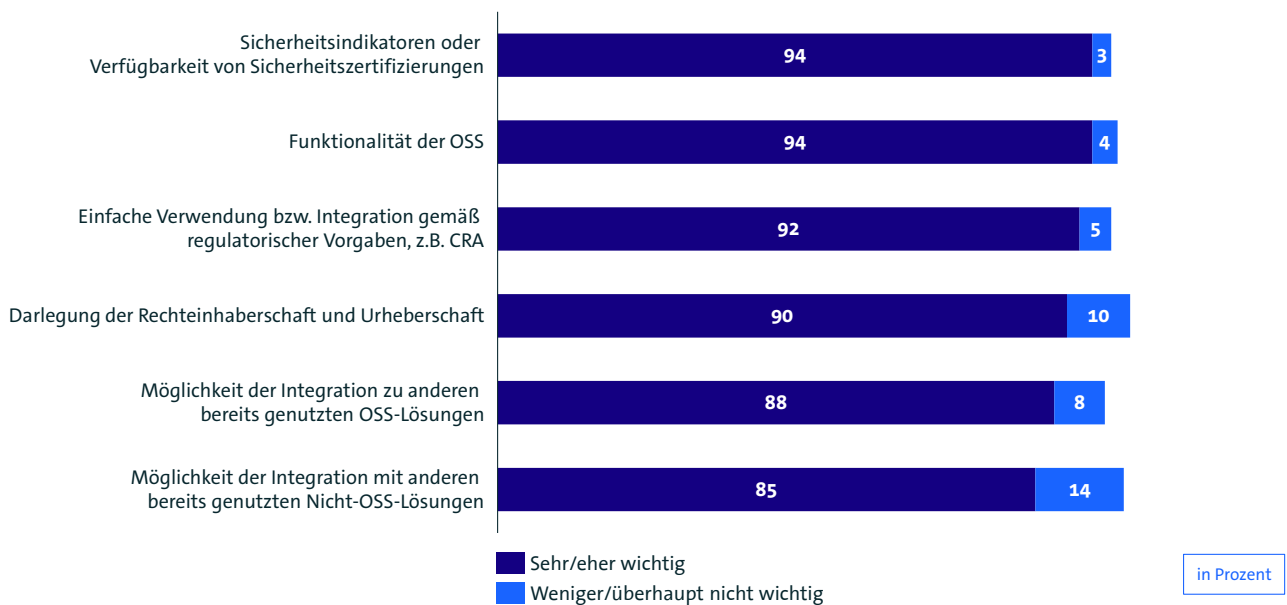
1.4 Auswahlkriterien bei Open Source Software

Bei der Auswahl von Open Source Software (OSS)-Projekten legen Unternehmen vor allem auf Sicherheits- und Funktionsaspekte großen Wert. Jeweils 94 Prozent halten Sicherheitsindikatoren oder Sicherheitszertifizierungen sowie die Funktionalität der OSS für sehr oder eher wichtig.

Auch die einfache Verwendung und Integration unter regulatorischen Vorgaben, wie etwa dem Cyber Resilience Act (CRA), spielt für 92 Prozent eine bedeutende Rolle. 90 Prozent achten zudem auf eine klare Darlegung der Rechteinhaberschaft und Urheberschaft.

Die Integrationsfähigkeit ist ebenfalls ein entscheidendes Kriterium: 88 Prozent bewerten die Möglichkeit der Integration mit anderen bereits genutzten OSS-Lösungen als wichtig, 85 Prozent achten auf die Kompatibilität mit Nicht-OSS-Lösungen. Insgesamt zeigt sich, dass nahezu alle befragten Unternehmen den genannten Kriterien eine hohe Relevanz beimessen.

Wie wichtig sind Ihnen die folgenden Kriterien bei der Auswahl von OSS-Projekten?



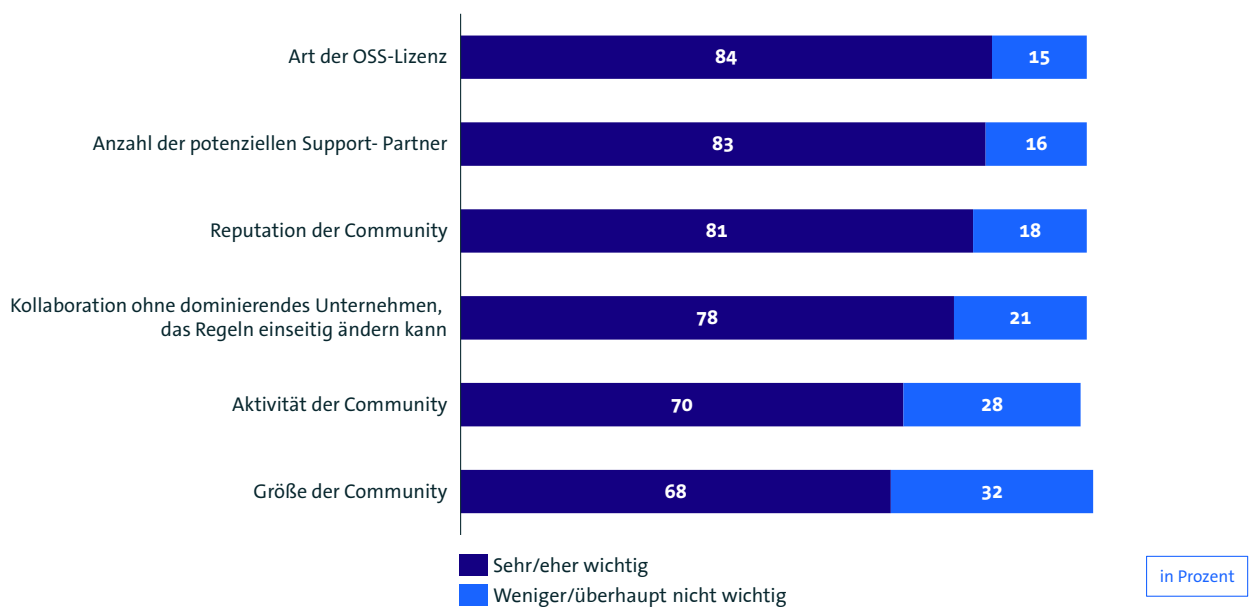
Basis: Unternehmen, die OSS verwenden, integrieren oder (weiter-)entwickeln (n=839) | Mehrfachnennungen möglich | Rest: »Weiß nicht/keine Angabe« | Quelle: Bitkom Research 2025

Abbildung 5: Auswahlkriterien für OSS: Sicherheit, Funktionalität und regulatorische Vorgaben

84 Prozent der Unternehmen halten die Art der OSS-Lizenz für sehr oder eher wichtig. Fast ebenso bedeutsam ist die Anzahl potenzieller Support-Partner (83 Prozent). Auch die Reputation der jeweiligen Community wird von 81 Prozent berücksichtigt.

78 Prozent achten darauf, dass es keine dominante Firma gibt, die Regeln einseitig verändern könnte. Etwas geringer ist die Bedeutung der Community-Aktivität (70 Prozent) sowie der Community-Größe (68 Prozent). Damit zeigt sich, dass zwar auch die Struktur und Lebendigkeit der Community relevant sind, die Mehrheit der Unternehmen jedoch rechtliche Klarheit und verlässliche Support-Möglichkeiten stärker gewichtet.

Wie wichtig sind Ihnen die folgenden Kriterien bei der Auswahl von OSS-Projekten?



Basis: Unternehmen, die OSS verwenden, integrieren oder (weiter-)entwickeln (n=839) | Mehrfachnennungen möglich | Rest: »Weiß nicht/keine Angabe« | Quelle: Bitkom Research 2025

Abbildung 6: Auswahlkriterien für OSS: Lizenzen, Support und Community-Aspekte

1.5 Beteiligung an der (Weiter-)Entwicklung von OSS

47 Prozent der Unternehmen beteiligen sich an der Entwicklung bzw. Weiterentwicklung von Open Source Software.

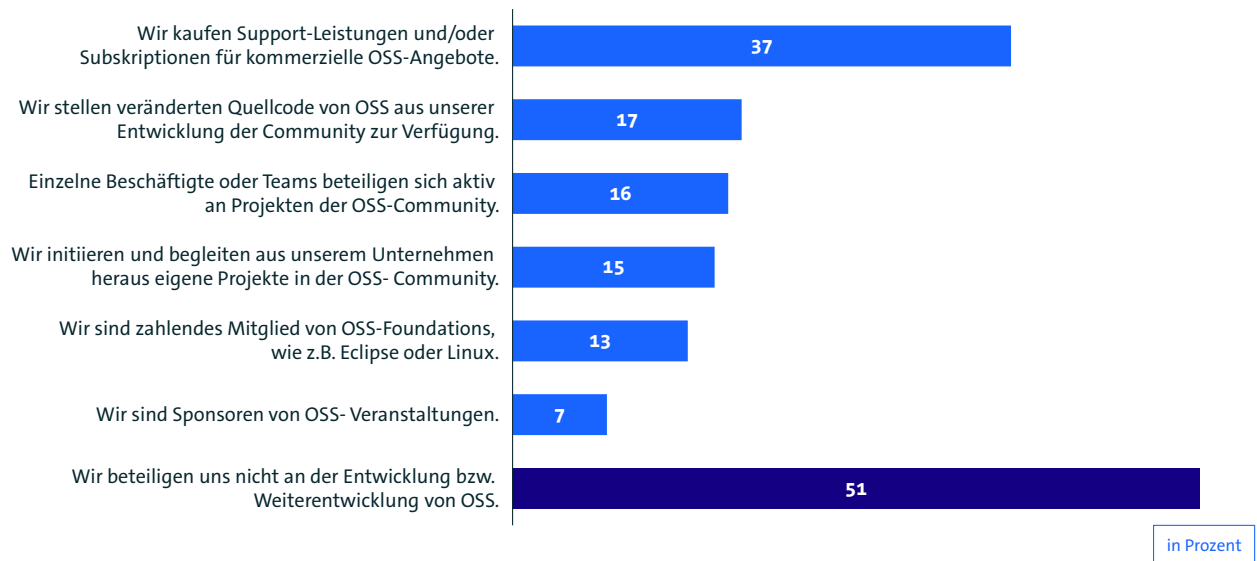
37 Prozent tun das, indem sie Support-Leistungen oder Subskriptionen für kommerzielle Open Source Software einkaufen.

Die weiteren Arten der Beteiligung sind deutlich weniger verbreitet. 17 Prozent stellen die eigenen Änderungen an OSS-Quellcode der Community zur Verfügung, 16 Prozent berichten davon, dass sich einzelne Beschäftigte oder Teams aktiv in OSS-Projekte einbringen.

15 Prozent initiieren eigene OSS-Projekte und 13 Prozent zahlen Mitgliedsbeiträge in OSS-Stiftungen wie Linux oder Eclipse.

Ein geringer Anteil von 7 Prozent sponsert selbst OSS-Veranstaltungen. Ganze 51 Prozent der Unternehmen beteiligt sich gar nicht an der Entwicklung und Weiterentwicklung von OSS.

Inwiefern beteiligt sich Ihr Unternehmen an der Entwicklung bzw. Weiterentwicklung von OSS?



Basis: Alle Befragten (n=1.152) | Nicht dargestellt: »Weiß nicht/keine Angabe« | Mehrfachnennungen möglich | Quelle: Bitkom Research 2025

Abbildung 7: Beteiligung von Unternehmen an der Entwicklung und Weiterentwicklung von OSS

1.6 Vorteile von Open Source Software

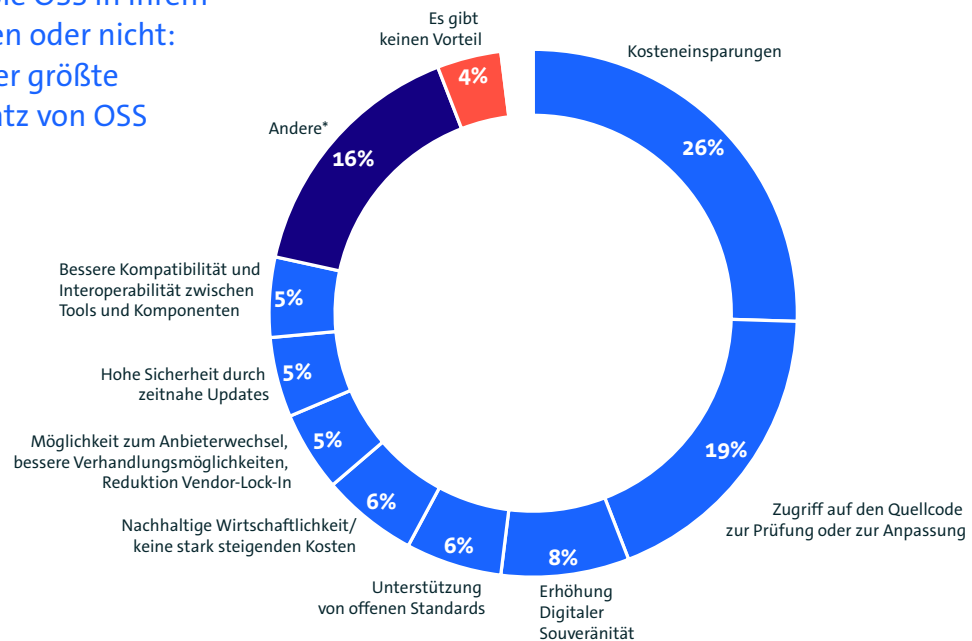
Als größter Vorteil des Einsatzes von Open Source Software (OSS) sehen die befragten Unternehmen vor allem Kosteneinsparungen: 26 Prozent nennen diesen Aspekt als entscheidend. An zweiter Stelle steht für 19 Prozent der Zugriff auf den Quellcode, sei es zur Prüfung oder zur individuellen Anpassung.

Weitere Vorteile sind die Erhöhung der digitalen Souveränität (8 Prozent) sowie die Unterstützung offener Standards (6 Prozent). Jeweils 6 Prozent heben zudem nachhaltige Wirtschaftlichkeit und das Ausbleiben stark steigender Kosten hervor. Weniger häufig werden Argumente wie die Möglich-

keit zum Anbieterwechsel und zur Reduktion von Abhängigkeiten (5 Prozent), eine hohe Sicherheit durch zeitnahe Updates (5 Prozent) sowie eine bessere Kompatibilität und Interoperabilität zwischen Tools und Komponenten (5 Prozent) genannt.

16 Prozent der Befragten führen andere Vorteile an, während nur 4 Prozent angeben, überhaupt keinen Nutzen in OSS zu sehen. Insgesamt überwiegen damit klar die positiven Einschätzungen, vor allem in Bezug auf Kosten und Flexibilität.

Unabhängig davon, ob Sie OSS in Ihrem Unternehmen verwenden oder nicht: Was ist aus Ihrer Sicht der größte Vorteil, der für den Einsatz von OSS spricht?



Basis: Alle Befragten (n=1.152) | Rest: »Weiß nicht/keine Angabe« | Quelle: Bitkom Research 2025

*Große Auswahl an OSS-Komponenten (4%); Breite und aktive Community für Wissensaustausch (4%); Attraktiver IT-Arbeitsplatz, Motivation für Beschäftigte (2%); Möglichkeit zur Anpassung an eigene Bedürfnisse/Adaption (2%); Vielzahl an OSS-Anbietern, die kommerziellen Support anbieten (1%); Bessere Wettbewerbschancen für unser Unternehmen (1%); Hohe Stabilität, geringe Fehleranfälligkeit (1%); Kurze Innovationszyklen (1%)

Abbildung 8: Wahrgenommene Vorteile von OSS für Unternehmen

1.7 Nachteile von Open Source Software

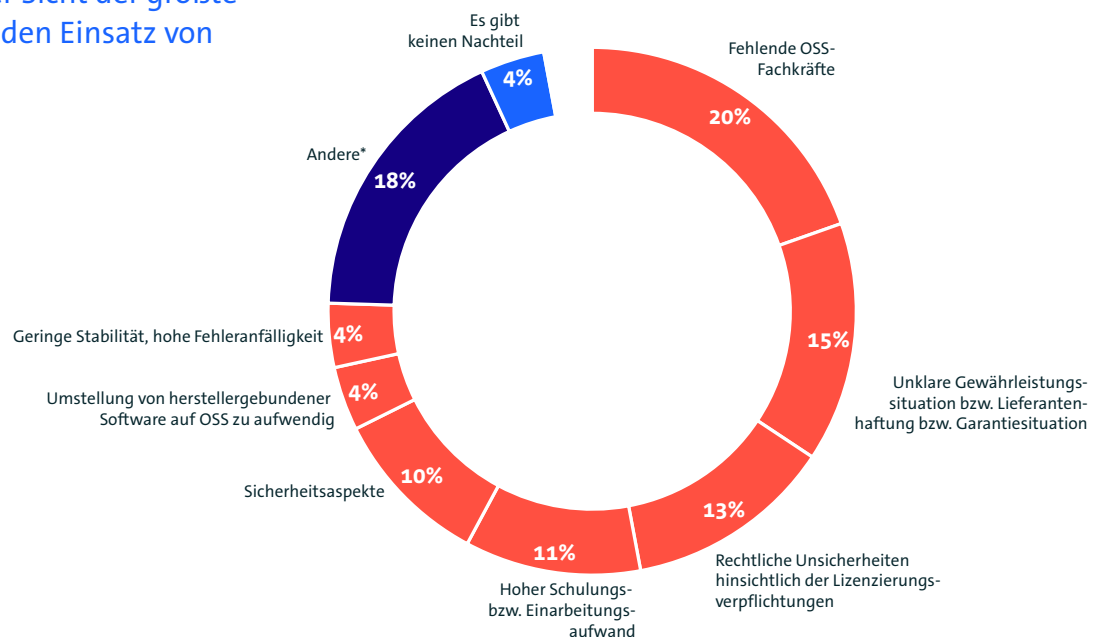
Als größter Nachteil beim Einsatz von Open Source Software (OSS) nennen Unternehmen vor allem fehlende Fachkräfte: 20 Prozent sehen hierin das größte Hemmnis. Ebenfalls häufig genannt werden unklare Gewährleistungssituationen sowie Fragen der Lieferantenhaftung oder Garantien (15 Prozent). 13 Prozent bezeichnen rechtliche Unsicherheiten hinsichtlich Lizenzverpflichtungen als problematisch.

Auch ein hoher Schulungs- und Einarbeitungsaufwand wird von 11 Prozent als Nachteil hervorgehoben, während 10 Prozent Sicherheitsaspekte kritisch sehen. Geringe Stabilität und hohe Fehleranfälligkeit (4 Prozent) sowie der Aufwand

bei der Umstellung von herstellergebundener Software auf OSS (4 Prozent) spielen dagegen eine geringere Rolle.

Bemerkenswert ist, dass 18 Prozent andere Nachteile nennen, während 4 Prozent der Befragten überhaupt keine Nachteile erkennen. Insgesamt zeigt sich, dass vor allem personelle, rechtliche und organisatorische Herausforderungen den Einsatz von OSS bremsen.

Und was ist aus Ihrer Sicht der größte Nachteil, der gegen den Einsatz von OSS spricht?



Basis: Alle Befragten (n=1.152) | Rest: »Weiß nicht/keine Angabe« | Quelle: Bitkom Research 2025

*Fehlende Schnittstellen zu anderen Systemen (3%); Fehlende Schulungsangebote (3%); Mangelnder kommerzieller Support, fehlende Enterprise Versionen (3%); Fehlende Zertifizierungen für OSS (3%); Herausforderungen in der Supply Chain Security (2%); Fehlende OSS-Lösungen für unsere Anwendungsfälle (2%); Mangelnde Akzeptanz im Unternehmen (1%); Schlechter Ruf von OSS (1%)

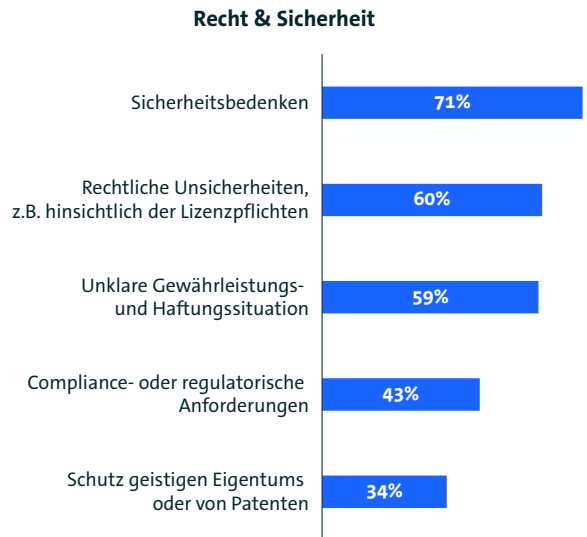
Abbildung 9: Wahrgenommene Nachteile von OSS für Unternehmen

1.8 Gründe gegen den Einsatz von OSS

Der häufigste Grund gegen den Einsatz von OSS sind Sicherheitsbedenken – 71 Prozent der Unternehmen sehen darin ein zentrales Hindernis. Auch rechtliche Unsicherheiten bei Lizenzpflichten (60 Prozent) und unklare Gewährleistungs- und Haftungsfragen (59 Prozent) sind weit verbreitet. Zudem stellen 43 Prozent Compliance- oder regulatorische Anforderungen als Hürde heraus, während 34 Prozent den Schutz geistigen Eigentums oder von Patenten als Problem sehen.

Ein weiteres zentrales Hemmnis sind fehlende personelle Ressourcen. 71 Prozent nennen den Mangel an Fachkräften im eigenen Unternehmen, während 46 Prozent auf unzureichenden Support im Vergleich zu kommerziellen Angeboten verweisen. Auch der Mangel an OSS-Fachkräften am Arbeitsmarkt (42 Prozent) sowie der hohe Aufwand einer Umstellung (36 Prozent) wirken bremsend. 46 Prozent geben an, dass für ihre Anwendungsfälle schlicht keine passenden OSS-Lösungen verfügbar sind. 32 Prozent beklagen mangelnde Akzeptanz im Unternehmen, 25 Prozent äußern Unsicherheit über die langfristige Unterstützung.

Aus welchen Gründen integrieren Sie in Ihrem Unternehmen bzw. einzelnen Unternehmensbereichen keinerlei OSS?

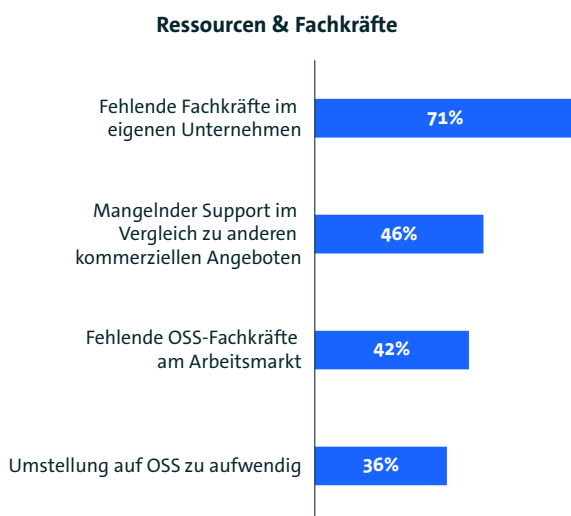


Basis: Alle Befragten (n=1.152) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2025

Abbildung 10: Gründe gegen den Einsatz von OSS: Recht & Sicherheit

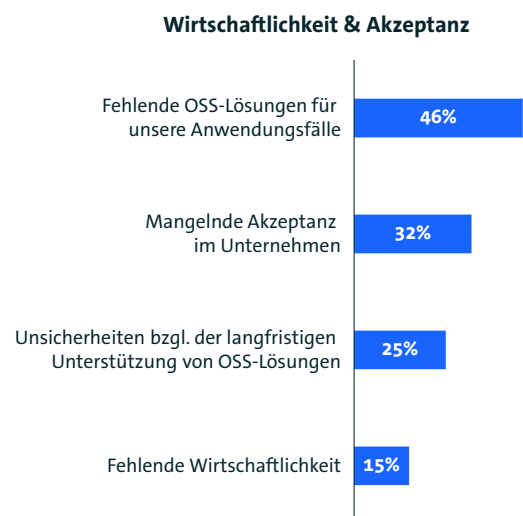
Aus welchen Gründen integrieren Sie in Ihrem Unternehmen bzw. einzelnen Unternehmensbereichen keinerlei OSS?

Aus welchen Gründen integrieren Sie in Ihrem Unternehmen bzw. einzelnen Unternehmensbereichen keinerlei OSS?



Basis: Alle Befragten (n=1.152) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2025

Abbildung 11: Gründe gegen den Einsatz von OSS: Ressourcen & Fachkräfte



Basis: Alle Befragten (n=1.152) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2025

Abbildung 12: Gründe gegen den Einsatz von OSS: Wirtschaftlichkeit & Akzeptanz

1.9 Personelle Ressourcen für Open Source Software

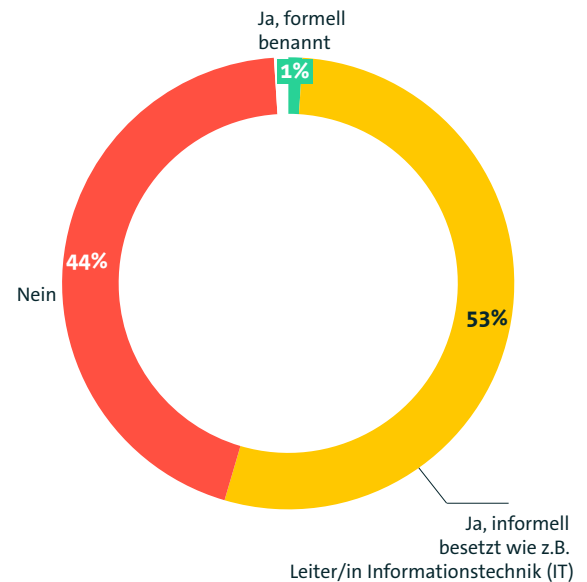
In den meisten Unternehmen (44 Prozent) gibt es keine formell benannte Person, die für das Thema Open Source Software (OSS) zuständig ist. Lediglich 1 Prozent der Befragten verfügt über eine offiziell eingesetzte Verantwortlichkeit.

In vielen Unternehmen gibt es nur eine geringe Zahl an Beschäftigten, die sich schwerpunktmäßig mit dem Management von Open Source Software (OSS) befassen. Im Durchschnitt liegt der Wert bei 1,9 Vollzeitäquivalenten (FTE).

Fast die Hälfte der Unternehmen (49 Prozent) setzt zwischen ein und fünf Vollzeitkräfte für das OSS-Management ein. 10 Prozent beschäftigen weniger als ein Vollzeitäquivalent, während 4 Prozent fünf oder mehr FTE einsetzen.

Gleichzeitig zeigt sich, dass in zahlreichen Unternehmen keine feste Zuordnung existiert: 18 Prozent erledigen entsprechende Aufgaben bei Bedarf intern, 3 Prozent vergeben diese extern. Bei 8 Prozent spielt OSS-Management überhaupt keine Rolle.

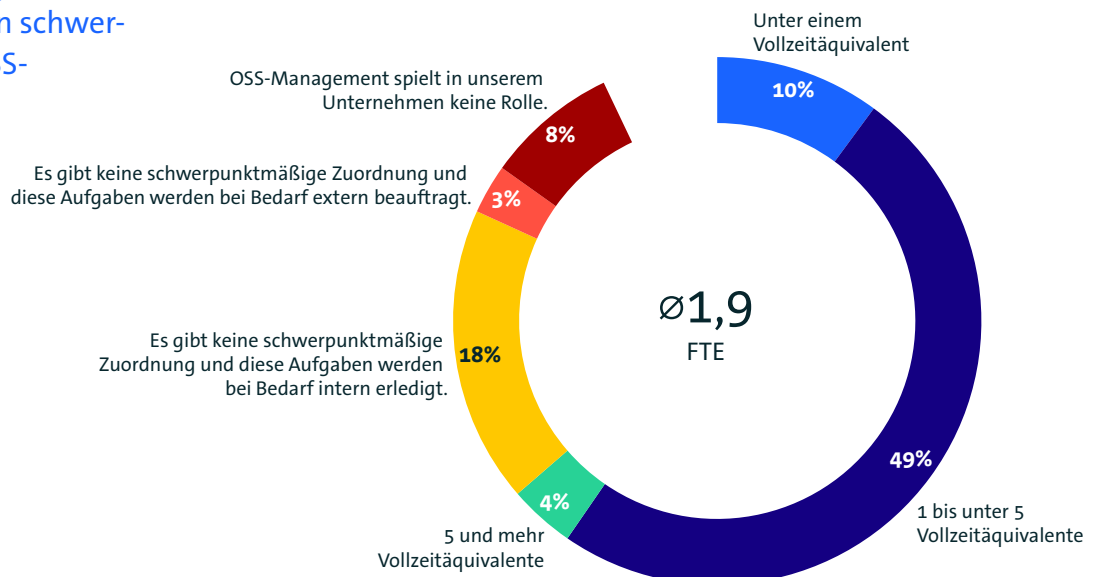
Gibt es in Ihrem Unternehmen eine Person, die für das Thema Open Source Software zuständig ist?



Basis: Alle Befragten (n=1.152) | Rest: »Weiß nicht/keine Angabe« | Quelle: Bitkom Research 2025

Abbildung 13: Personelle Zuständigkeiten und Ressourcen für OSS-Management in Unternehmen

Wie viele Beschäftigte befassen sich in Ihrem Unternehmen schwerpunktmäßig mit OSS-Management*?



*Unter OSS-Management verstehen wir die Praktiken und Prozesse, die verwendet werden, um die Entwicklung und den Einsatz von OSS innerhalb Ihres Unternehmens zu steuern und zu koordinieren.
Basis: Unternehmen, die OSS verwenden, integrieren oder (weiter-)entwickeln (n=839) | Rest: »Weiß nicht/keine Angabe« | Quelle: Bitkom Research 2025

Abbildung 14: Anzahl der Beschäftigten, die sich im Unternehmen schwerpunktmäßig mit OSS-Management beschäftigen

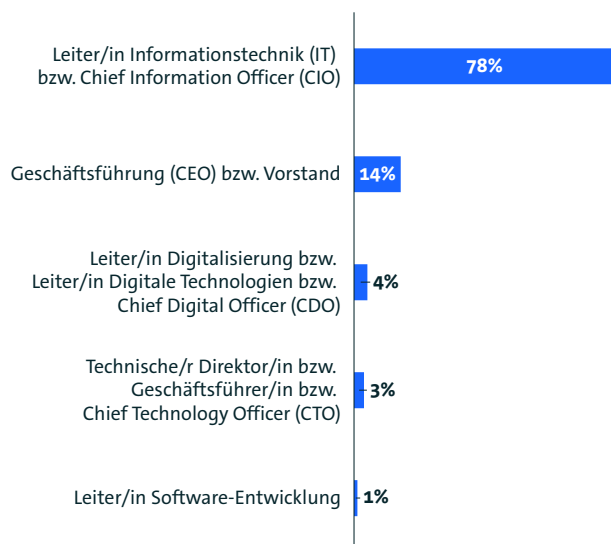
2 Policy & Compliance

2 Policy & Compliance

Zur Verantwortung für Open Source Software gehören neben dem Einsatz, der Integration, und ggf. der Weiterentwicklung, auch die Einhaltung rechtlicher Rahmenbedingungen und Compliance-Vorgaben. Bei nur 1 Prozent der Unternehmen gibt es eine formell benannte Person für OSS (s. ↗Kapitel 1.7). Deutlich häufiger (bei 53 Prozent der Unternehmen) übernehmen diese Aufgabe informell bestimmte Personen, wie etwa die IT-Leitung. Knapp jedes zweite Unternehmen (44 Prozent) hat hingegen überhaupt keine zuständige Person für OSS benannt.

2.1 Zuständigkeit für Open Source Software

Und wer ist in Ihrem Unternehmen zuständig für das Thema Open Source Software?



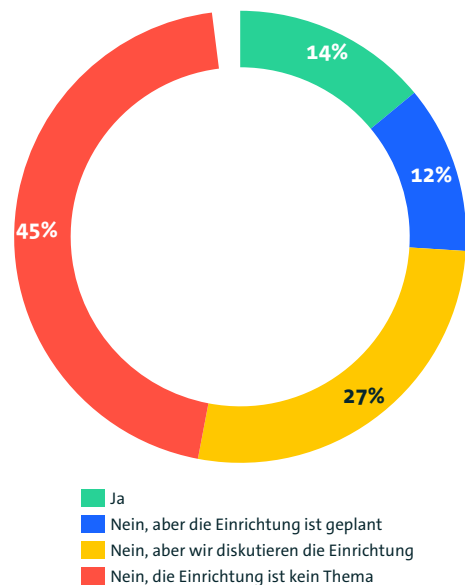
Basis: Unternehmen, bei denen eine Person informell für Open Source Software zuständig ist (n=616)
Quelle: Bitkom Research 2025

Abbildung 15: Zuständigkeiten für OSS im Unternehmen

78 Prozent geben an, dass der Leiter bzw. die Leiterin der Informationstechnik oder der Chief Information Officer (CIO) dafür verantwortlich ist. In 14 Prozent der Unternehmen ist die Geschäftsführung oder der Vorstand zuständig. Wesentlich seltener übernehmen andere Rollen diese Verantwortung: 4 Prozent nennen den Chief Digital Officer (CDO) oder die Leitung Digitalisierung, 3 Prozent den Chief Technology Officer (CTO) bzw. technische Direktoren.

Nur wenige Unternehmen haben bislang ein Open Source Program Office (OSPO) eingerichtet. Lediglich 14 Prozent verfügen bereits über eine solche zentrale Organisationseinheit für Open-Source-Belange. Weitere 12 Prozent planen die Einrichtung konkret, und 27 Prozent diskutieren derzeit darüber. Fast die Hälfte der Unternehmen (45 Prozent) erklärt jedoch, dass die Einrichtung eines OSPO für sie kein Thema ist.

Haben Sie ein Open Source Program Office* (OSPO) eingerichtet?



*eine zentrale Organisationseinheit, die sich übergreifend um Open-Source-Software-Belange kümmert
Basis: Unternehmen, die OSS verwenden, integrieren oder (weiter-)entwickeln (n=839)
Rest: »Weiß nicht/keine Angabe« | Quelle: Bitkom Research 2025

Abbildung 16: Anteil der Unternehmen mit Open Source Program Offices

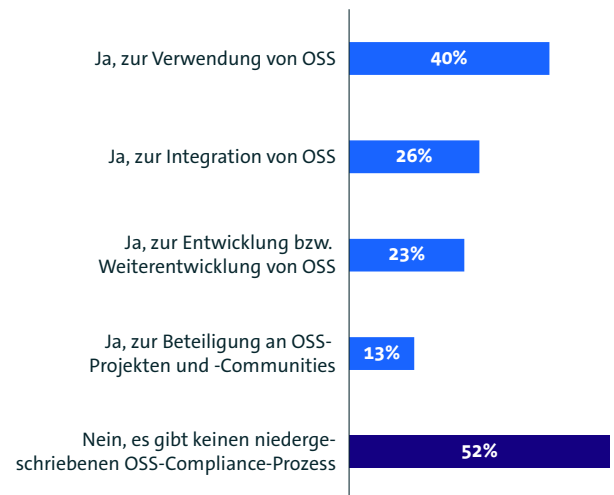
2.2 OSS-Policy

Die Mehrheit der Unternehmen, die mit OSS zu tun haben, verfügt über keine **allgemeine OSS-Policy, also schriftlich festgehaltene Richtlinien und Regeln zum Umgang mit OSS**: 62 Prozent haben in ihrem Unternehmen keine solcher Regelungen. Der Anteil steigt kontinuierlich: 22 Prozent in 2021, 26 Prozent in 2023, und 36 Prozent in 2025.

Knapp ein Drittel (29 Prozent) hat Vorgaben zur Verwendung von OSS etabliert. Weitere Bereiche werden deutlich seltener abgedeckt: 16 Prozent besitzen eine Policy zur Integration von OSS in ihre Systeme, und 15 Prozent haben Regeln zur Entwicklung oder Weiterentwicklung.

Mehr als die Hälfte der Unternehmen (52 Prozent) verfügt über keinerlei niedergeschriebene **Compliance-Vorgaben, die Mitarbeitenden die Einhaltung regulatorischer Vorgaben verbindlich vorschreibt**. Bei den Unternehmen, die entsprechende Vorgaben haben, stehen Regelungen zur Verwendung von OSS an erster Stelle: 40 Prozent haben dafür verbindliche Prozesse etabliert.

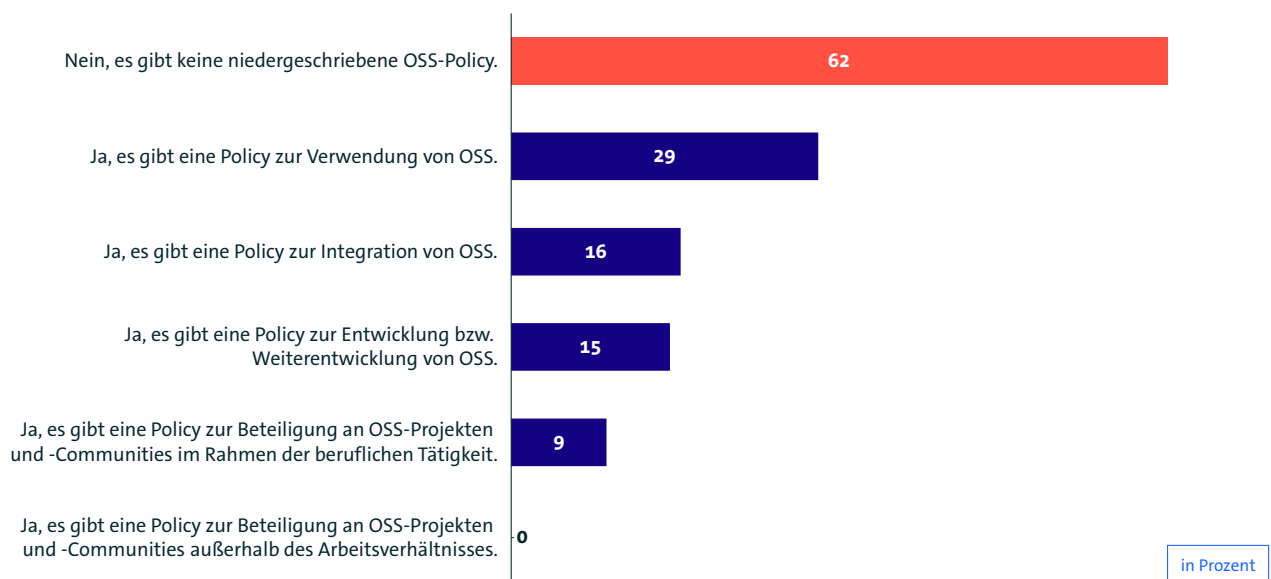
Gibt es in Ihrem Unternehmen niedergeschriebene Compliance-Prozesse, welche die Einhaltung der regulatorischen Vorgaben im Umgang mit OSS für Mitarbeitende verbindlich vorschreiben?



Basis: Unternehmen, die OSS verwenden, integrieren, (weiter-)entwickeln, oder sich anderweitig beteiligen (n=841) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2025

Abbildung 17: Compliance-Prozesse für Mitarbeitende im Umgang mit OSS

Gibt es in Ihrem Unternehmen eine OSS-Policy*?



*d.h. ein Dokument, in dem Richtlinien und Regeln zum Umgang mit OSS in Ihrem Unternehmen niedergeschrieben sind
Basis: Unternehmen, die OSS verwenden, integrieren, (weiter-)entwickeln, oder sich anderweitig beteiligen (n=841) | Mehrfachnennungen möglich | Nicht dargestellt: »Weiß nicht/keine Angabe« | Quelle: Bitkom Research 2025

Abbildung 18: OSS-Policy in Unternehmen

2.3 Europäische Compliance-Vorgaben

Die Auseinandersetzung mit dem Thema Compliance in Unternehmen hat sich über die Jahre unterschiedlich entwickelt. 7 Prozent der befragten Unternehmen beschäftigen sich bereits seit der Zeit vor 2000 verstärkt mit Compliance-Fragen.

Ein Viertel (25 Prozent) begann im Zeitraum 2000 bis 2010, weitere 23 Prozent im Zeitraum 2010 bis vor 2020. Noch einmal 23 Prozent gaben an, dass sie sich erst ab 2020 intensiver mit Compliance befassen.

Für viele Unternehmen waren regulatorische Neuerungen ausschlaggebend, um ihre Compliance-Prozesse neu zu definieren oder bestehende Abläufe zu ersetzen. Besonders häufig genannt wird die Critical Entities Resilience (CER), die für 61 Prozent der Unternehmen maßgeblich war. Knapp dahinter folgt der Cyber Resilience Act (CRA) mit 57 Prozent.

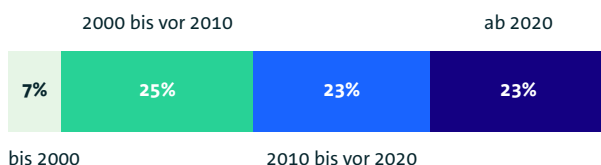
Die Product Liability Directive (PLD) spielte bei 44 Prozent eine Rolle, während 38 Prozent ihre Compliance-Prozesse aufgrund des Digital Operational Resilience Act (DORA) ange-

passt haben. Eine vergleichsweise geringe Bedeutung hatte die Network and Information Security Directive (NIS2), die nur 2 Prozent der Befragten beeinflusst hat.

Darüber hinaus geben 25 Prozent an, dass nicht regulatorische Ereignisse oder andere Themen ausschlaggebend für Veränderungen im Compliance-Bereich waren. Damit wird deutlich, dass vor allem europäische Vorgaben wie CER und CRA die zentralen Treiber für Anpassungen in den Unternehmen sind.

58 Prozent der Unternehmen, die OSS (weiter-) entwickeln oder in ihre Produkte integrieren, werden als Folge des CRA »mehr OSS integrieren«. Bei 31 Prozent soll die Nutzung »unverändert« bleiben, 6 Prozent wollen weniger OSS integrieren.

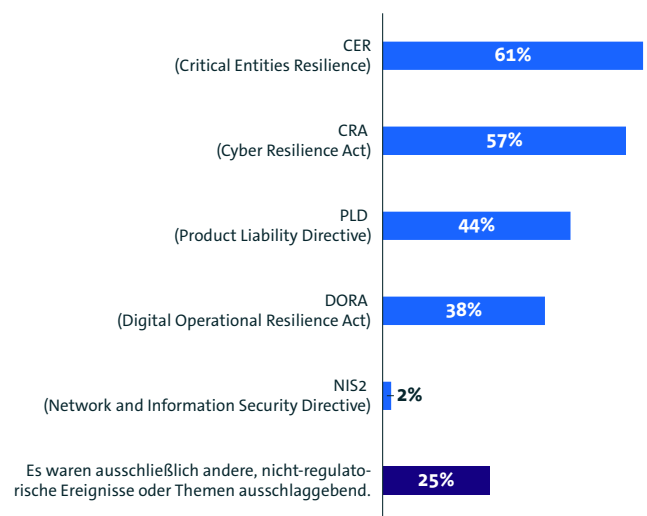
In welchem Jahr hat Ihr Unternehmen angefangen, sich verstärkt mit dem Thema Compliance zu beschäftigen?



Basis: Organisationen mit Compliance-Prozess (n=367) | Nicht dargestellt: »Weiß nicht/keine Angabe«
Quelle: Bitkom Research 2025

Abbildung 19: Beginn der Beschäftigung mit Compliance-Fragen

Welche regulatorischen Neuerungen waren ausschlaggebend dafür, einen Compliance-Prozess zu definieren bzw. den bestehenden Compliance-Prozess abzulösen?



Basis: Organisationen mit Compliance-Prozess (n=367) | Nicht dargestellt: »Weiß nicht/keine Angabe«
Quelle: Bitkom Research 2025

Abbildung 20: Einfluss europäischer Vorgaben (CER, CRA, PLD, DORA, NIS2) auf Compliance-Prozesse

2.4 Compliance-Maßnahmen und -Instrumente

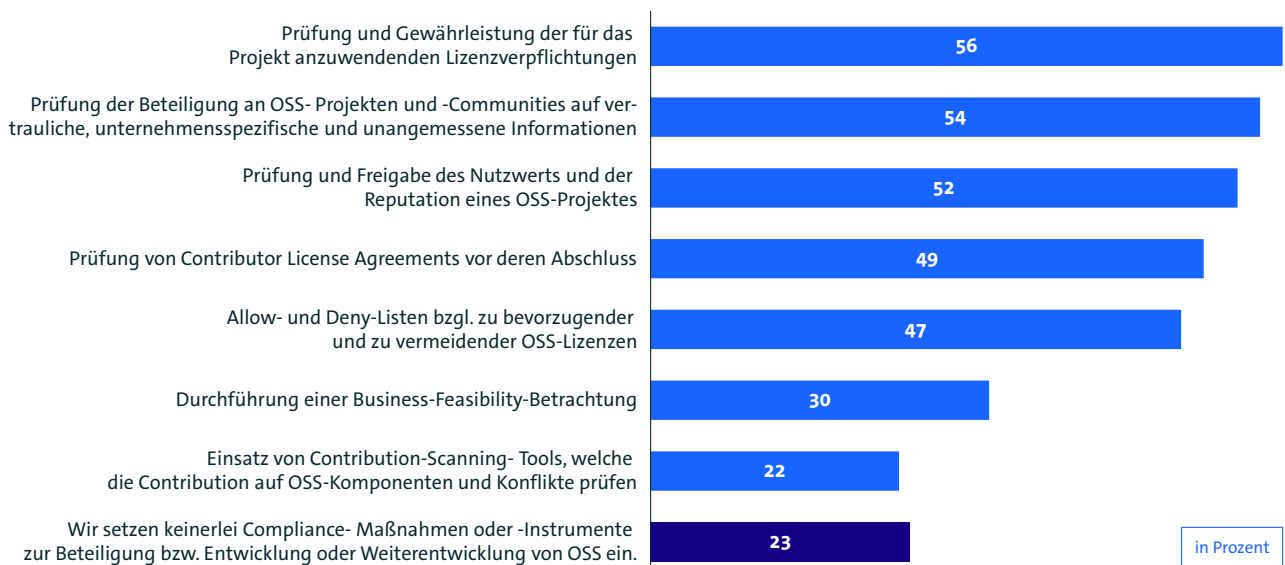
Beim internen Compliance-Management zur Beteiligung an Open Source Software (OSS)-Projekten oder zur Weiterentwicklung von OSS setzen Unternehmen vor allem auf formale Prüf- und Kontrollmaßnahmen. Am häufigsten wird die Prüfung und Gewährleistung der anzuwendenden Lizenzverpflichtungen genannt (56 Prozent).

Ebenso prüfen 54 Prozent die Beteiligung an Projekten und Communities auf vertrauliche oder unternehmensspezifische Informationen. 52 Prozent bewerten und geben den Nutzwert sowie die Reputation eines Projekts frei. Fast die Hälfte der Unternehmen prüft Contributor License Agreements (49

Prozent) oder nutzt Allow- und Deny-Listen für bevorzugte bzw. zu vermeidende Lizenzen (47 Prozent).

Weniger verbreitet sind Business-Feasibility-Betrachtungen (30 Prozent) oder der Einsatz von Contribution-Scanning-Tools (22 Prozent). Auffällig ist zudem, dass 23 Prozent keinerlei Compliance-Maßnahmen oder -Instrumente in diesem Bereich einsetzen.

Welche Maßnahmen und Instrumente kommen für Ihr internes Compliance Management zur Beteiligung an OSS-Projekten bzw. zur (Weiter-)Entwicklung von OSS zum Einsatz?



Basis: Unternehmen, die OSS verwenden, integrieren oder (weiter-)entwickeln (n=839) | Mehrfachnennungen möglich | Nicht dargestellt: »Weiß nicht/keine Angabe« | Quelle: Bitkom Research 2025

Abbildung 21: Eingesetzte Compliance-Maßnahmen und -Instrumente im OSS-Management

2.5 OSS-Standards in der Supply Chain

Beim Umgang mit der Supply Chain im Rahmen des Open Source Software (OSS)-Managements setzen Unternehmen unterschiedliche Standards ein. Am häufigsten wird dabei die ISO 5230 zu Lizenz-Compliance genutzt, die von 37 Prozent der Befragten angewendet wird.

32 Prozent greifen auf die BSI-Richtlinie 03183 zu SBOM (Software Bill of Materials) zurück – und damit 23 Prozent aller Unternehmen – sowie ebenfalls 32 Prozent auf die ISO 18974 zu OSS-Security.

Damit zeigt sich, dass Standards zwar in einem Teil der Unternehmen Anwendung finden, jedoch keines der genannten Regelwerke von einer Mehrheit genutzt wird.

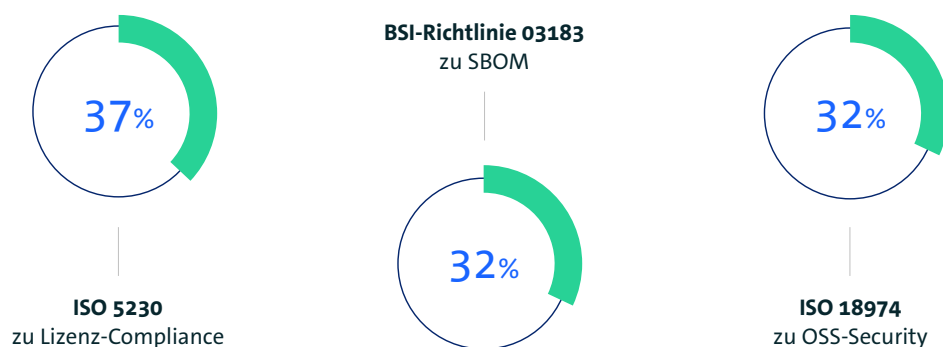
Vor allem Lizenz-Compliance nach ISO 5230 ist verbreiteter, während Sicherheits- und Transparenzstandards bislang von knapp einem Drittel berücksichtigt werden.



Basis: Alle Befragten (n=1.152) | Quelle: Bitkom Research 2025

Abbildung 22: Einsatz von SBOMs in Unternehmen

Welche der folgenden Standards verwenden Sie in Ihrem Unternehmen zum OSS-Management im Umgang mit der Supply Chain?



Basis: Unternehmen, die OSS verwenden, integrieren oder (weiter-)entwickeln (n=839) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2025

Abbildung 23: Verbreitung von Standards in der Supply Chain (ISO 5230, ISO 18974, BSI 03183)

2.6 Budget für Compliance-Maßnahmen

Beim Thema Budget für OSS-Compliance zeigt sich im Vergleich zu 2024 ein eher stabiles Bild. 39 Prozent der Unternehmen geben an, dass ihr Budget unverändert geblieben ist. 21 Prozent verfügen über mehr Mittel – davon 14 Prozent »eher mehr« und 7 Prozent »deutlich mehr«.

Demgegenüber berichten nur 10 Prozent von einer Verringerung der finanziellen Mittel, aufgeteilt in 6 Prozent »eher weniger« und 4 Prozent »deutlich weniger«. Auffällig ist

zudem, dass ein Viertel der Unternehmen (25 Prozent) kein festgelegtes Budget für OSS-Compliance hat.

Insgesamt überwiegt damit die Tendenz zu stabilen oder leicht steigenden Budgets, während echte Kürzungen vergleichsweise selten vorkommen.

Verglichen mit dem Jahr 2024: Haben Sie in diesem Jahr mehr oder weniger Budget für das Thema OSS-Compliance zur Verfügung?



in Prozent

Basis: Unternehmen, die OSS verwenden, integrieren, (weiter-)entwickeln, oder sich anderweitig beteiligen (n=841) | Nicht dargestellt: »Weiß nicht/keine Angabe« | Quelle: Bitkom Research 2025

Abbildung 24: Entwicklung der Budgets für OSS-Compliance

3 Zukunftsaussichten, Politik & KI

3 Zukunftsaussichten, Politik & KI

Der Blick in die Zukunft zeigt, dass Künstliche Intelligenz (KI) und Open Source eng miteinander verknüpft werden. Unternehmen setzen KI in der eigenen Softwareentwicklung bislang eher zögerlich ein: 38 Prozent planen keinen Einsatz, ein Drittel (33 Prozent) bereitet diesen vor, während 29 Prozent KI bereits gelegentlich oder regelmäßig nutzen. Parallel dazu werden Open-Source-KI-Modelle von mehr als der Hälfte (51 Prozent) der Befragten als empfehlenswert bewertet, 45 Prozent sehen darin eine Möglichkeit zur Vermeidung künftiger Abhängigkeiten.

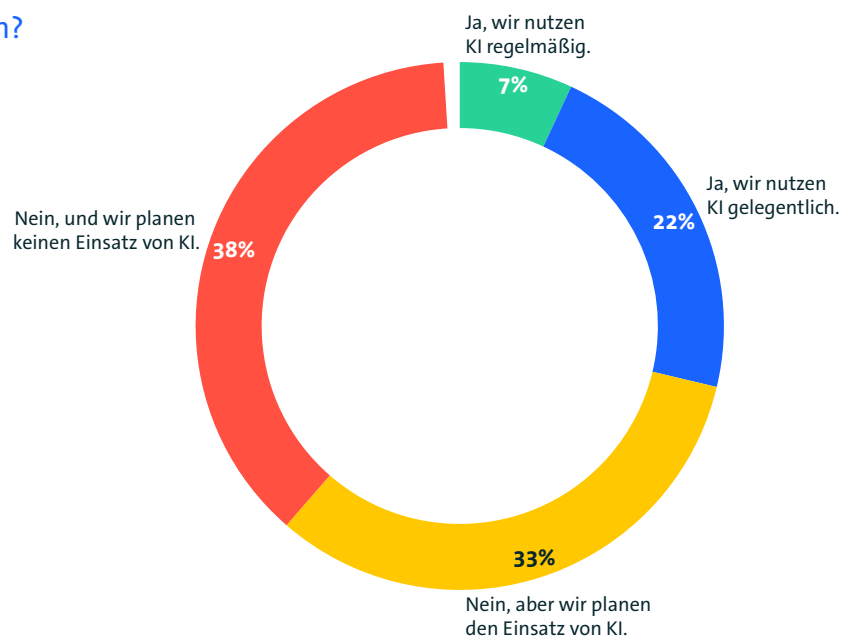
3.1 KI in der Softwareentwicklung

Der Einsatz von Künstlicher Intelligenz (KI) in der Softwareentwicklung ist in vielen Unternehmen noch ausbaufähig. 38 Prozent geben an, dass sie derzeit keine KI nutzen und dies auch nicht planen. Ein weiteres Drittel (33 Prozent) setzt bislang ebenfalls keine KI ein, plant jedoch die Einführung.

Aktiv im Einsatz ist KI bei knapp drei von zehn Unternehmen: 22 Prozent nutzen sie gelegentlich, während nur 7 Prozent angeben, KI regelmäßig in der Softwareentwicklung einzusetzen.

Damit zeigt sich ein gemischtes Bild: Während ein Teil der Unternehmen bereits erste Erfahrungen mit KI sammelt, bleibt sie für die Mehrheit entweder ein Zukunftsthema oder spielt bislang keine Rolle.

Setzt Ihr Unternehmen bereits KI in der Softwareentwicklung ein?



Basis: Alle Befragten (n=1.152) | Rest: »Weiß nicht/keine Angabe« | Quelle: Bitkom Research 2025

Abbildung 25: Einsatz von KI in der Softwareentwicklung in Unternehmen

3.2 Open-Source-KI-Modelle

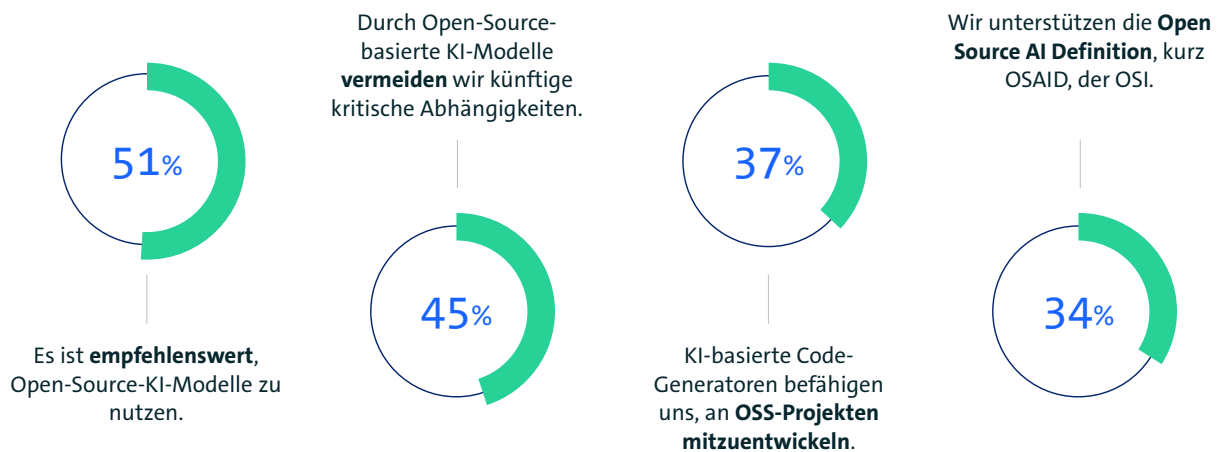
Mehr als die Hälfte der befragten Unternehmen (51 Prozent) hält es für empfehlenswert, Open-Source-KI-Modelle zu nutzen. 45 Prozent sehen darin zudem eine Möglichkeit, künftige kritische Abhängigkeiten zu vermeiden.

37 Prozent geben an, dass KI-basierte Code-Generatoren sie befähigen, aktiv an Open-Source-Projekten mitzuwirken. Ein Drittel der Unternehmen (34 Prozent) unterstützt außerdem

die »Open Source AI Definition« (OSAID) der Open Source Initiative (OSI).

Damit zeigt sich, dass Open-Source-KI in vielen Unternehmen als sinnvoller Ansatz bewertet wird – sei es zur Stärkung der Unabhängigkeit, zur aktiven Beteiligung an Projekten oder zur Unterstützung gemeinsamer Standards.

Inwiefern treffen die folgenden Aussagen auf Ihr Unternehmen bzw. Ihrer Meinung nach zu?



Basis: Alle Befragten (n=1.152) | Antworten für »Trifft voll und ganz zu« und »Trifft eher zu« | Quelle: Bitkom Research 2025

Abbildung 26: Einschätzungen zu Open-Source-KI-Modellen

3.3 Nutzung von und Bedenken gegenüber KI-Code-Generatoren



Basis: Alle Befragten (n=1.152) | Werte für »Trifft voll und ganz« oder »eher« zu | Quelle: Bitkom Research 2025

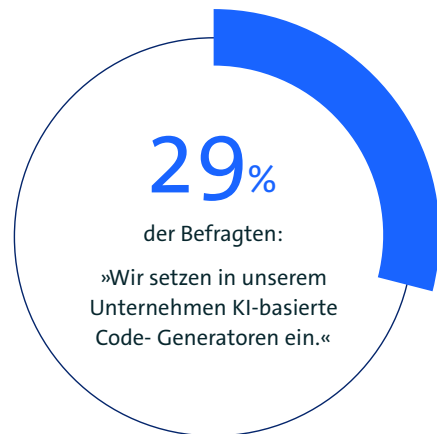
Abbildung 27: Wahrgenommene Risiken durch KI-generierten Code

Mehr als die Hälfte der Unternehmen sieht den Einsatz von KI-generiertem Code kritisch. 56 Prozent der Befragten stimmen der Aussage zu, dass die Nutzung solcher Codes eine Gefahr darstellt.

Damit wird deutlich, dass trotz der wachsenden Bedeutung von KI in der Softwareentwicklung erhebliche Sicherheits- und Vertrauensbedenken bestehen. Viele Unternehmen sehen potenzielle Risiken – etwa in Bezug auf Qualität, Sicherheit oder rechtliche Fragen – stärker im Vordergrund als mögliche Chancen.

Knapp drei von zehn Unternehmen setzen bereits KI-basierte Code-Generatoren in ihrer Softwareentwicklung ein. 29 Prozent der Befragten bestätigen, dass solche Tools in ihrem Unternehmen genutzt werden.

KI findet zwar schon praktische Anwendung, ihre Verbreitung ist aber noch begrenzt. Während ein Teil der Unternehmen die Potenziale bereits aktiv ausschöpft, zögern viele andere offenbar noch – möglicherweise aufgrund von Bedenken hinsichtlich Qualität, Sicherheit oder rechtlichen Fragen.



Basis: Alle Befragten (n=1.152) | Werte für »Trifft voll und ganz« oder »eher« zu | Quelle: Bitkom Research 2025

Abbildung 28: Nutzung von KI-Code-Generatoren in Unternehmen

3.4 Open-Source-KI-Modelle

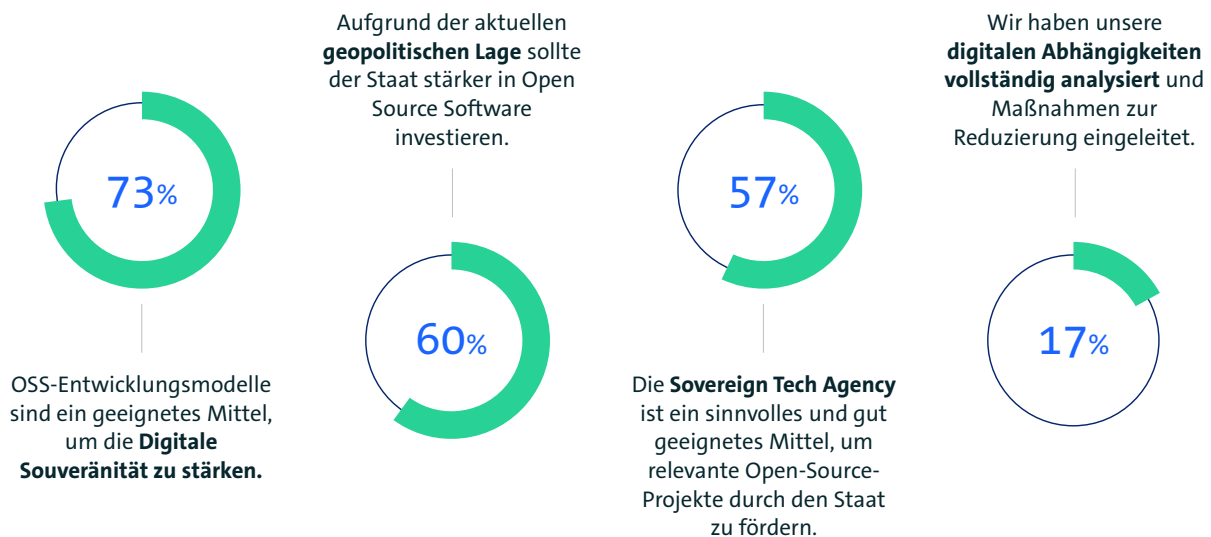
Die Mehrheit der Unternehmen sieht in Open Source Software (OSS) ein wichtiges Instrument zur Stärkung der digitalen Souveränität. 73 Prozent stimmen der Aussage zu, dass OSS-Entwicklungsmodelle hierfür besonders geeignet sind.

60 Prozent sprechen sich zudem dafür aus, dass der Staat aufgrund der aktuellen geopolitischen Lage stärker in OSS investieren sollte. Auch staatliche Förderinstrumente wie die Sovereign Tech Agency finden Zustimmung: 57 Prozent der

Befragten halten sie für ein sinnvolles Mittel, um relevante Open-Source-Projekte gezielt zu unterstützen.

Deutlich geringer fällt die Zustimmung bei der praktischen Umsetzung im eigenen Unternehmen aus. Nur 17 Prozent geben an, ihre digitalen Abhängigkeiten bereits vollständig analysiert und konkrete Maßnahmen zur Reduzierung eingeleitet zu haben.

Inwiefern treffen die folgenden Aussagen auf Ihr Unternehmen bzw. Ihrer Meinung nach zu?



Basis: Alle Befragten (n=1.152) | Quelle: Bitkom Research 2025

Abbildung 29: Zustimmung zu Aussagen über OSS als Instrument für Digitale Souveränität

4 Open Source im Public Sector

4 Open Source im Public Sector

Im öffentlichen Sektor ist Open Source weit verbreitet, wenn auch mit teils abweichenden Schwerpunkten im Vergleich zur Wirtschaft. 63 Prozent der befragten Behörden und Organisationen setzen OSS ein, wobei durchschnittlich 4 Vollzeitäquivalente für das Management bereitgestellt werden – etwa doppelt so viel wie in der Wirtschaft. Die Grundhaltung ist mehrheitlich positiv: 52 Prozent sind sehr oder eher aufgeschlossen, 32 Prozent jedoch unentschieden.

4.1 Grundhaltung zu Open Source Software

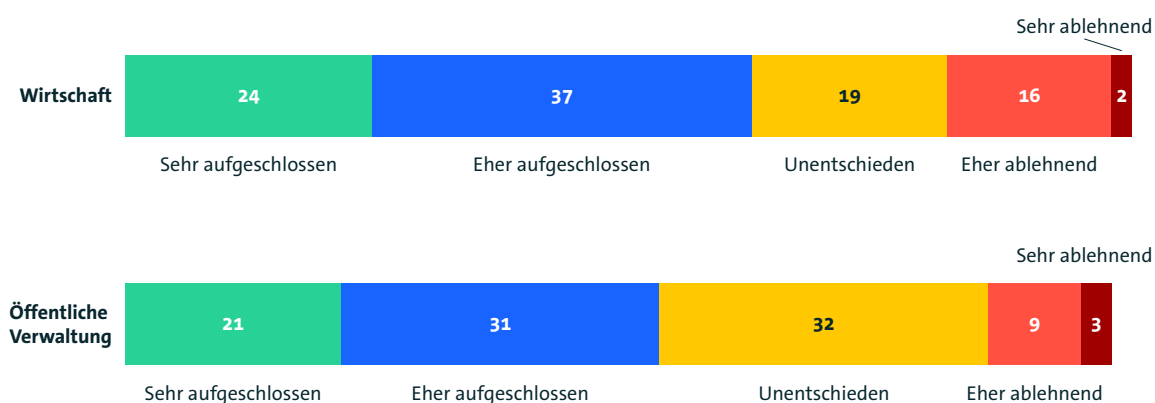
In der Wirtschaft ist die Haltung überwiegend positiv: 24 Prozent sind sehr aufgeschlossen und 37 Prozent eher aufgeschlossen. Damit signalisiert mehr als die Hälfte eine klare Offenheit. Unentschieden äußern sich 19 Prozent, während 16 Prozent eher ablehnend und nur 2 Prozent sehr ablehnend eingestellt sind (s. ↗Kapitel 1.1).

Auch in der öffentlichen Verwaltung zeigt sich ein positives Bild, wenngleich mit etwas geringerer Zustimmung. Hier sind 21 Prozent sehr aufgeschlossen und 31 Prozent eher aufge-

schlossen. Auffällig ist jedoch der höhere Anteil Unentschiedener: 32 Prozent der Befragten haben sich weder klar positiv noch negativ positioniert. Ablehnend äußern sich 9 Prozent eher und 3 Prozent sehr

Insgesamt wird OSS sowohl von der Wirtschaft als auch von der öffentlichen Verwaltung überwiegend positiv gesehen, wobei die Wirtschaft stärker zustimmend reagiert und die Verwaltung zurückhaltender auftritt, mit einem deutlich größeren Anteil Unentschiedener.

Wie steht Ihre Organisation generell zum Thema OSS?



in Prozent

Basis: Alle Befragten (Wirtschaft: n=1.152 | Öffentliche Verwaltung: n=103) | Rest: »Weiß nicht/keine Angabe« | Quelle: Bitkom Research 2025

Abbildung 30: Grundhaltung gegenüber OSS: Wirtschaft vs. öffentlicher Sektor

4.2 Einsatz von Open Source Software

In der Wirtschaft nutzen 73 Prozent OSS, während 27 Prozent darauf verzichten (s. ↗Kapitel 1.3). In der öffentlichen Verwaltung liegt der Anteil etwas niedriger: 63 Prozent setzen OSS ein, 35 Prozent nicht

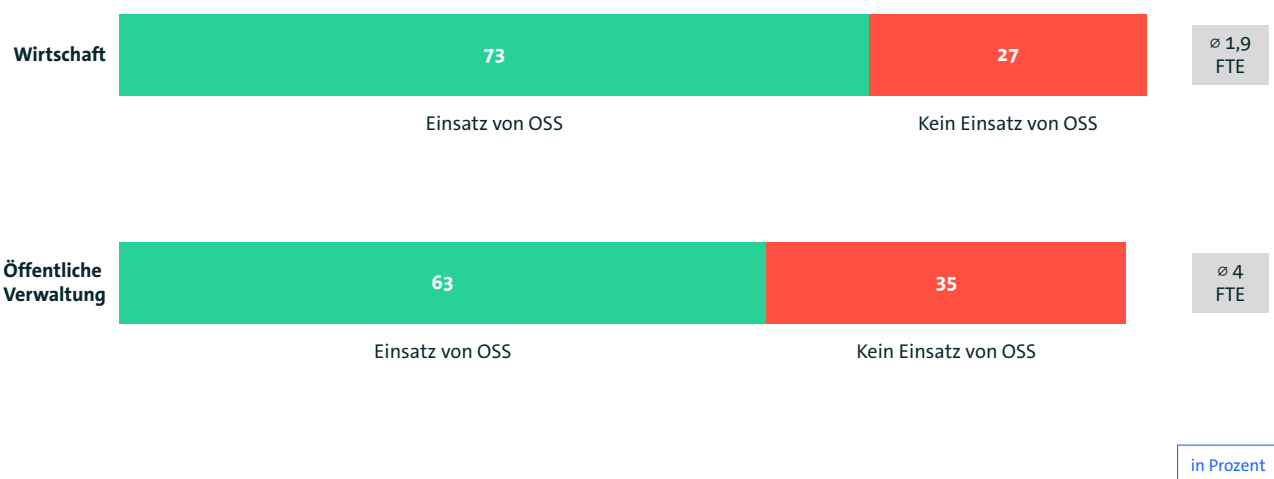
Ein weiterer Aspekt ist die Anzahl der Beschäftigten, die sich schwerpunktmäßig mit OSS-Management befassen. In der Wirtschaft sind es im Durchschnitt 1,9 Vollzeitäquivalente

(FTE), während die öffentliche Verwaltung mit 4 FTE deutlich mehr Kapazitäten einsetzt.

Insgesamt zeigt sich: OSS wird sowohl in Unternehmen als auch in der Verwaltung mehrheitlich genutzt, wobei die Wirtschaft eine etwas höhere Verbreitung aufweist. Die öffentliche Verwaltung investiert jedoch im Durchschnitt mehr Personalressourcen in das Management von OSS.

Setzt Ihre Organisation OSS ein?

Und falls ja: Wie viele Beschäftigte befassen sich schwerpunktmäßig mit OSS-Management?



Basis: Alle Befragten (Wirtschaft: n=1.152 | Öffentliche Verwaltung: n=103) | Rest: »Weiß nicht/keine Angabe« | Quelle: Bitkom Research 2025

Abbildung 31: OSS- und Personaleinsatz im Vergleich: Wirtschaft vs. öffentliche Verwaltung

4.3 Auswahlkriterien bei Open Source Software

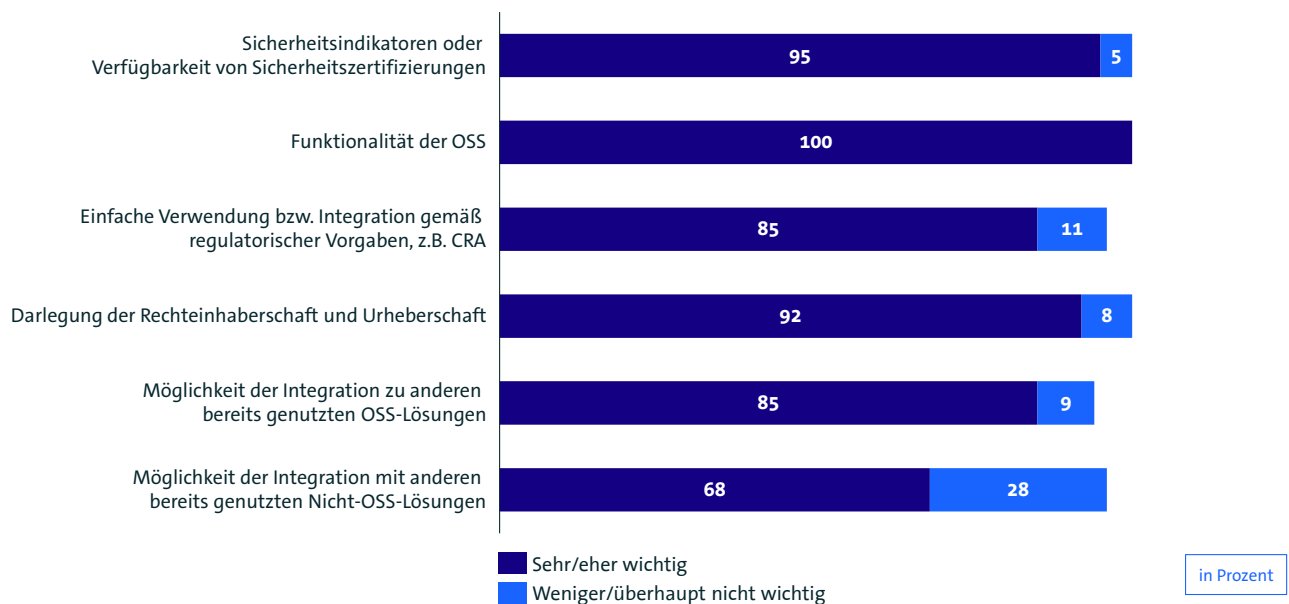
An erster Stelle steht im Public Sector die Funktionalität: Alle Befragten (100 Prozent) bewerten dieses Kriterium als sehr oder eher wichtig für die Auswahl von OSS-Projekten (in der Wirtschaft liegt der Wert mit 94 Prozent ähnlich hoch; s. ↗Kapitel 1.4). Auch Sicherheitsaspekte haben einen hohen Stellenwert: 95 Prozent achten auf Sicherheitsindikatoren oder Zertifizierungen.

Die Darlegung von Rechteinhaberschaft und Urheberschaft ist in der öffentlichen Verwaltung für 92 Prozent ein relevan-

tes Auswahlkriterium. Eine einfache Verwendung beziehungsweise Integration nach regulatorischen Vorgaben, etwa dem Cyber Resilience Act (CRA), halten 85 Prozent für wichtig. Ebenfalls 85 Prozent legen Wert auf die Möglichkeit der Integration mit anderen bereits genutzten OSS-Lösungen.

Etwas weniger stark ausgeprägt ist die Bedeutung der Integration mit bestehenden Nicht-OSS-Lösungen: 68 Prozent bewerten dieses Kriterium als wichtig.

Wie wichtig sind Ihnen die folgenden Kriterien bei der Auswahl von OSS-Projekten?



Basis: Organisationen, die OSS verwenden, integrieren oder (weiter-)entwickeln (n=65) | Mehrfachnennungen möglich | Rest: »Weiß nicht/keine Angabe« | Quelle: Bitkom Research 2025

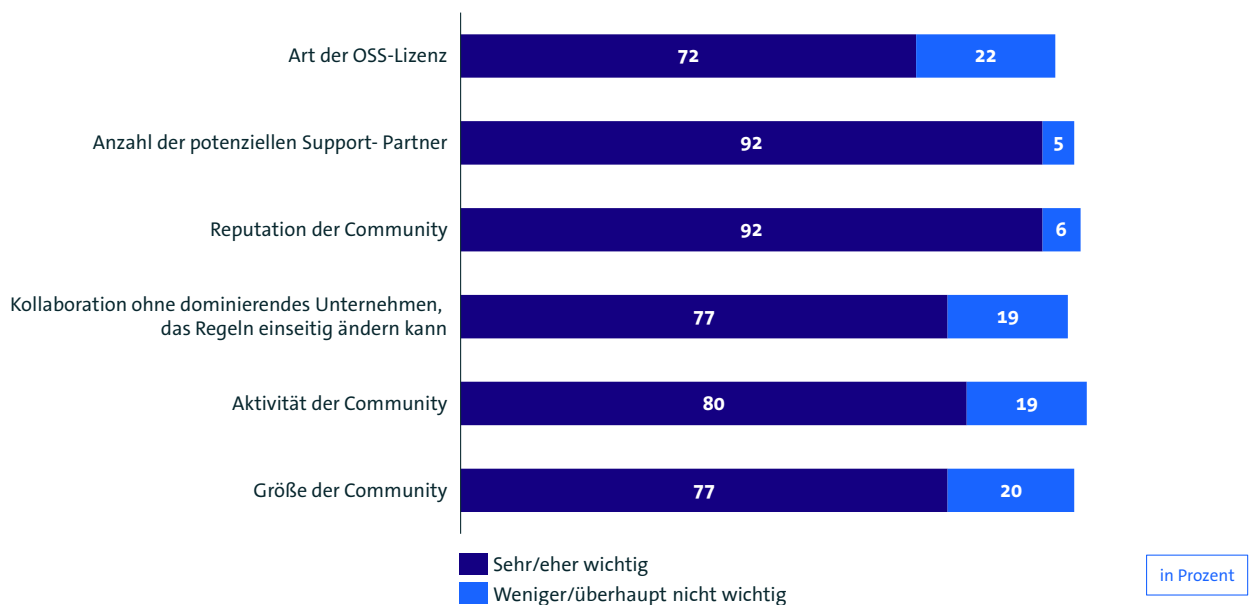
Abbildung 32: Auswahlkriterien für OSS im Public Sector: Sicherheit, Funktionalität, Rechte

Besonders stark gewichtet werden auch die Anzahl potenzieller Support-Partner (92 Prozent) sowie die Reputation der Community (ebenfalls 92 Prozent). Dazu ist die Aktivität der Community für 80 Prozent von Bedeutung.

Insgesamt wird deutlich, dass in der öffentlichen Verwaltung neben technischen Aspekten vor allem die Community-Struktur und Unterstützungsoptionen zentrale Rollen bei der Bewertung von OSS-Projekten spielen.

Die Größe der Community und die Möglichkeit zur Zusammenarbeit ohne dominierendes Unternehmen, das einseitig Regeln ändern könnte, halten jeweils 77 Prozent für wichtig. Weniger stark im Vordergrund steht die Art der OSS-Lizenz: 72 Prozent stufen dieses Kriterium als wichtig ein, während 22 Prozent es weniger oder gar nicht wichtig finden.

Wie wichtig sind Ihnen die folgenden Kriterien bei der Auswahl von OSS-Projekten?



Basis: Unternehmen, die OSS verwenden, integrieren oder (weiter-)entwickeln (n=65) | Mehrfachnennungen möglich | Rest: »Weiß nicht/keine Angabe« | Quelle: Bitkom Research 2025

Abbildung 33: Auswahlkriterien für OSS im Public Sector: Community und Support-Struktur

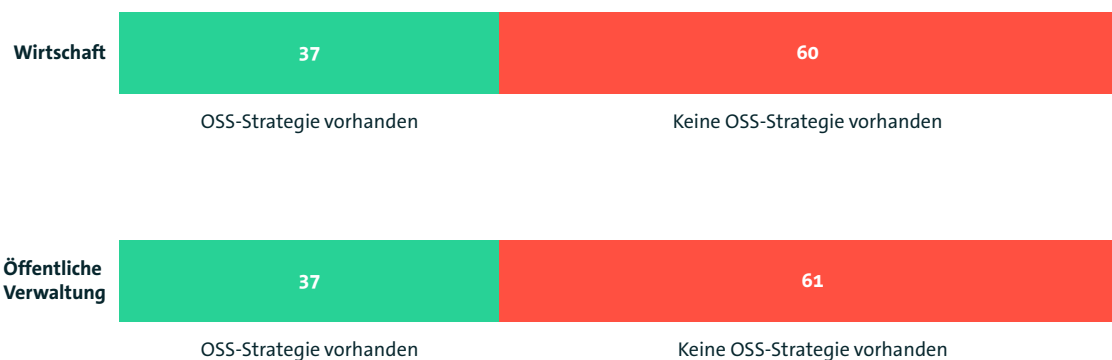
4.4 Strategie für Open Source Software

In der Wirtschaft haben 37 Prozent der Befragten eine entsprechende Strategie, während 60 Prozent keine solche Strategie verfolgen (s. ↗Kapitel 1.2).

Ein nahezu identisches Bild zeigt sich in der öffentlichen Verwaltung: Auch hier geben 37 Prozent an, eine OSS-Strategie zu besitzen, während 61 Prozent keine haben.

Damit wird deutlich, dass sowohl in Unternehmen als auch in der Verwaltung nur eine Minderheit über eine klare strategische Ausrichtung zu OSS verfügt, während die Mehrheit bislang ohne festgelegte Strategie agiert.

Gibt es in Ihrer Organisation eine Strategie zur Verwendung bzw. zur Beteiligung an OSS?



in Prozent

Basis: Alle Befragten (Wirtschaft: n=1.152 | Öffentliche Verwaltung: n=103) | Rest: »Weiß nicht/keine Angabe« | Quelle: Bitkom Research 2025

Abbildung 34: Strategien für OSS: Wirtschaft vs. öffentliche Verwaltung

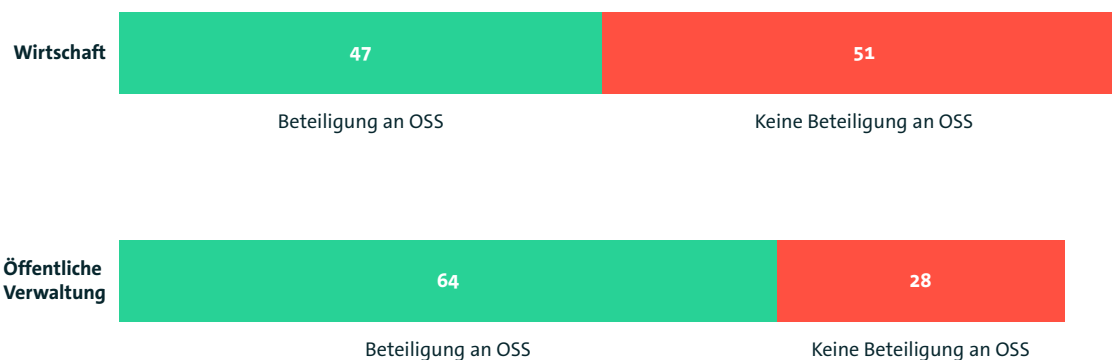
4.5 Beteiligung an der (Weiter-)Entwicklung von OSS

In der Wirtschaft beteiligen sich 47 Prozent aktiv an OSS-Projekten, während 51 Prozent keine Beteiligung angeben (s. ↗Kapitel 1.5).

Während die Beteiligung in der Wirtschaft in etwa ausgeglichen ist, engagiert sich die Mehrheit der öffentlichen Verwaltung aktiv im OSS-Umfeld.

In der öffentlichen Verwaltung fällt das Ergebnis deutlich positiver aus: Hier nehmen 64 Prozent an der Entwicklung oder Weiterentwicklung teil, lediglich 28 Prozent sind nicht beteiligt.

Beteiligen Sie sich an der Entwicklung bzw. Weiterentwicklung von OSS?



in Prozent

Basis: Alle Befragten (Wirtschaft: n=1.152 | Öffentliche Verwaltung: n=103) | Rest: »Weiß nicht/keine Angabe« | Quelle: Bitkom Research 2025

Abbildung 35: Beteiligung an der Entwicklung und Weiterentwicklung von OSS: Wirtschaft vs. Verwaltung

4.6 Vorteile von OSS

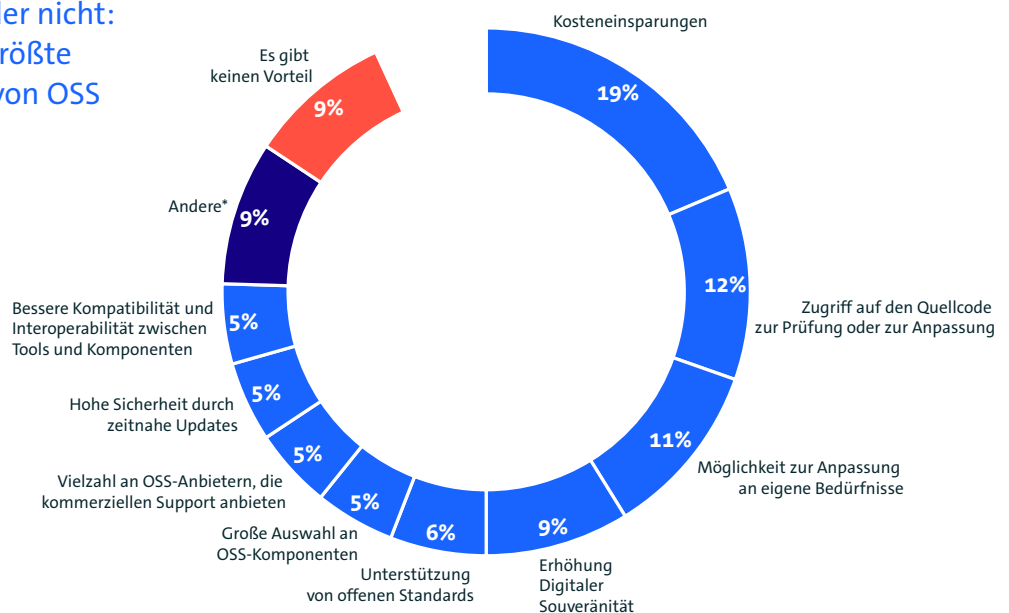
Auch in der öffentlichen Verwaltung bleibt die Preisführerschaft das beste Argument für Open-Source-Lösungen: Der am häufigsten genannte Vorteil sind Kosteneinsparungen mit 19 Prozent. Weitere wichtige Vorteile sind der Zugriff auf den Quellcode zur Prüfung oder Anpassung (12 Prozent) sowie die Möglichkeit zur individuellen Anpassung an eigene Bedürfnisse (11 Prozent).

Jeweils 9 Prozent nennen die Erhöhung der digitalen Souveränität sowie »andere« Vorteile. Ebenfalls 9 Prozent geben

an, dass sie in OSS keinen Vorteil sehen. Dieser Anteil liegt in der Wirtschaft niedriger, bei 4 Prozent (s. ↗Kapitel 1.6).

Mit jeweils 5 Prozent werden weitere Kriterien wie die große Auswahl an OSS-Komponenten, die Vielzahl an Anbietern mit kommerziellem Support, hohe Sicherheit durch zeitnahe Updates sowie eine bessere Kompatibilität und Interoperabilität zwischen Tools und Komponenten genannt.

Unabhängig davon, ob Sie OSS in Ihrer Organisation verwenden oder nicht: Was ist aus Ihrer Sicht der größte Vorteil, der für den Einsatz von OSS spricht?



Basis: Alle Befragten (Wirtschaft: n=1.152 | Öffentliche Verwaltung: n=103) | Rest: »Weiß nicht/keine Angabe« | Quelle: Bitkom Research 2025

*Hohe Stabilität, geringe Fehleranfälligkeit (3%); Attraktiver IT-Arbeitsplatz, Motivation für Beschäftigte (2%); Nachhaltige Wirtschaftlichkeit/keine stark steigenden Kosten (2%); Kurze Innovationszyklen (1%); Möglichkeit zum Anbieterwechsel, bessere Verhandlungsmöglichkeiten, Reduktion Vendor-Lock-In (1%)

Abbildung 36: Wahrgenommene Vorteile von OSS in der öffentlichen Verwaltung

4.7 Nachteil von Open Source Software

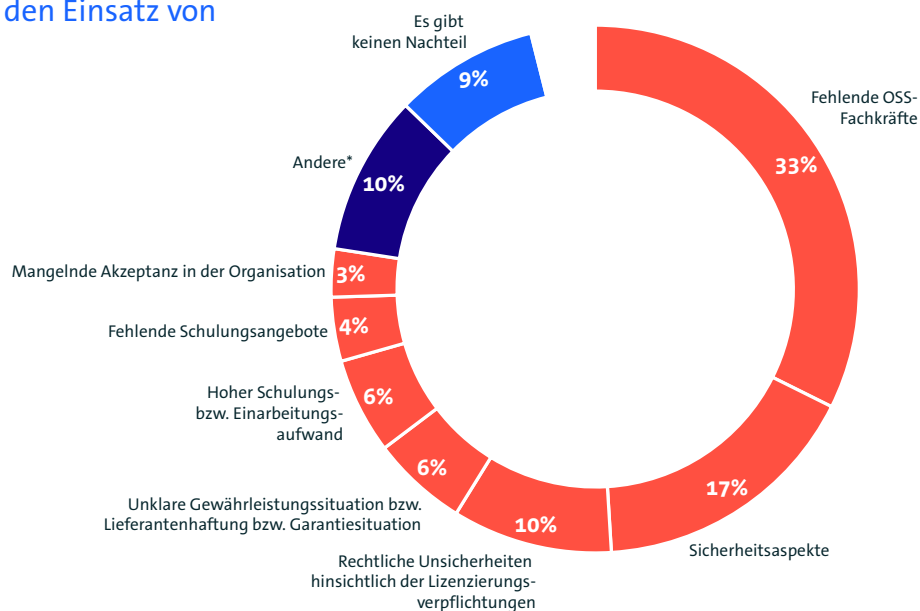
Am häufigsten genannt wird der Mangel an OSS-Fachkräften: 33 Prozent der Befragten sehen hierin das größte Problem. An zweiter Stelle stehen Sicherheitsaspekte, die von 17 Prozent hervorgehoben werden.

Rechtliche Unsicherheiten bezüglich Lizenzierungsverpflichtungen werden von 10 Prozent genannt, ebenso wie »andere« Nachteile. Unklare Gewährleistungssituationen oder Lieferantenhaftung sowie ein hoher Schulungs- oder Einar-

beitungsaufwand spielen für jeweils 6 Prozent eine Rolle. Fehlende Schulungsangebote nennen 4 Prozent, mangelnde Akzeptanz in der Organisation 3 Prozent.

Bemerkenswert ist, dass 9 Prozent der Befragten angeben, keinerlei Nachteile im Einsatz von OSS zu sehen. In der freien Wirtschaft vertreten 4 Prozent diesen Punkt (s. ↗Kapitel 1.7).

Und was ist aus Ihrer Sicht der größte Nachteil, der gegen den Einsatz von OSS spricht?



Basis: Alle Befragten (Wirtschaft: n=1.152 | Öffentliche Verwaltung: n=103) | Rest: »Weiß nicht/keine Angabe« | Quelle: Bitkom Research 2025
*Umstellung von herstelleregebundener Software auf OSS zu aufwendig (2%); Ungewisse Zukunft von OSS (2%); Fehlende Schnittstellen zu anderen Systemen (1%); Geringe Stabilität, hohe Fehleranfälligkeit (1%); Herausforderungen in der Supply Chain Security (1%); Sonstige (3%)

Abbildung 37: Wahrgenommene Nachteile von OSS in der öffentlichen Verwaltung

4.8 Open Source Program Offices (OSPOs)

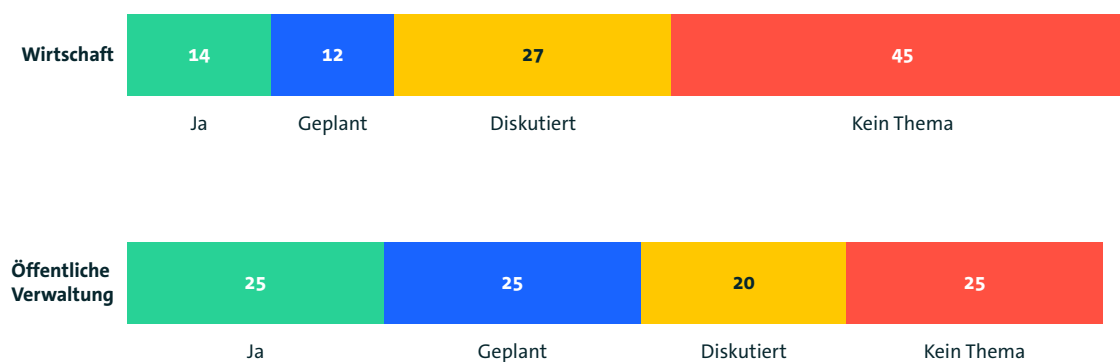
In der Wirtschaft haben 14 Prozent ein OSPO etabliert, weitere 12 Prozent planen die Einführung. 27 Prozent diskutieren das Thema, während für 45 Prozent ein OSPO derzeit kein Thema ist (s. ↗Kapitel 2.1).

In der öffentlichen Verwaltung liegt der Anteil derjenigen, die bereits ein OSPO eingerichtet haben, deutlich höher bei 25 Prozent. Weitere 25 Prozent planen die Einführung, und 20 Prozent diskutieren darüber. Nur ein Viertel der Befragten

(25 Prozent) gibt an, dass ein OSPO in ihrer Organisation kein Thema ist.

Insgesamt zeigt sich, dass OSPOs in der Verwaltung stärker verbreitet und konkreter in Planung sind, während in der Wirtschaft fast die Hälfte keinen Bezug zu diesem Thema sieht.

Haben Sie ein Open Source Program Office (OSPO) eingerichtet?



in Prozent

Basis: Unternehmen, die OSS verwenden, integrieren oder (weiter-)entwickeln (Wirtschaft: n=839 | Öffentliche Verwaltung: n=65) | Rest: »Weiß nicht/keine Angabe« | Quelle: Bitkom Research 2025

Abbildung 38: Anteil der Organisationen mit OSPOs im Public Sector

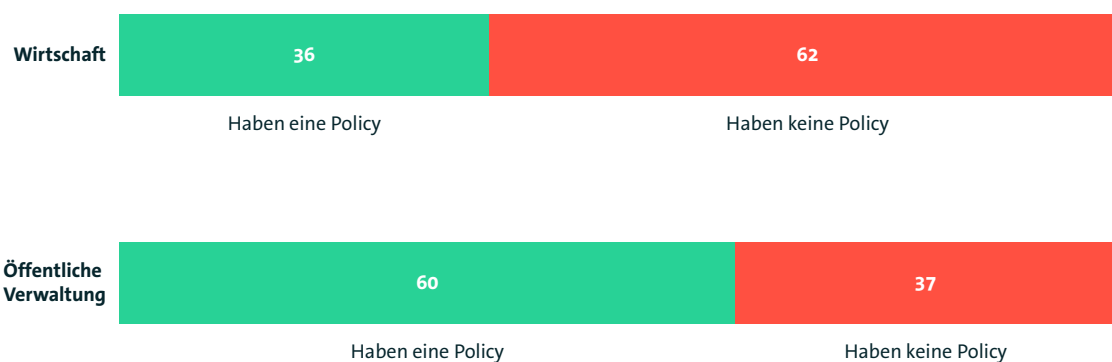
4.9 OSS-Policy

Ein Dokument mit Richtlinien und Regeln zum Umgang mit Open Source Software haben in der Wirtschaft 36 Prozent, während 62 Prozent keine festgelegten Regeln besitzen (s. ↗Kapitel 2.2).

In der öffentlichen Verwaltung ist das Bild beinahe invers: 60 Prozent geben hier an, eine OSS-Policy zu haben, während 37 Prozent darauf verzichten.

Damit wird deutlich, dass die öffentliche Verwaltung beim formalen Umgang mit OSS strukturierter vorgeht als die Wirtschaft. Während dort eine Mehrheit ohne definierte Richtlinien arbeitet, hat die Verwaltung überwiegend klare Regelungen etabliert.

Gibt es in Ihrer Organisation eine OSS-Policy, d. h. ein Dokument, in dem Richtlinien und Regeln zum Umgang mit OSS in Ihrem Unternehmen niedergeschrieben sind?



in Prozent

Basis: Unternehmen, die OSS verwenden, integrieren, (weiter-)entwickeln, oder sich anderweitig beteiligen (Wirtschaft: n=841 | Öffentliche Verwaltung: n=68) | Rest: »Weiß nicht/keine Angabe« | Quelle: Bitkom Research 2025

Abbildung 39: Vorhandensein einer OSS-Policy im Public Sector vs. Wirtschaft

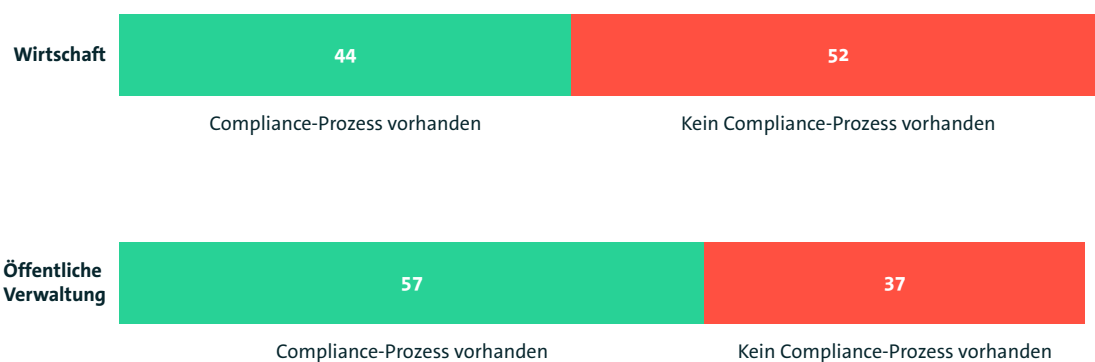
4.10 Compliance-Prozess für Mitarbeitende

In der Wirtschaft verfügen 44 Prozent über einen festgeschriebenen Compliance-Prozess, der für ihre Mitarbeitenden die Einhaltung regulatorischer Vorgaben verbindlich vorschreibt, während 52 Prozent angeben, keinen etabliert zu haben (s. ↗Kapitel 2.2).

Insgesamt zeigt sich, dass die öffentliche Verwaltung strukturierter mit verbindlichen Prozessen zum Einsatz von OSS umgeht, während in der Wirtschaft etwas mehr als die Hälfte noch ohne formalisierte Vorgaben arbeitet.

In der öffentlichen Verwaltung liegt der Anteil höher: Mehr als die Hälfte (57 Prozent) hat einen Compliance-Prozess eingerichtet, und nur 37 Prozent nicht.

Gibt es in Ihrer Organisation einen niedergeschriebenen Compliance-Prozess zum Umgang von Mitarbeitenden mit OSS?



in Prozent

Basis: Unternehmen, die OSS verwenden, integrieren, (weiter-)entwickeln, oder sich anderweitig beteiligen (Wirtschaft: n=841 | Öffentliche Verwaltung: n=68) | Rest: »Weiß nicht/keine Angabe« | Quelle: Bitkom Research 2025

Abbildung 40: Compliance-Prozesse für Mitarbeitende im Public Sector vs. Wirtschaft

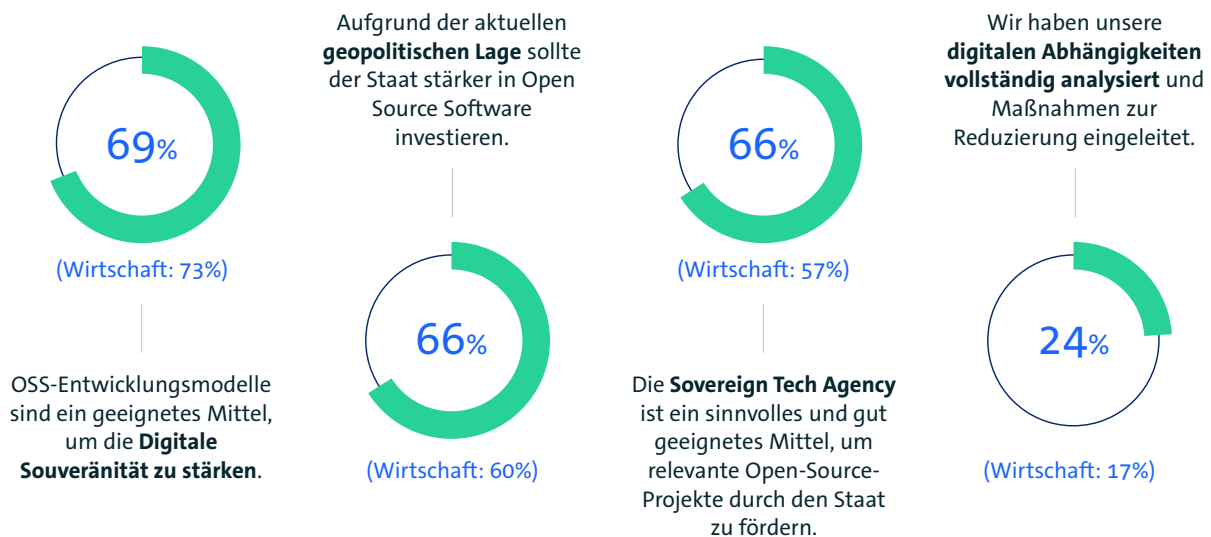
4.11 OSS als Instrument für Digitale Souveränität

69 Prozent sehen in OSS-Entwicklungsmodellen ein geeignetes Mittel, um die Digitale Souveränität zu stärken. In der Wirtschaft liegt der Anteil mit 73 Prozent noch etwas höher.

66 Prozent der Befragten stimmen zu, dass der Staat aufgrund der aktuellen geopolitischen Lage stärker in Open Source investieren sollte. Ebenfalls 66 Prozent halten die »Sovereign Tech Agency« für ein sinnvolles Instrument, um relevante Open-Source-Projekte staatlich zu fördern.

Deutlich geringer fällt die Zustimmung bei der Analyse und Reduzierung digitaler Abhängigkeiten aus: Nur 24 Prozent geben an, ihre Abhängigkeiten bereits vollständig analysiert und entsprechende Maßnahmen eingeleitet zu haben. In der Wirtschaft ist der Anteil noch niedriger, hier liegt er bei lediglich 17 Prozent (s. ↗Kapitel 3.4).

Inwiefern treffen die folgenden Aussagen auf Ihre Organisation bzw. Ihrer Meinung nach zu?



Basis: Alle Befragten (Wirtschaft: n=1.152 | Öffentliche Verwaltung: n=103) | Quelle: Bitkom Research 2025

Abbildung 41: Zustimmung zu Aussagen über OSS als Instrument für Digitale Souveränität in der öffentlichen Verwaltung

4.12 KI in der Softwareentwicklung

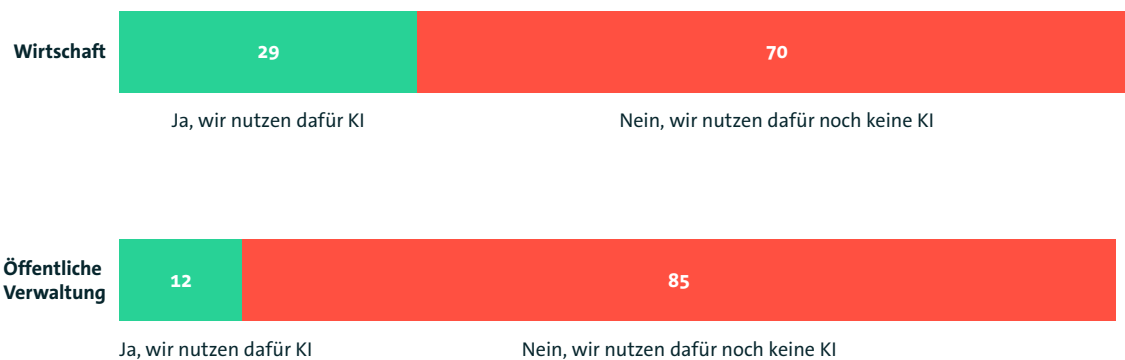
In der Wirtschaft nutzen 29 Prozent der Unternehmen bereits jetzt KI im Bereich Softwareentwicklung, während 70 Prozent das noch nicht tun (s. ↗Kapitel 3.1).

In der öffentlichen Verwaltung fällt der Anteil deutlich geringer aus: Nur 12 Prozent setzen KI in der Softwareentwicklung ein, hingegen 85 Prozent nicht.

Sowohl die freie Wirtschaft als auch die öffentliche Verwaltung stehen KI-generiertem Code zum Großteil kritisch gegenüber:

Je 56 Prozent der Befragten sagen, dass sie darin »eine Gefahr« sehen.

Setzt Ihre Organisation bereits KI in der Softwareentwicklung ein?



in Prozent

Basis: Alle Befragten (Wirtschaft: n=1.152 | Öffentliche Verwaltung: n=103) | Rest: »Weiß nicht/keine Angabe« | Quelle: Bitkom Research 2025

Abbildung 42: Einsatz von KI in der Softwareentwicklung im Public Sector vs. Wirtschaft

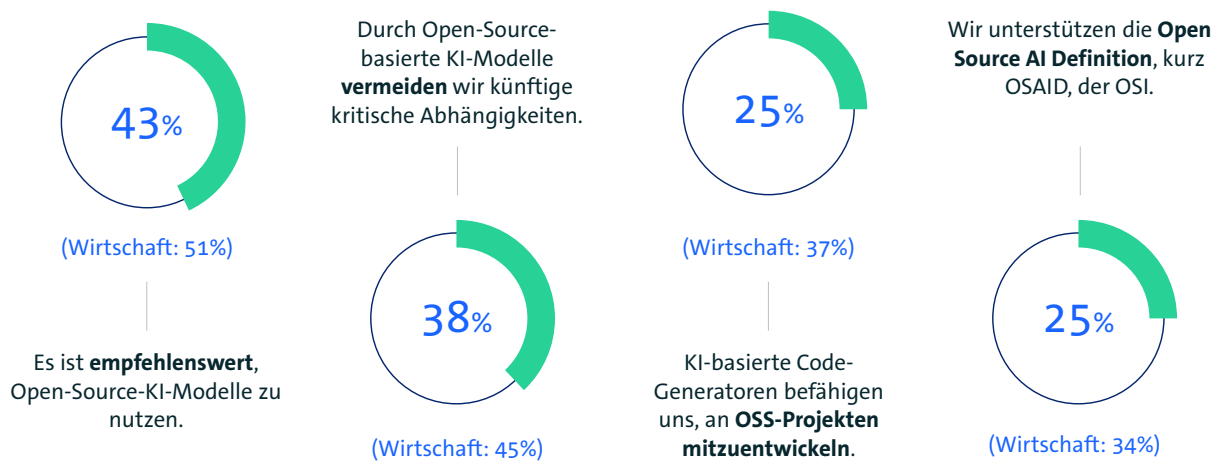
4.13 Open-Source-KI-Modelle

43 Prozent halten es in der öffentlichen Verwaltung für empfehlenswert, Open-Source-KI-Modelle zu nutzen. In der Wirtschaft liegt dieser Wert mit 51 Prozent noch etwas höher (s. 7Kapitel 3.2).

38 Prozent stimmen der Aussage zu, dass durch Open-Source-basierte KI-Modelle zukünftige kritische Abhängigkeiten vermieden werden können. Hierbei liegt die Wirtschaft mit 45 Prozent ebenfalls über dem Gesamtdurchschnitt.

Deutlich geringer fällt die Zustimmung bei zwei weiteren Aussagen aus: Nur 25 Prozent sehen in KI-basierten Code-Generatoren eine Möglichkeit, sich an OSS-Projekten zu beteiligen. Ebenso 25 Prozent unterstützen die »Open Source AI Definition« (OSAID) der OSI.

Inwiefern treffen die folgenden Aussagen auf Ihre Organisation bzw. Ihrer Meinung nach zu?



Basis: Alle Befragten (Wirtschaft: n=1.152 | Öffentliche Verwaltung: n=103) | Antworten für »Trifft voll und ganz zu« und »Trifft eher zu« | Rest: »Weiß nicht/keine Angabe« | Quelle: Bitkom Research 2025

Abbildung 43: Einschätzungen zu Open-Source-KI-Modellen in der öffentlichen Verwaltung

5 Case Studies

Hinweis

Die folgenden Beiträge sind Case Studies von Bitkom-Mitgliedsunternehmen. Sie bieten Einblicke aus Unternehmensperspektive und machen Projekte sowie praxisnahe Lösungen sichtbar.

Die Case Studies werden im Rahmen eines Sponsorings in dieser Publikation präsentiert. Für den Inhalt der jeweiligen Seite ist das entsprechende Unternehmen selbst verantwortlich.

5.1 OCCTET: Open Source Compliance für den CRA – kostenlos und praxisnah

Open Source ist allgegenwärtig – und regulatorisch im Fokus: Moderne Softwareprodukte bestehen zu über 90 Prozent aus Open-Source-Komponenten. Diese Beschleunigung der Entwicklung bringt jedoch auch Sicherheitsrisiken mit sich. Mit dem neuen Cyber Resilience Act (CRA) verpflichtet die EU alle Hersteller digitaler Produkte zu umfassenden Maßnahmen: Schwachstellen müssen fortlaufend identifiziert, dokumentiert und behoben werden – inklusive aller Open-Source-Bestandteile. Die Herausforderung: Die Anforderungen treffen auch kleine und mittelständische Unternehmen (KMU), die oft weder das Know-how noch die Ressourcen haben, um die komplexen Compliance-Pflichten zu erfüllen.

SBOMs & Cybersecurity

Für den Nachweis der CRA-Konformität wird eine lückenlose »Software Bill of Materials« (SBOM) benötigt – mit regelmäßiger Prüfung auf Sicherheitsstatus und Update-Strategien. Doch viele Komponenten sind tief eingebettet oder nur schwer erkennbar. Voll automatisierte Scans sind ungenau, manuelle Nacharbeit teuer. Der Zeit- und Kostenaufwand kann insbesondere für KMUs ein Hemmnis sein – und führt in der Praxis häufig zu Intransparenz über die tatsächlichen Open-Source-Bestandteile im Produkt.

Lösung: Bitsea: KI für rechtssichere Lizenzanalysen OCCTET

Das OCCTET-Projekt (Open Source Compliance Comprehensive Tools and Resources) ist eine von der EU finanzierte Initiative zur Verbesserung der Cybersicherheit und der Einhaltung des CRA. Der Schwerpunkt des Projekts liegt auf der Erstellung eines Open-Source-Toolkits zur Automatisierung des Compliance-Prozesses für freie und quelloffene Software, die in digitalen Produkten verwendet wird – speziell auf die Bedürfnisse europäischer KMU zugeschnitten.

Das Toolkit besteht unter anderem aus:

- einer CRA-Compliance-Checkliste.
- einem intelligenten Scanner zur SBOM-Erstellung, mit Identifikation zugehöriger bekannter Sicherheitslücken.
- einer föderierten Datenbankplattform zur Veröffentlichung der Ergebnisse von
- OSS-Komponentenbewertungen, die Beiträge verschiedener Interessengruppen ermöglicht.
- einem Reporting-Tool zur Dokumentation der Sicherheits- und Lizenzlage.

OCCTET wird von einem Konsortium aus Cybersicherheitsexperten, Open -Source-Organisationen und europäischen KMU getragen. Es baut auf etablierten Werkzeugen wie dem OSS Review Toolkit und ScanCode auf, die gezielt erweitert werden.

Ein zentrales Projektmitglied ist Bitsea, welche KI-basierte Funktionen beisteuert. Besonders im Fokus: die Automatisierung der Erkennung von Open Source. Hier analysiert eine KI auf Basis umfangreicher Daten Codefragmente und Metainformationen, um Komponenten korrekt zu identifizieren – ein enormer Zeitgewinn bei gleichzeitiger Fehlerreduktion. Auch »False Positives« werden per KI herausgefiltert.

Fazit: CRA-Compliance als Open Source

OCCTET zeigt, dass CRA-Compliance nicht teuer und kompliziert sein muss. Durch offene Entwicklung und Einbeziehung der Community wird ein Werkzeug geschaffen, das nicht nur Einzelunternehmen hilft, sondern die europäische Cybersicherheit insgesamt stärkt. Weiterführende Informationen finden sich unter occtet.eu. Die Veröffentlichung ist für Mitte 2026 geplant. Sprechen Sie uns zu diesem Thema gerne an!

Bitsea identifiziert versteckte Risiken in Softwaresystemen und unterstützt bei der Wahrung von IT-Compliance. Wir beraten Kunden bezüglich der nachhaltigen Nutzung und dem Management von Open Source Software. Zu unseren Kunden zählen namhafte Konzerne aller Branchen. Bitsea ist Partner des Bitkom und des OpenChain-Projektes.

Dr. Andreas Kotulla
Geschäftsführer Bitsea GmbH

5.2 Open Source Compliance in der Supply Chain

Moderne Softwareentwicklung ohne die Einbeziehung von Open-Source-Komponenten ist heutzutage undenkbar. So zeigt die Studie »The Value of Open Source« der Harvard Business School, dass viele kommerzielle Anwendungen zu über 90 Prozent aus Open-Source-Komponenten bestehen und damit erheblichen kommerziellen Wert für ihre Nutzer kreieren. Selbst in Nischenanwendungen werden häufig Entwicklungswerkzeuge auf OSS-Basis verwendet. Umso verwunderlicher ist es, dass dieser Einsatz von OSS häufig scheinbar mehr oder weniger unkoordiniert stattfindet.

Zumindest lassen die Antworten auf die Frage in der vorliegenden Ausgabe des Bitkom Open Source Monitors, ob es im Unternehmen eine OSS-Policy gibt, diesen Schluss zu. Verstärkt wird dieser Eindruck auch durch die geringe Verbreitung von Open Source Program Offices (OSPO). Die Bereitschaft, ein OSPO zu etablieren, kann als Indikator gesehen werden, dass das Unternehmen die Relevanz von OSS sowohl aus Sicht der Compliance als auch als strategisches Element sieht. Im Entwicklungsverbund zwischen Lieferanten und Kunden sind die OSPOs eine nicht zu verachtende vertrauensbildende Entität, da sie ein guter Ansprechpartner sowohl für interne als auch externe Anfragen sind.

Regelungen wie der Cyber Resilience Act (CRA) und andere Anforderungen zum Thema Security/Vulnerability oder SBOMs werden die Softwareentwicklung, insbesondere im Entwicklungsverbund, in Richtung mehr Transparenz verändern. Diese Veränderungen setzen eine OSS-Strategie voraus, die über ein OSPO konsistent gehalten werden sollte. Zurückblickend auf 12 Jahre OSPO bei Bosch und Mitarbeit in diversen Communities, haben sich folgende Schritte beim Umgang mit OSS als essenziell erwiesen:

Schritt 1: Organisation und Prozesse

Mit der OpenChain-Spezifikation (ISO5230) haben wir eine Grundlage, die Prozessbeschreibungen und auch organisatorische Maßnahmen für die Einhaltung von OSS-Compliance beschreibt. Diese Norm ist kostenfrei erhältlich, zusammen mit einer Vielzahl von weitergehenden Dokumenten, Prüflisten und einer Methode zur Selbstbewertung.

Schritt 2: Tools

Eine durchgängige OSS Compliance Toolchain betrachtet die Analyse der Abhängigkeiten, Scanning des Quelltextes, Aufzeigen von Schwachstellen, Anwendung der Leitplanken und Dokumentation der Ergebnisse.

Die Beschaffung der Tools ist häufig eine Kostenfrage und sorgt für Variantenvielfalt in der Supply Chain. In letzter Zeit wurden hier mehrere OSS-Projekte gestartet.

Aus unserer Sicht sind das Open Source Review Toolkit (ORT) und das darauf basierende Eclipse Apoapsis Projekt Lösungen, die eine Standardisierung innerhalb einer Organisation vorantreiben können, weshalb sich Bosch aktiv an der Entwicklung beteiligt. ORT ist auch Teil der Toolchains im mit EU-Mitteln finanzierten Projekt OCCTET, das KMUs und OSS-Entwickler bei der Einhaltung von Compliance mit dem CRA unterstützen soll. Dies unterstreicht die vielfältigen Einsatzmöglichkeiten für unterschiedliche Organisationen.

Schritt 3: Austauschformate

Aktuell haben wir mehrere Standards für Austauschformate von Compliance-Informationen und wiederum viele Normen und gesetzliche Regelungen, die unterschiedliche Informationen fordern.

Aus unserer Sicht ist hier das SEPIA-Projekt, das im Rahmen der SBOM Study Group des OpenChain-Projekts organisiert wird, eine gangbare Lösung. Aber auch hier gilt, wie in allen OSS-Projekten: Sie leben von der Einbringung unterschiedlicher Perspektiven und Kontributionen.

5.3 Brücken und Betriebssysteme – über das Unsichtbare, das uns alle trägt

Open Source Software ist das Fundament unserer digitalen Welt – sie steckt in Mobilitätssystemen, sicherheitskritischen Steuergeräten, Cloud-Plattformen und zunehmend auch in der öffentlichen Verwaltung. Doch wie bei Straßen und Brücken erkennen wir ihre Bedeutung oft erst, wenn sie nicht mehr tragen.

Was Open Source möglich macht, ist oft unsichtbar – aber systemrelevant.

Wir von der Kernkonzept GmbH übernehmen als Maintainerin des Open-Source-Betriebssystem-Frameworks L4Re Verantwortung für eine dieser tragenden Schichten. L4Re ist eine Mikrokern-Technologie, die weltweit in zertifizierten Infrastrukturen eingesetzt wird – vom Automobil über Smartphones und DSL-Router bis zur Avionik.

L4Re-Versionen werden in bis zu VS GEHEIM oder ISO 26262 ASIL B zertifizierten Anwendungen eingesetzt und sind selbst für die Verarbeitung von bis VS GEHEIM und NATO SECRET eingestuft Daten zugelassen und Common Criteria EAL4+ zertifiziert – alles basiert auf der Open-Source-Version.

Was L4Re ermöglicht – geprüfte Sicherheit auf Basis von Open Source – ist das Ergebnis einer kontinuierlichen Entwicklung seit fast 30 Jahren: begonnen an der TU Dresden, über Generationen an Forscher:innen hinweg weitergeführt und schließlich in eine haftende GmbH überführt. Heute übernehmen wir Verantwortung für Sicherheit, Zulassung, Patchpolitik – nicht nur für Code. Wir stehen mit Namen, Haftung und langfristigem Commitment für diese Infrastruktur ein.

»Solche Infrastrukturen lassen sich nicht allein durch Idealismus und Querfinanzierung sichern. Wer digitale Resilienz ernst meint, muss auch das staatliche Commitment für Forschung und Maintainerschaft mitdenken.«

Der Bitkom Monitor 2025 zeigt: 73Prozent der Unternehmen nutzen Open Source Software, aber nur 47Prozent beteiligen sich aktiv – und davon der Großteil über Subskriptionen und Services. Was wie freie Verfügbarkeit erscheint, ist oft stille Infrastrukturarbeit – zunehmend belastet durch Haftung, Sicherheitsdruck und neue EU-Regulierungen.

»Manche sehen Open Source als öffentlichen Code. Wir sehen darin Infrastruktur. L4Re ist wie eine digitale Brücke – tief im System, kaum sichtbar, aber sicherheitsstiftend. Damit sie hält, braucht es verlässliche Kooperation zwischen allen Stakeholdern.«

Praxis und Studien zeigen: Wenn Nutzung nicht durch Mitverantwortung flankiert wird, drohen Übernutzung und Erosion. Ein funktionierendes Open-Source-Ökosystem braucht klare Rollen, faire Beteiligung und strukturelle Rückkopplung – nicht nur neue Pflichten.

Wenn Open Source Teil digitaler Souveränität sein soll, braucht es politische wie wirtschaftliche Verlässlichkeit. Die Weiterentwicklung von Open Source ebenso wie die Maintainerarbeit sind keine Randerscheinung, sondern Teil der digitalen Grundversorgung.

Was es dazu braucht? Eine nachhaltige Beschaffungspolitik, die Open Source versteht und gleichwertig oder sogar bevorzugt behandelt. Mut zur Verantwortung und auch Wissen – auf Unternehmensseite. Und Ausbildungswege an Schulen, Universitäten und Betrieben, die jungen Menschen nicht nur zu Nutzer:innen, sondern zu Gestalter:innen unserer digitalen Infrastruktur machen.

Dr.-Ing. Adam Lackorzynski
CTO & Gründer

Katrin Kahle
Head of Product

5.4 Open Source ist allgegenwärtig – und ab 2027 auch reguliert

Mit dem Cyber Resilience Act (CRA) hat die EU erstmals ein umfassendes Cybersicherheitsgesetz für digitale Produkte mit Software geschaffen. Auch wenn viele Open-Source-Projekte vom CRA selbst ausgenommen sind, trifft er doch **jedes Unternehmen**, das Open-Source-Komponenten in seine Produkte integriert und damit kommerziell vertreibt – also praktisch die gesamte Industrie.

Besonders im Fokus: **Pflichten zur Erstellung und Pflege von SBOMs (Software Bill of Materials), Sicherheitsupdates über Jahre, und eine strukturierte Schwachstellenkommunikation**. Wer OSS-Komponenten einsetzt, haftet künftig auch für deren Risiken – unabhängig davon, ob diese selbst entwickelt oder von Dritten übernommen wurden.

Das verändert die Spielregeln

Neu ist dabei nicht, dass juristische Governance erforderlich ist – sondern dass sie erstmals gesetzlich verpflichtend geregelt wird. War Open-Source-Compliance bislang vor allem durch Lizenzbedingungen getrieben, ergänzt der CRA ergänzt diese Pflichten nun um explizite sicherheitsbezogene Vorgaben. Das hat Auswirkungen auf Vertragsgestaltung, interne Prozesse und die Zusammenarbeit mit Zulieferern.

Unternehmen brauchen jetzt nicht nur technische, sondern auch **juristische Governance** rund um OSS: Wer ist für die Lizenz- und Sicherheitsprüfung verantwortlich? Wie lässt sich der Open-Source-Einsatz im Produktlebenszyklus transparent dokumentieren? Und: Wie wird sichergestellt, dass betroffene Komponenten rechtzeitig gepatcht oder ersetzt werden?

Die gute Nachricht: Der CRA kann zum Katalysator für **besseres Open-Source-Management** werden – wenn Unternehmen frühzeitig reagieren. Wer jetzt in ein **Open Source Program Office (OSPO)** investiert, klare **Open-Source-Policies** etabliert und Tools für **automatisiertes SBOM-Tracking** einführt, schafft nicht nur Compliance – sondern auch **Vertrauen am Markt**.

Der CRA kommt – und mit ihm die Verantwortung, Open Source **strategisch, rechtssicher** und **resilient** zu nutzen. Für Unternehmen bedeutet das nicht nur Pflichten, sondern auch eine Chance, ihre digitalen Produkte robuster, transparenter und vertrauenswürdiger zu gestalten.

Osborne Clarke berät regelmäßig Unternehmen beim Aufbau rechtskonformer OSS-Prozesse, etwa durch:

- Vertragsgestaltung mit Zulieferern (Open-Source-Klauseln)
- Erstellung und Prüfung von SBOMs
- Compliance-Audits und Risikobewertung
- Etablierung von Incident-Response-Strukturen im OSS-Kontext

5.5 Open Source ermöglicht weitere Wertschöpfung und Digitale Souveränität

OSS Maturity als strategischer Vorteil

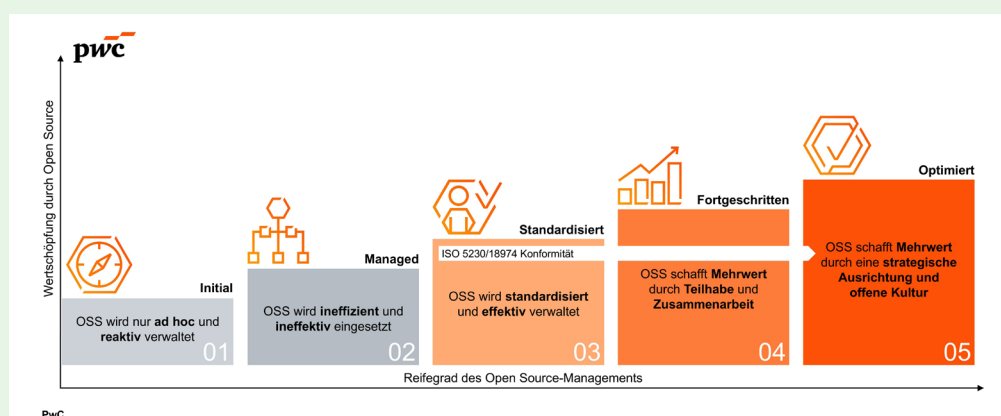
Angesichts geopolitischer Spannungen wird OSS¹ zum Werkzeug für Digitale Souveränität. Die hier vorliegende Bitkom-Umfrage hat gezeigt, dass mehr als 70 Prozent der Befragten OSS-Entwicklungsmodelle als geeignetes Mittel sehen, um die Digitale Souveränität zu stärken. Ebenso viele geben an, OSS einzusetzen, doch nur wenige Organisationen haben eine OSS-Strategie, und weniger als 40 Prozent wirksame Compliance-Maßnahmen implementiert. Zur Stärkung der Digitalen Souveränität muss jedoch sichergestellt sein, dass OSS standardisiert eingesetzt wird – übertragen auf unser Reifegradmodell, entspricht dies mindestens dem Reifegrad Level 3. Dazu gehören die effektive Implementierung von Strategie, Richtlinien, Prozessen, Compliance- und Sicherheitstools mit automatisierten Workflows für vollständige und korrekte Software-Stücklisten (SBOMs) sowie entsprechende Schulungen. Nach dieser Umsetzung ist es möglich, weiteren Mehrwert für die Organisation zu schaffen. Höhere Reifegrade bieten strategische Vorteile und fördern durch Zusammenarbeit und Offenheit maximale Wertschöpfung durch und mit OSS. Langfristig kann dadurch eine Kultur der Offenheit etabliert werden. OSS wird somit zum Dreh- und Angelpunkt für die Stärkung, Ausweitung und Erschaffung von Geschäftsmodellen.

Regulatorik fordert und fördert OSS Maturity

Regularien wie CRA, DORA, PLD, CER und NIS2 verpflichten zur strukturierten Handhabung von Open Source. ISO-Normen wie ISO/IEC 5230 und 18974 bieten dafür eine klare Grundlage: Sie fordern standardisierte Prozesse für Lizenz- und Sicherheitsmanagement und fördern so die Erfüllung regulatorischer Vorgaben. Eine robuste SBOM-Erstellungspraxis und rollenbasierte Trainings fördern die korrekte Anwendung. Besonders im Finanzsektor zeigt sich: Wer OSS professionell managt, steigert nicht nur die digitale Resilienz, sondern erreicht schneller höhere Reifegradlevel und positioniert sich als vertrauenswürdiger Marktteilnehmer und IKT-Dienstleister.

Unterstützung der Open Source Maturity

Unsere Services, von der OSS-Strategie zur operativen Umsetzung, von der Richtlinie zum Code-Scan und SBOM-Generierung, optimieren Ihren Open-Source-Reifegrad. Mit Hilfe gezielter Benchmarkings zeigen wir Ihnen den aktuellen Reifegrad Ihrer OSS-Praktiken und unterstützen Sie in der strategischen Ausrichtung, helfen bei der Einrichtung oder Optimierung Ihres Open Source Program Offices (OSPO), um OSS Security, Compliance und Wertschöpfung zu fördern. Höhere Reifegrade werden damit durch ein klares Service-Modell, strategische Kollaboration sowie Frameworks für Kontribution, Co-Creation und Inner Source unterstützt.



»PwC« bezeichnet in diesem Dokument die PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, die eine Mitgliedsgesellschaft der PricewaterhouseCoopers International Limited (PwCIL) ist.

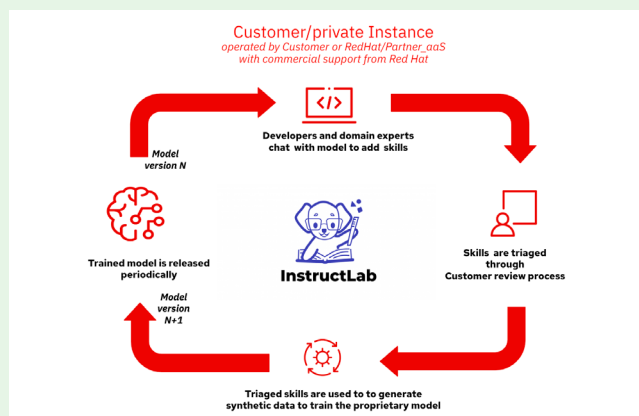
¹ <https://www.pwc.de/opensource>

Marcel Scholze
Director | Open Source Services,
Digitale Souveränität

5.6 Mit Open Source zur transparenten KI-Nutzung

Um wettbewerbsfähig und zukunftssicher zu bleiben, führt für Unternehmen kein Weg an Künstlicher Intelligenz vorbei. Doch gerade in kritischen Unternehmensbereichen ist ein uneingeschränkter Einsatz dieser Technologie selten verantwortbar. Sicherheit, Transparenz, Stabilität und Unabhängigkeit müssen gewahrt bleiben. Genau hier rücken Open-Source-Prinzipien, -Technologien und -Lösungen zunehmend in den Fokus.

Open Source zeichnet sich durch Transparenz, Interoperabilität und Vermeidung eines Vendor-Lock-ins aus. Darüber hinaus steht Open Source für Agilität, Flexibilität, Skalierbarkeit und eine hohe Innovationskraft durch die dynamische, Community-getriebene Entwicklung. Diese Vorteile von Open Source kommen insbesondere im Bereich KI zum Tragen. Schließlich sollte beim Einsatz von KI zum einen immer ein hohes Maß an Nachvollziehbarkeit gewährleistet sein. Kaum ein Unternehmen möchte eine Blackbox in Bezug auf Algorithmen, Trainingsdaten oder Modelle haben. Zum anderen bilden Open-Source-basierte Plattformen, Tools und Technologien auch die optimale Basis für den erfolgreichen und flexiblen Betrieb von KI-Modellen – unabhängig davon, ob diese letztlich der Definition Open-Source-KI entsprechen. Im KI-Kontext bedeutet der Open-Source-Ansatz zum Beispiel auch einen Zugang zu zertifizierten KI-Partnern im Rahmen eines Ökosystem-Konzepts. Unternehmen können so Komplettlösungen für die Entwicklung, das Deployment und das Management von Modellen für KI-gestützte Anwendungen relativ einfach und schnell nutzen.



Das von IBM und Red Hat ins Leben gerufene Community-Projekt InstructLab unterstützt ein vereinfachtes Experimentieren mit generativen KI-Modellen und eine optimierte Modellanpassung. | Quelle: Red Hat

Der Siegeszug von Open Source und offenen Standards hält im Softwarebereich bereits seit mehr als drei Jahrzehnten an. Die Open-Source-Konzepte werden im KI-Bereich dieselbe Katalysator-Funktion einnehmen. Denn nur mit einem offenen Ansatz wird es letztlich möglich sein, mit der schnellen KI-Entwicklung Schritt zu halten. Unterstrichen wird die zunehmende Bedeutung von Open Source im Bereich KI dadurch, dass hier derzeit viele Projekte intensiv vorangetrieben werden. Zu nennen sind beispielsweise das Instruct-Lab-Projekt oder die Granite-Familie von Open-Source-lizenzierten Modellen. InstructLab ist eine Lösung zur Optimierung von LLMs, die weniger Daten und Rechenressourcen für das Training eines Modells benötigt. Außerdem ist InstructLab auch für Anwender nutzbar, die keine Data Scientists sind. Die Granite-3.0-Modellfamilie bietet Unternehmen die Möglichkeit, KI-Anwendungsfälle wie Codegenerierung, Verarbeitung natürlicher Sprache oder Erkenntnisgewinnung aus großen Datensätzen abzudecken. Nicht zuletzt ist derzeit auch das Open-Source-Projekt vLLM in aller Munde. Mit der vLLM-Technologie können Berechnungen mit einem LLM schneller durchgeführt werden, beispielsweise durch eine effizientere Nutzung des GPU-Speichers. Damit werden auch die Geschwindigkeit, Performance und die Flexibilität bei der Nutzung generativer Anwendungen verbessert. Dass Unternehmen zunehmend den Open-Source-Weg bei der Nutzung von KI gehen, unterstreicht auch der aktuelle »Open Source Monitor« von Bitkom Research. An der Untersuchung zum Open-Source-Einsatz in Deutschland beteiligten sich mehr als 1.100 Firmen. Über 50 Prozent halten es für empfehlenswert, Open-Source-KI-Modelle zu nutzen. Außerdem erklärt auch mehr als die Hälfte der Unternehmen, dass durch Open-Source-basierte KI-Modelle künftige kritische Abhängigkeiten vermieden werden können. Zweifellos wird die breite Open-Source-Community die Open-Source-KI-Innovation konsequent vorantreiben. Damit wird die Welt der KI weiter geöffnet und demokratisiert. Das ist gerade in einer Zeit geopolitischer Verwerfungen von Bedeutung, in der Digitale Souveränität eine immer wichtigere Rolle spielt. Auch Open-Source-KI kann ein zentraler Baustein zur Erreichung dieser Unabhängigkeit sein.

Gregor von Jagow
Senior Director & Country
Manager Germany

5.7 NeoNephos Foundation: Open Source für Europas Digitale Souveränität

Am [31. März 2025](#) wurde unter dem Dach der Linux Foundation Europe die gemeinnützige [NeoNephos Foundation](#) gegründet. Ziel ist es, Open-Source-Technologien zu fördern, die mit den strategischen Zielen des europäischen Förderprogramms [IPCEI-CIS](#) (Important Project of Common European Interest in Cloud Infrastructure and Services) übereinstimmen – insbesondere durch offene, interoperable Cloud- und Edge-Komponenten.

Ein aktueller [Marktbericht](#) der Synergy Research Group (Juli 2025) zeigt die Dringlichkeit: **Europäische Cloud-Anbieter halten nur 15 Prozent Marktanteil**, während US-Hyperscaler dominieren. NeoNephos setzt hier an – mit dem Ziel, technologische Abhängigkeiten zu reduzieren und Digitale Souveränität durch offene Referenzarchitekturen und offen zugängliche Softwarekomponenten zu stärken.

Das IPCEI-CIS Budget von 3,5 Milliarden Euro fließt in über 110 Projekte von mehr als 100 Unternehmen aus 12 EU-Mitgliedstaaten. Die Investition zielt im Einklang mit der EU Digitalstrategie darauf ab, Europas Digitale Souveränität zu stärken, technologische Abhängigkeiten zu reduzieren, Interoperabilität zu fördern, Nachhaltigkeit sicherzustellen und die Cybersicherheit innerhalb eines dezentralen Multi-Provider Cloud-Edge Kontinuums zu verbessern.

SAP ist mit dem Projekt **Apeiro Reference Architecture** ([ApeiroRA](#)) maßgeblich an der Entwicklung von Standards und Referenzarchitekturen im IPCEI-CIS Förderprogramm beteiligt. SAP hat alle Beiträge zu Apeiro als Open Source (Apache 2.0) in die NeoNephos Foundation gestiftet. Dies ermöglicht eine vendor-neutrale Governance und eine kollaborative Weiterentwicklung mit anderen Firmen im Sinne der öffentlichen Förderung.

Viele der Projekte, die SAP eingebracht hat, werden bereits produktiv bei SAP und anderen Partnern eingesetzt oder sind Projekte, die SAP aktuell in der NeoNephos Foundation aufbaut und unterstützt, um sie zukünftig einzusetzen. Diese produktive Nutzung sichert eine Weiterentwicklung weit über die Laufzeit des IPCEI-CIS Programms hinaus.

Das Ziel der Gründungsmitglieder von NeoNephos – darunter STACKIT, Deutsche Telekom, TNO, Cyberus Technology, Clyso und 23 Technologies – ist es, dieses Ökosystem mit eigenen, komplementären Open-Source-Projekten zu stärken. Diese Beiträge erweitern die Referenzarchitektur gezielt um zusätzliche Funktionen und fördern ihre Verbreitung im europäischen Markt.

So bringt etwa die Deutsche Telekom zusammen mit anderen europäischen Telekommunikationsanbietern das Projekt **Katalis** in die Stiftung ein. Dieses Projekt zielt auf die Standardisierung des Zugangs zu Telekommunikationsdiensten und -ressourcen ab.

Die Idee, durch die Förderung von Offenheit und Interoperabilität eine nachhaltige und innovative Cloud-Infrastruktur in Europa zu schaffen, weckt Interesse. Nach der Stiftungsgründung sind auch die Firmen x-cellent und Elastx hinzugekommen, und weitere potenzielle Partner haben ihr Interesse bekundet.

Die **Linux Foundation Europe** bietet NeoNephos eine neutrale Governance-Struktur und Zugang zu einem etablierten Open-Source-Ökosystem. In enger Verbindung zur Cloud Native Computing Foundation (CNCF) profitieren die Projekte von Best Practices und Community-Standards, ohne selbst von CNCF verwaltet zu sein.

Mit der NeoNephos Foundation entsteht somit ein strategisches, offenes Technologie-Ökosystem, das als operative Säule der europäischen Cloud-Initiative fungiert – herstellerneutral, gemeinschaftlich weiterentwickelt und auf langfristige Souveränität ausgerichtet.

Peter Giese
Director of SAP Open Source
Program Office

5.8 Experten-Statement

Seit 2021 erhebt der Open Source Monitor, wie der öffentliche Sektor generell zu Open Source Software steht. Von 2021 ursprünglich 32Prozent positiven Rückmeldungen ist diese Anzahl 2025 auf 52Prozent gestiegen. Währenddessen hielt sich die ablehnende Fraktion bis 2023 auf einem gleichbleibenden Niveau von 23Prozent, hat sich jedoch in den letzten zwei Jahren auf 12Prozent fast halbiert. Diese Entwicklung reflektiert deutlich die fortwährende Debatte um offene Technologien und die Notwendigkeit, technologische Abhängigkeiten von einzelnen Herstellern in Zeiten geopolitischer Veränderungen zu verringern. Hier haben besonders Organisationen wie das ZenDiS die Wahrnehmung von Open Source Software (OSS) in der öffentlichen Hand sehr positiv beeinflusst.

Die Welt verändert sich...

Auch ein Blick in die genannten Vor- und Nachteile spiegelt diese Veränderungen in der IT-Welt deutlich wider. So verdoppelt sich der Anteil derjenigen, die in OSS eine Erhöhung der Digitalen Souveränität sehen, von 4Prozent (2023) auf 9Prozent (2025) und es halbiert sich im gleichen Zeitraum der Anteil derjenigen, die in OSS gegenüber proprietärer Software keinen Vorteil sehen (16Prozent auf 9Prozent). Trotzdem bleibt der Einsatz von OSS über die Jahre hinweg auf einem gleichbleibenden Niveau (64Prozent, 59Prozent, 63Prozent).

Wirtschaftsfaktor Open Source

Diese Entwicklung im öffentlichen Sektor scheint vor allem in einem Faktor begründet: Dem fehlenden Fachpersonal (2023: 28Prozent, 2025: 33Prozent). Vergessen wird, dass die Nutzung von OSS potenziellen Fachkräften eine moderne, flexible und zukunftsorientierte IT-Struktur bietet und Arbeitgeber so deutlich attraktiver macht. Ist es also ein klassisches Henne-Ei-Problem? Um Einstiegshürden zu überwinden, stehen im starken OSS-Ökosystem in Deutschland kommerzielle Lösungsanbieter und Dienstleister zur Verfügung. Gerade Open Source ermöglicht durch die Entwicklungsmodelle und Innovationskraft ein liberales, unternehmerisches Handeln und somit die Option, die heimische Digitalwirtschaft einzubinden und zu entwickeln. Damit ist die Nutzung von OSS

gleichzeitig auch Industriepolitik und fördert damit wiederum den Ausbau von Fachkräften in der Region.

Nachhaltig wirtschaftlich

Auch wenn 17Prozent der Befragten in der Nutzung von OSS geringere Kosten als wesentlichen Vorteil sehen, betrachten nur 2Prozent dies aus einer langfristigen Perspektive im Kontext einer nachhaltigen Wirtschaftlichkeit. Dabei ist Letzteres strategisch betrachtet enorm wichtig. Ein Einstieg von vorhandenen Lösungen hin zu Open Source wird i.d.R. von Migrationskosten begleitet, die mitunter den preislichen Vorteil durch Wegfall von Lizenzgebühren aufzehren oder gar übersteigen können. Der Kostenvorteil stellt sich also oftmals erst im weiteren Verlauf ein. Der strategische Wert, mit Open Source eine Multi-Vendor-Strategie umsetzen zu können, umso eher. Und gerade die Offenheit, Transparenz und Wechselbarkeit von Open Source erlauben einzelnen Anbietern kein Preisdiktat. Denn der nächste Anbieter ist in der Lage, ein wettbewerbsfähiges Angebot zu unterbreiten. Gleichwohl empfehlen wir, die »Vergabekriterien für eine nachhaltige Beschaffung von Open Source Software«¹ zu beachten, um so das OSS-Ökosystem aktiv zu unterstützen und langfristig ökologisch Open-Source-Lösungen einsetzen zu können.

Alles in allem ist die Zeit reif, in Deutschland raus aus der Debatte, rein in die Umsetzung zu mehr Nutzung von OSS zu kommen. Mit den Worten von Goethe: »Es ist nicht genug zu wissen, man muss auch anwenden; es ist nicht genug zu wollen, man muss auch tun.«

¹ Gekennzeichnet ist die Stelle mit einer 1 im Statement. <https://osb-alliance.de/publikationen/veroeffentlichungen/vergabekriterien-fuer-eine-nachhaltige-beschaffung-von-open-source-software>

Torsten Hallmann

Berater für Innovation und Open Source in der öffentlichen Hand

5.9 Software automatisiert prüfen mit dem Badgesystem

Digitale Souveränität ist als zentrales Thema in der öffentlichen Wahrnehmung angekommen. Damit steigt auch das Angebot an Open-Source-Lösungen, die ein Wegbereiter für Souveränität sind. Doch nur Quelloffenheit allein ist kein qualitatives Merkmal. Die Software muss sicher sein, richtig lizenziert und auch aktiv gewartet werden. Bisher wird das vor allem per Einzelfallprüfung sichergestellt – ein herausfordernder und zeitintensiver Prozess. Es braucht einfache Verfahren, um als Verwaltung nicht in ein Skalierungsproblem zu geraten. Das Badge-Programm auf openCode ebnet den Weg dafür, indem es Aktivität und Integrität messbar macht und so den Weg zur Nachnutzung bereitet.



Das Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS) verantwortet seit Januar 2024 die Plattform openCode, die seit 2022 verfügbar ist. In nur drei Jahren hat sich openCode zur zentralen Anlaufstelle für Open-Source-Projekte der Öffentlichen Hand entwickelt: Inzwischen sind über 8.000 User registriert, die an 3.000 Projekten arbeiten. Pro Monat kommen etwa 200 neue Projekte hinzu. Damit diese Projekte leichter in die Nachnutzung kommen, wurde Anfang 2025 das Badge-Programm eingeführt.

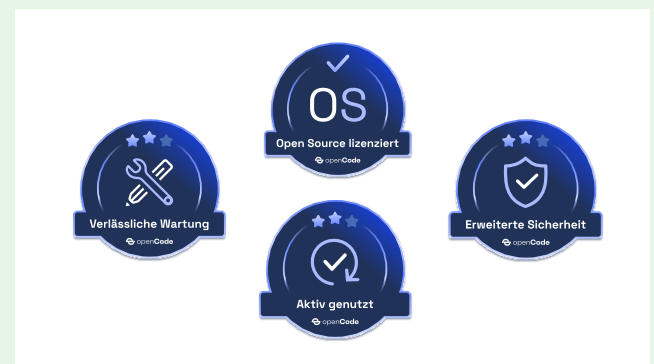
Auf einen Blick: Wartung, Nutzung, Sicherheit

Das Badge-Programm prüft Softwareprojekte nach bestimmten Kriterien automatisch und vergibt auf dieser Basis einen detaillierten Report und Auszeichnungen (Badges). Neben der Prüfung auf Aktivität innerhalb des Projekts, Softwarelizenzen und Nachnutzung stehen Sicherheitsaspekte und Softwarequalität im Fokus.

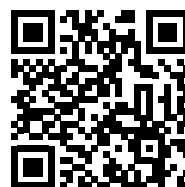
Paradigmenwechsel: keine Einzelfallprüfungen

openCode strebt einen Paradigmenwechsel in der Bewertung von Software an. In der Regel wird die Einsatzfähigkeit einer Software durch Einzelfallprüfungen nach lokalen Kriterien bestimmt. Diesen zeit- und ressourcenintensiven Prozess lässt openCode mit dem Badge-Programm hinter sich. Stattdessen liegt der Fokus auf der Zuverlässigkeit des Prüfverfahrens selbst. Das bedeutet, dass nicht nur die Code-Qualität selbst bewertet wird. Vielmehr bewertet das Badge-System den attestierten Einsatz, die Aktivität im

Projekt und klare Sicherheitsmerkmale. Im Vergleich zu Einzelfallprüfungen ist dieses Verfahren aufwandsarm und weitestgehend auf Softwareprodukte anwendbar, da die Bewertung anhand einheitlicher Kriterien stattfindet. Das macht das Prüfverfahren effizient, konsistent, automatisierbar, und ermöglicht zudem vergleichbare Ergebnisse. Momentaufnahmen gehören der Vergangenheit an.



Insgesamt ermöglicht das Badge-Programm von openCode eine skalierte Prüfung, die dem gestiegenen Softwareaufkommen gerecht wird. Es kann mit der Innovationsgeschwindigkeit von Open-Source-Technologien Schritt halten und schafft durch ein einheitliches und standardisiertes Verfahren Transparenz und Vertrauen bei der Bewertung von Software. Durch die Früherkennung von Risikofaktoren verschiebt es Sicherheitsprüfungen von der Reaktion in die Prävention und kann damit zum wichtigen Baustein für eine digital sichere Verwaltungslandschaft werden.



Mehr zum Programm erfahren:

↗ <https://badges.opencode.de/>

Leonhard Kugler
Leiter Open-Source-Plattform

6 Methodik & Anhang

Befragung Wirtschaft

Auftraggeber	Bitkom
Methodik	Computergestützte telefonische Befragung/ Computer Assisted Telephone Interview (CATI)
Grundgesamtheit	Unternehmen in Deutschland mit mindestens 20 Beschäftigten
Zielpersonen	Verantwortliche für das Thema Open Source Software im Unternehmen, alternativ: Verantwortliche für das Thema Software-Einsatz bzw. Software-Entwicklung
Stichprobengröße	n=1.152
Befragungszeitraum	KW 15 bis KW 21 2025
Gewichtung	Repräsentative Gewichtung des Datensatzes auf Grundlage des aktuellen Unternehmensregisters des Statistischen Bundesamtes
Statistische Fehlertoleranz	+/- 3 Prozent

Befragung Public Sector

Auftraggeber	Bitkom
Methodik	Computergestützte telefonische Befragung/ Computer Assisted Telephone Interview (CATI)
Grundgesamtheit	Organisationen in Deutschland mit mindestens 20 Beschäftigten
Zielpersonen	Verantwortliche für das Thema Open Source Software in der Organisation, alternativ: Verantwortliche für das Thema Software-Einsatz bzw. Software-Entwicklung
Stichprobengröße	n=103
Befragungszeitraum	KW 16 bis KW 22 2025
Gewichtung	Keine Gewichtung
Statistische Fehlertoleranz	-

Herausgeber

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Fachliche Leitung

Felix Ansmann

Wissenschaftliche Leitung

Bettina Lange

Redaktion

Lennart Glamann

Copyright

Bitkom 2025
CC BY 4.0

DOI

10.64022/2025-open-source-monitor

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte wurden mit größtmöglicher Sorgfalt erstellt, jedoch besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität. Insbesondere kann diese Publikation nicht den besonderen Umständen des Einzelfalls Rechnung tragen. Eine Verwendung liegt daher in der eigenen Verantwortung der Leserin bzw. des Lesers. Jegliche Haftung wird ausgeschlossen.

Die Studie untersucht den Stand von Open Source Software (OSS) in deutschen Unternehmen und öffentlichen Verwaltungen im Jahr 2025. Sie zeigt: 73 Prozent der Unternehmen und 63 Prozent der Behörden setzen OSS bereits ein, meist intern und zur Kostenreduktion. Sicherheits- und Funktionsaspekte sind die zentralen Auswahlkriterien, doch fehlen vielerorts Strategien, Policies und spezialisierte Fachkräfte. Europäische Vorgaben wie der Cyber Resilience Act treiben den Aufbau von Compliance-Strukturen, wobei erst 14 Prozent der Unternehmen ein Open Source Program Office etabliert haben. Künstliche Intelligenz wird bislang zurückhaltend genutzt, 29 Prozent verwenden KI-Code-Generatoren, 56 Prozent sehen darin jedoch Risiken. Mehrheitlich gilt OSS als Schlüssel zur digitalen Souveränität – 73 Prozent der Unternehmen und 69 Prozent der Verwaltungen sehen darin ein geeignetes Mittel, Abhängigkeiten zu reduzieren.

Grundlage der Studie ist eine repräsentative Befragung von 1.152 Unternehmen ab 20 Beschäftigten sowie 103 Organisationen des Public Sector in Deutschland.

DOI

10.64022/2025-open-source-monitor